UNIVERSIDADE DE LISBOA
FACULDADE DE CIÊNCIAS
DEPARTAMENTO DE INFORMÁTICA

DETEÇÃO E RESPOSTA A INTRUSÕES EM DISPOSITIVOS MÓVEIS

Tiago Oliveira Martins Sanina dos Santos

MESTRADO EM SEGURANÇA INFORMÁTICA

Dissertação orientada por:
Prof. Doutor Tiago João Vieira Guerreiro

Prof. Doutor Fernando Manuel Valente Ramos

2016

Agradecimentos

Aos meus pais pelo incentivo, apoio e ensinamentos de sempre. À restante família pela motivação e palavras de encorajamento durante todo o meu percurso académico e pessoal.

Aos Professores Doutor Tiago Guerreiro e Doutor Fernando Ramos pelo profissionalismo, partilha de conhecimentos e de experiências, orientação e disponibilidade que sempre demonstraram. Ao meu colega Diogo Marques pelo seu contributo valioso para o sucesso alcançado nas diferentes etapas deste processo.

À equipa do DI-LaSIGE pela forma como me integrou e pelos novos desafios que me proporcionaram.

Uma palavra de apreço também a todos aqueles que participaram nos grupos de foco e nos testes de usabilidade por tornarem possível a concretização da minha dissertação.

Agradeço ainda aos meus amigos e colegas a amizade, o companheirismo e os bons momentos que me proporcionaram.

A todos o meu obrigado.

Aos meus avós.

Resumo

Os *smartphones* estão cada vez mais presentes de forma ubíqua na nossa vida pessoal, social e profissional. Estes contêm um grande volume de informação sensível que queremos proteger contra intrusões físicas, preservando a sua segurança e a nossa privacidade.

Os principais mecanismos de segurança são os métodos de autenticação. Embora eficazes numa situação de perda/roubo, são vulneráveis a ataques perpetrados por pessoas socialmente próximas. Acresce que, quando o dispositivo é partilhado, independentemente das medidas de supervisão adotadas, a barreira de autenticação é ultrapassada e não existem mecanismos de segurança adicionais.

Os utilizadores, quando partilham o *smartphone*, receiam, por um lado, que a pessoa invada a sua privacidade e, por outro, que atitudes de vigilância explícitas possam comprometer as suas relações sociais.

Um sistema de deteção e resposta a intrusões físicas para *smartphones* deverá colmatar quaisquer limitações inerentes aos métodos de autenticação e (in)disponibilizar o acesso a determinados conteúdos e funcionalidades em situações de acesso indevido e de partilha.

Uma das contribuições deste trabalho foi conceber e desenvolver um sistema (designado *SmartIDR*) de deteção e resposta a intrusões para s*martphones* com recurso a um dispositivo secundário *wearable* – *smartwatch* –, que permite a interação inconspícua com o dispositivo primário. Os mecanismos de deteção e resposta são baseados na distância (comunicação *Bluetooth*) entre os dispositivos.

O sistema caracteriza-se por monitorizar os eventos ocorridos no *smartphone* e responder remotamente, e em tempo real, a situações de intrusão através do *smartwatch*; por oferecer um conjunto de múltiplas configurações de resposta; por ser acessível a utilizadores comuns; e por não comprometer a usabilidade dos dispositivos.

Para analisar o impacto desta nova abordagem foram efetuados estudos transversais com potenciais utilizadores. Os resultados obtidos indicaram que o *SmartIDR* vai ao encontro das necessidades e expetativas de segurança e privacidade dos utilizadores de *smartphones*, com eficácia, eficiência e um nível de satisfação bastante positivo.

Palavras-chave: Dispositivos Móveis, Segurança, Usabilidade, Sistema de Deteção e Resposta a Intrusões Físicas.

Abstract

Smartphones are increasingly ubiquitous in our personal, social and professional lives. They contain a large amount of sensitive information that we want to protect against physical intrusions, preserving their security and our privacy.

The main security mechanisms of these devices are the authentication methods based on a secret or biometrics. Although effective in a situation of loss/theft, they are vulnerable to attacks by people socially close.

When users share their smartphones, they fear, on the one hand, that the person might invade their privacy and, on the other hand, that attitudes of explicit surveillance could compromise their social relations.

An intrusion detection and response system to physical intrusions for smartphones should address any limitations inherent to authentication methods, and provide (or not) access to certain content and functionality in situations of unauthorized access and sharing.

In this work, we designed and developed an intrusion detection and response system (called *SmartIDR*) for smartphones using a secondary wearable device – smartwatch –, which allows the inconspicuous interaction with the primary device.

The mechanisms of detection and response are based on distance (Bluetooth communication) between devices.

The system is characterized by monitoring events happening on the smartphone and responding remotely, and in real-time, to intrusion situations, by using a smartwatch; providing a set of multiple response settings; be accessible to ordinary users; and not compromising the usability of devices.

To analyze the impact of this new approach, we conducted cross-sectional studies with potential users. The results indicated that *SmartIDR* meets the needs and expectations of security and privacy of smartphone users, with effectiveness, efficiency and high user satisfaction.

Keywords: Mobile Devices, Security, Usability, Intrusion Detection and Response Systems.

Conteúdo

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução

"*The citizens will divide between those who prefer convenience and those who prefer privacy.*"

Niels Ole Finnemann[1]

Na sociedade contemporânea, a mobilidade, impulsionada pela massificação de dispositivos móveis, transformou a forma como interagimos, comunicamos e nos relacionamos.

Os *smartphones* destacam-se como um dos dispositivos pessoais mais utilizados para navegar na *Internet*, partilhar ficheiros, escrever mensagens de texto, efetuar chamadas de voz e vídeo, e aceder a contas de *email*. Nestes dispositivos armazenamos grandes e variadas quantidades de informação, desde os nossos dados pessoais a dados empresariais, assim como efetuamos inúmeras atividades, desde acedermos a redes sociais e a contas bancárias, fotografarmos e filmarmos, efetuarmos compras e pagamentos, entre uma multiplicidade de outras tarefas [6].

Por necessidade ou conveniência também é usual a partilha do *smartphone* para efetuar chamadas telefónicas, enviar mensagens de texto, jogar, navegar na *Internet*, ou partilhar conteúdos [3, 51].

Hoje em dia, a utilização de *smartphones* cada vez mais inovadores e o modo como articulamos e integramos a nossa vida real com a nossa vida digital expõe-nos a novos riscos e ameaças. Garantir a segurança e a privacidade na utilização destes dispositivos foram as principais motivações que nos conduziram ao desenvolvimento desta dissertação.

[1] Professor e diretor do NetLab, DIGHUMLAB – Dinamarca.

1.1 Motivação

Os *smartphones* estão presentes de forma ubíqua no nosso dia a dia, armazenando um grande volume de informações pessoais – que podem incluir dados sensíveis, privados e confidenciais – e informações empresariais, a que podemos aceder em qualquer lado e em qualquer altura. No entanto, estes sistemas não têm sido concebidos segundo uma lógica de segurança. A primazia do seu desenho está na facilidade de utilização, relegando a segurança e a privacidade para um plano secundário. Dessa forma, estes dispositivos são vulneráveis a intrusões físicas, perpetradas por atacantes com acesso físico ao dispositivo, que podem comprometer a confidencialidade, integridade e disponibilidade da informação [36].

Os principais mecanismos de segurança disponíveis nos *smartphones* são os métodos de autenticação baseados no conhecimento (através de um PIN – número de identificação pessoal, de um padrão de desbloqueio *Android* ou de uma *password*) e aqueles baseados nas características biométricas (tais como o reconhecimento facial, da voz ou da impressão digital). Contudo, estes métodos não previnem o acesso não autorizado aos dados sensíveis por pessoas socialmente próximas do utilizador, como familiares, amigos ou colegas de trabalho [36, 40]. De facto, uma em cada cinco pessoas admitiu, em estudos recentes, ter acedido ao *smartphone* de outra pessoa sem autorização, o que demonstra a ineficácia destes métodos [36, 40].

Apesar de cientes dos dados sensíveis que os dispositivos móveis armazenam, os utilizadores consideram, de uma maneira geral, que os métodos de autenticação existentes não só exigem esforço e atenção, como também são complexos, morosos e aborrecidos de utilizar [25]. Por estas razões, muitos optam por não os utilizar [19, 25]. Assim, ao invés de protegerem a sua informação, optam pela usabilidade do *smartphone* [19], tornando essa informação vulnerável a intrusões.

No entanto, a utilização de métodos de autenticação também não resolve todos os problemas. De facto, os métodos de autenticação baseados no conhecimento são vulneráveis a ataques de observação, tais como o de *shoulder surfing* e o de *smudge*, facilmente realizados por pessoas socialmente próximas, permitindo ultrapassar as barreiras de segurança impostas. Nos ataques de *shoulder surfing*, o atacante observa a interação do utilizador com o dispositivo para, deste modo, obter o método de autenticação, enquanto nos ataques de *smudge* o atacante obtém esta informação através das dedadas deixadas no ecrã pelo utilizador [6, 19, 42].

A maioria dos utilizadores divide-se entre as preocupações com a privacidade e o desejo de partilhar o seu *smartphone* [34]. Embora afirmem que, normalmente, partilham os dispositivos com pessoas em quem confiam, receiam, por outro lado, que as pessoas

com quem o partilham acedam à sua informação pessoal, privada e confidencial [30, 34, 51]. Neste tipo de ataque concreto – intrusão realizada por alguém socialmente próximo – independentemente da supervisão efetuada, a barreira de autenticação é sempre ultrapassada e não existem quaisquer mecanismos de segurança complementares. Além disso, os utilizadores consideram que atitudes de vigilância ou de recusa de partilha podem comprometer as suas relações pessoais.

O desafio a que nos propusemos – explorar soluções para as limitações dos métodos de autenticação existentes que forneçam um novo leque de mecanismos de segurança adicionais que permitam controlar o acesso indevido e que, simultaneamente, possibilitem a partilha *segura* de dispositivos móveis pessoais – conduziu-nos ao desenvolvimento de um sistema de deteção e resposta a intrusões físicas para *smartphones*.

1.2 Objetivos

Os propósitos traçados, para esta dissertação, centram-se nos desafios assinalados na secção anterior. Assim, foram estabelecidos os seguintes objetivos:

1. **Conceber** um sistema de deteção e resposta a intrusões físicas para *smartphones*, facilmente configurável, acessível a utilizadores comuns, e que não comprometa a usabilidade dos dispositivos;
2. **Implementar** mecanismos que possibilitem a partilha segura, simples e espontânea do *smartphone*;
3. **Avaliar** a qualidade do sistema, através de um estudo de grupos de foco e da aplicação de testes de usabilidade.

1.3 Abordagem Metodológica

A abordagem metodológica adotada neste estudo foi objeto de particular atenção, tendo em conta a sua importância para os resultados a atingir. Deste modo, numa primeira fase, procedeu-se ao estudo do estado da arte relacionado com o tema proposto, incluindo a recolha e análise de diversos trabalhos, dos problemas levantados, das lacunas e das soluções existentes.

Seguidamente, e de modo a atingir os objetivos delineados, iniciou-se a fase de conceção do sistema de deteção e resposta a intrusões físicas. Esta fase consistiu na definição de um conjunto de cenários ilustrativos de situações e contextos (cenários do problema) e propostas de solução, a partir dos quais o desenho do sistema foi adquirindo consistência. Em particular, os resultados desta fase levaram-nos a optar por utilizar, como dispositivo auxiliar para deteção e resposta, um *smartwatch*. A motivação para esta escolha foi

o facto de este dispositivo, contrariamente ao *smartphone*, estar em contacto direto com o utilizador, normalmente no seu pulso, e permitir a interação com o *smartphone*. Assim, o *smartwatch* surgiu como uma solução interessante por permitir, através das tecnologias *Bluetooth* ou *Wi-Fi*, o controlo remoto das ações desencadeadas no *smartphone*.

Relativamente à implementação, o sistema foi concebido para *smartphones* com sistema operativo *Android* e *smartwatches* com sistema operativo *Android Wear*. Este sistema operativo continua a dominar o mercado de vendas dos *smartphones* relativamente aos seus concorrentes (*iOS* e *Windows Phone*), razão pela qual considerámos uma vantagem a sua adoção neste estudo [15].

Numa fase posterior, procedeu-se à avaliação da qualidade do sistema desenvolvido. Primeiro, com a realização de três sessões de grupos de foco presenciais para, através de uma discussão informal com os participantes, identificarmos os métodos de segurança adotados, compreendermos as motivações e os receios com a partilha dos dispositivos móveis pessoais e ainda obtermos informações de caráter qualitativo relativamente ao sistema apresentado. Além disso, permitiu-nos recolher propostas de melhoria do sistema. A análise dos resultados obtidos conduziu-nos a uma reflexão aprofundada acerca das sugestões que considerámos mais pertinentes e levou-nos também a reestruturar algumas das funcionalidades do sistema desenvolvido.

Após a implementação das propostas de melhoria (e consequente reestruturação da aplicação) concluímos esta fase com a avaliação da usabilidade do sistema.

A realização de dez sessões com testes, a aplicação da escala de usabilidade (SUS) e as entrevistas permitiram-nos, através da interação dos participantes com o sistema, determinar a sua eficácia e eficiência e a satisfação dos potenciais utilizadores da aplicação, assim como a deteção de problemas e a recolha de sugestões.

1.4 Contribuições

As principais contribuições desta dissertação são:

1. O estudo das limitações dos métodos de autenticação existentes, das suas vulnerabilidades e da problemática das intrusões físicas nos *smartphones*;
2. A conceção e implementação de um sistema (disponível *online*[2]) que permita detetar e responder a intrusões físicas em *smartphones*, acessível a utilizadores comuns;
3. A avaliação do sistema através de grupos de foco e de testes de usabilidade.

[2] https://github.com/40329tiagosantos?tab=repositories

1.5 Estrutura do Documento

Este documento está estruturado em seis capítulos e inclui um conjunto de apêndices:

1. **Capítulo 1 – Introdução:** neste capítulo efetuou-se o levantamento dos principais problemas e das motivações que conduziram ao estudo apresentado. Procedeu-se também à definição dos objetivos a atingir, à abordagem metodológica adotada para o seu desenvolvimento e elencaram-se as principais contribuições desta dissertação. A conclusão do capítulo incidiu sobre o enquadramento institucional que norteou esta dissertação;
2. **Capítulo 2 – Trabalho Relacionado:** visa dar conta do estado da arte relativamente ao tema que é objeto desta dissertação;
3. **Capítulo 3 – Desenho do Sistema:** contempla a descrição dos cenários do problema, o modelo adversarial considerado, a abordagem e as soluções que propomos. São, ainda, enunciados os requisitos funcionais e não-funcionais do sistema proposto;
4. **Capítulo 4 – Implementação:** são apresentados os detalhes de implementação e a arquitetura do sistema desenvolvido;
5. **Capítulo 5 – Avaliação:** engloba os métodos e as conclusões dos resultados da avaliação do sistema, bem como as implicações e as propostas de solução implementadas;
6. **Capítulo 6 – Conclusões:** neste capítulo são apresentadas as principais conclusões do trabalho realizado, as suas limitações e ainda sugestões de melhoria e de trabalho futuro;
7. **Apêndices:** inclui os guiões e os formulários utilizados na fase de avaliação do sistema.

1.6 Enquadramento Institucional

O trabalho desenvolvido no âmbito desta dissertação decorreu na unidade de investigação científica Laboratório de Sistemas Informáticos de Grande Escala, Departamento de Informática (DI-LaSIGE), da Faculdade de Ciências da Universidade de Lisboa.

O trabalho foi efetuado sob a orientação do Professor Doutor Tiago João Vieira Guerreiro e coorientação do Professor Doutor Fernando Manuel Valente Ramos.

Capítulo 2

Trabalho Relacionado

Neste capítulo apresenta-se o estado da arte, através da abordagem de diversos estudos, resultados e soluções existentes contra intrusões físicas em dispositivos móveis pessoais, que comprometem a segurança da informação e a privacidade dos utilizadores.

Iniciamos o capítulo com breves considerações sobre os dados que os dispositivos móveis pessoais armazenam e os riscos e as ameaças a que esses dados poderão estar sujeitos. De seguida, são apresentados os métodos de autenticação existentes, com foco nas suas limitações, assim como as razões pelas quais não são adotados e ainda algumas das vulnerabilidades a que estão sujeitos. Serão igualmente analisadas as problemáticas subjacentes à partilha de um dispositivo móvel, assim como as propostas existentes. Concluímos este capítulo com a apreciação crítica que, com base no enquadramento dos estudos efetuados, nos conduziu ao desenvolvimento da solução proposta nesta dissertação.

2.1 Smartphones e Dados Sensíveis

Os dispositivos móveis pessoais, em particular os *smartphones*, armazenam cada vez mais informações de âmbito pessoal e empresarial que podem conter dados sensíveis – mensagens de texto, *emails*, contactos, registo de chamadas, fotografias, *passwords*, entre outros [14] – que representam informações privadas ou confidenciais [40], que os utilizadores querem proteger de forma adequada contra o acesso indevido [12]. Para protegerem esses dados, os dispositivos móveis disponibilizam mecanismos de proteção que requerem a autenticação do utilizador.

Os *smartphones* tornaram-se ubíquos e a sua utilização é frequente e constante. Porém, esta conveniência acarreta consigo um conjunto de riscos consideráveis para a segurança da informação e para a privacidade do utilizador. Se, por um lado, os métodos de autenticação visam proteger o acesso não autorizado de terceiros aos dados armazenados nos dispositivos (segurança), por outro, se o esforço e o tempo requeridos com o processo

de autenticação comprometerem a sua usabilidade, o utilizador tenderá a não os adotar, colocando em risco a segurança da informação [26].

2.2 Intrusões em Dispositivos Móveis Pessoais

A massificação dos *smartphones* originou um crescimento de adversários que, através do acesso indevido aos dados sensíveis dos dispositivos (intrusão), ameaçam a privacidade dos utilizadores.

Uma intrusão pode ser definida como qualquer conjunto de ações que têm como intuito comprometer a confidencialidade, a disponibilidade ou a integridade de um recurso [27]. A segurança dos dados está em risco quando as informações sensíveis são acedidas por terceiros – confidencialidade, quando é impedido o acesso do utilizador à informação – disponibilidade, ou quando ocorre a modificação e/ou eliminação não autorizada de dados – integridade [39, 49].

A maioria das pessoas, quando tem oportunidade de utilizar um *smartphone* alheio, tenta aceder a dados sensíveis, tais como aplicações de redes sociais, fotografias, *passwords*, *emails* e aplicações bancárias [40, 53]. Estudos recentes demonstram que esta tendência para "bisbilhotar" (*snooping*) e/ou utilizar dispositivos alheios sem autorização poderá atingir níveis preocupantes [35, 36, 40, 53].

A *Symantec*, numa experiência realizada em 5 cidades americanas, "perdeu" intencionalmente 50 *smartphones* sem qualquer método de autenticação, tendo verificado que 96% das pessoas que os encontraram examinaram os dados sensíveis [53].

Os utilizadores enfrentam, no dia a dia, ameaças reais à sua privacidade, que incluem o acesso não autorizado aos dados e funcionalidades dos *smartphones* por parte de pessoas socialmente próximas (familiares, amigos e/ou colegas de trabalho). Os resultados obtidos num estudo empírico [40] revelaram que 12% dos participantes referiram terem tido uma experiência negativa de acesso indevido aos seus *smartphones* por parte de pessoas que lhes são próximas, enquanto 9% reconheceram que foram "atacantes". Estes resultados sugerem que, para os vários utilizadores, as pessoas próximas são motivo de preocupação porque representam uma ameaça séria para a sua privacidade.

Esta tendência também foi analisada no estudo realizado por Marques *et al.* [35], através da aplicação de duas técnicas de inquirição distintas: na primeira, realizada face-a-face, apenas 10% dos participantes admitiram ter acedido aos dados sensíveis num dispositivo móvel de uma pessoa socialmente próxima sem o seu consentimento e/ou conhecimento; na segunda, realizada de forma anónima, o número de respostas afirmativas alcançou um valor consideravelmente superior – 60% – o que indicia que, embora não seja admitido abertamente, a oportunidade pode ser motivadora deste tipo de comportamento.

A utilização intensiva e o conhecimento cada vez mais profundo dos conteúdos sensíveis que estes dispositivos poderão conter tornam, por um lado, os utilizadores mais conscientes do que têm a perder ou a ganhar num eventual ataque aos seus dispositivos e, por outro lado, poderão ser um fator aliciante para terceiros "espiarem" os dispositivos alheios. Num outro estudo de larga escala realizado por Marques *et al.* [36] concluiu-se que uma em cada cinco pessoas já acedeu ao *smartphone* de outra pessoa sem o seu consentimento. Contudo, e apesar de a maioria (52%) destes ataques estar associada à camada mais jovem da população (com idades compreendidas entre os 18 e os 24 anos), é considerado, neste estudo, que o uso generalizado de *smartphones* poderá esbater esta relação, aumentar a motivação e a tendência das pessoas comuns (de outras faixas etárias) os efetuarem [36].

As conclusões dos estudos anteriores revelam que "bisbilhotar" os dados sensíveis no *smartphone* de uma pessoa socialmente próxima, sem deixar pistas, deve ser relativamente fácil uma vez que é uma prática tão comum.

2.3 Métodos de Autenticação

Com o intuito de garantir a segurança e impedir o acesso indevido aos *smartphones* é indispensável a autenticação do utilizador. A autenticação consiste num processo de identificação para determinar que a pessoa que acede ao sistema tem permissão para o fazer (pessoa legítima) [38].

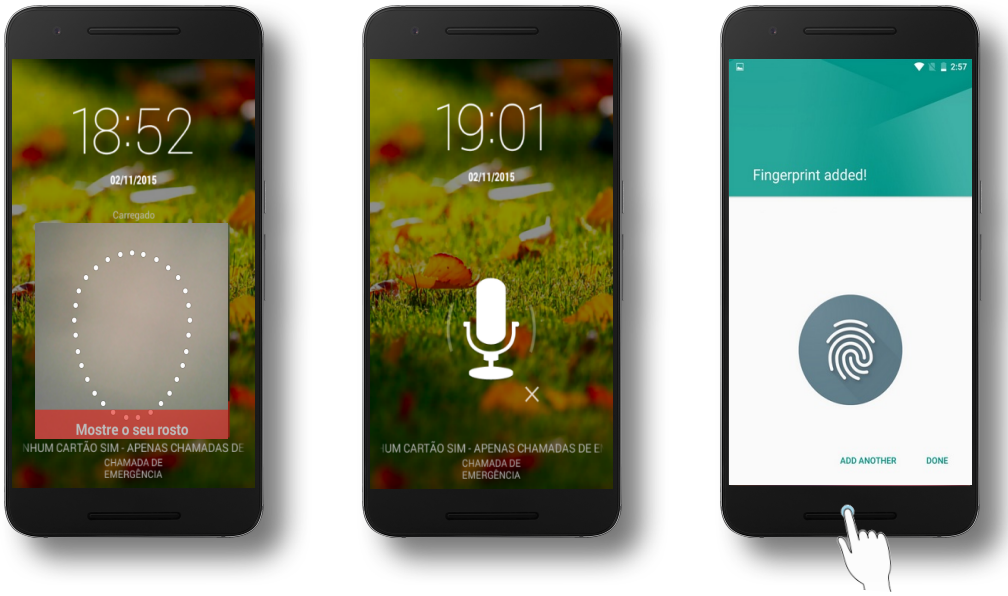
Os principais métodos de autenticação disponibilizados nos *smartphones* são os baseados [26]:

- No conhecimento de um "segredo" ("algo que sei") como: um PIN – número de identificação pessoal (Figura 2.1a), um padrão de desbloqueio *Android* (Figura 2.1b) ou uma *password* (Figura 2.1c);

(a) PIN. (b) Padrão de desbloqueio *Android*. (c) *Password*.

Figura 2.1: Métodos de autenticação baseados no conhecimento.

- Nas características biométricas do dono do dispositivo ("algo que sou") (Figura 2.2), como: o reconhecimento facial (Figura 2.2a), de voz (Figura 2.2b) ou de impressão digital (Figura 2.2c);



(a) Reconhecimento facial.

(b) Reconhecimento da voz.

(c) Reconhecimento da impressão digital.[3]

Figura 2.2: Métodos de autenticação biométricos.

- Em *tokens* ("algo que o utilizador tem"), ou seja, a posse de um dispositivo físico fidedigno através do qual se realiza a autenticação (tipicamente, um dispositivo com ligação *Bluetooth* ao *smartphone*).

Um método de autenticação eficaz deverá reunir as seguintes características [13]:

- Minimizar o esforço do utilizador (por exemplo, não exigindo que o PIN seja inserido sempre que se queira utilizar o *smartphone*);
- Estar menos dependente do conhecimento de um "segredo" como, por exemplo, uma *password*;
- Resistir a ataques de observação (*shoulder surfing* e *smudge*).

[3] Fonte: http://beebom.redkapmedia.netdna-cdn.com/wp-content/uploads/2016/03/Android-fingerprint-added.jpg [Online; 12-Dezembro-2015].

2.3.1 Motivações dos Utilizadores (Segurança vs. Usabilidade)

Proteger os conteúdos sensíveis, preservar a privacidade e impedir o acesso de terceiros são algumas das razões apontadas pelos utilizadores para adotarem métodos de autenticação.

No estudo efetuado por Egelman *et al.* [19] ficou patente que as principais preocupações dos participantes se prendiam com o acesso não autorizado por estranhos (pessoas não socialmente próximas) – 55% – e em impedir a sua utilização por parte de amigos e familiares – 23%. Outro estudo que reforça esta tendência foi conduzido por Harbach *et al.* [25], em que se concluiu que cerca de 43% dos participantes utilizavam métodos de autenticação, tendo referido como principais motivações para o seu uso o controlo do acesso ao *smartphone*, a proteção da informação, a perda, o roubo ou a proteção contra eventuais atacantes.

Apesar de os equipamentos atualmente existentes no mercado disponibilizarem diferentes mecanismos de segurança, os utilizadores optam por métodos de autenticação cujo esforço e tempo gastos no processo de autenticação sejam reduzidos e permitam o acesso rápido aos conteúdos do *smartphone.* Ou seja, optam pela usabilidade, relegando a segurança e a proteção dos seus dados sensíveis para segundo plano [25].

De facto, se cada vez que um utilizador aceder a um sistema demorar cerca de 10 segundos a autenticar-se e se o fizer, em média, 50 vezes por dia [19, 26] é provável que considere o tempo gasto como excessivo. No estudo de Egelman *et al.* [19] os participantes consideraram que aumentar o tempo de inatividade, necessário para bloquear o *smartphone* automaticamente, permitiria reduzir o número de autenticações e, consequentemente, melhorar a usabilidade do dispositivo, o que demonstra que o tempo é um fator relevante no processo de autenticação.

Assim, os utilizadores tendem a selecionar métodos que permitam a interação frequente e constante com o dispositivo, não comprometendo a usabilidade do *smartphone*, optando por PIN's, *passwords* e padrões de desbloqueio *Android* memorizáveis, simples (normalmente PIN's com 4 dígitos e *passwords* fracas, tais como "1234") [11] e, consequentemente, poucos seguros e fáceis de adivinhar [19, 26, 44].

Acresce ainda que estes métodos são potencialmente vulneráveis a ataques de *shoulder surfing* que, através da observação direta ou indireta, "descobrem o segredo", e de ataques *smudge* que permitem, através da análise das dedadas deixadas no ecrã, identificar o "segredo" [54].

Os métodos de autenticação biométricos (embora recentes e ainda não disponíveis

no mercado para uma grande maioria dos equipamentos) surgem como uma boa alternativa aos métodos anteriores, na medida em que não exigem memorização, não podem ser adivinhados e permitem o acesso rápido ao sistema. No entanto, também apresentam limitações. Alguns utilizadores consideram-nos um pouco embaraçosos e intrusivos (em termos de utilização abusiva de identidade, reconhecimento comportamental, quebra de anonimato, entre outros) [1, 9, 14, 43]. Além disso podem também sofrer interferências relacionadas com o ambiente (falta de luminosidade, ruído, poeiras, entre outras) e com o próprio utilizador (rouquidão, transpiração, alterações fisionómicas, entre outras).

Embora conscientes dos dados sensíveis que os dispositivos armazenam, alguns utilizadores optam por não usar métodos de autenticação.

Estudos recentes analisaram as motivações para a não adoção de qualquer método. No estudo de Egelman *et al.* [19], 42% dos inquiridos não utilizavam métodos de autenticação. A principal razão mencionada foi o facto de serem demasiado aborrecidos. A inconveniência (onde se incluiu a perda de tempo e o uso frequente do *smartphone*) e a ausência de ameaças (considerando como factos não conterem dados sensíveis e manterem o *smartphone* fisicamente seguro, por exemplo no bolso) foram também razões apontadas por 57% dos participantes, no estudo de Harbach *et al.* [25], para não os adotarem.

Num outro estudo [39], a maioria dos participantes considerou, ainda, que os PIN's e as *passwords* eram inadequados porque impediam o acesso imediato às aplicações e aos dados que não consideravam sensíveis, tais como jogos, aplicações de meteorologia ou navegadores de *Internet*. Os participantes também referiram ser inapropriado ter de inserir um código sempre que pretendiam utilizar o *smartphone* [39]. Outros, apesar de desejarem que o seu dispositivo estivesse protegido, consideraram-nos desnecessários em contextos privados e seguros (casa, carro) [25].

Noutros casos, apesar de considerarem que possuíam dados sensíveis e terem anteriormente utilizado métodos de autenticação, os utilizadores deixaram de o fazer por questões de usabilidade, tais como o número excessivo de autenticações exigido, mesmo quando não pretendiam aceder a dados sensíveis [40].

2.3.2 Ataques de Observação

Conforme mencionado na Secção 2.2, a oportunidade de utilização de dispositivos móveis alheios, sem autorização, tende a atingir níveis preocupantes [35]. Acresce, ainda, que os métodos de autenticação existentes são pouco eficazes nas situações em que "alguém" tem a oportunidade de observar e/ou analisar as dedadas deixadas no ecrã com o intuito de obter o método de autenticação para aceder aos dados sensíveis do utilizador.

Os métodos de autenticação comumente adotados são vulneráveis a ataques de *shoulder surfing* (Figura 2.3a) [44]. Neste caso, através da observação direta ou da utilização de espelhos ou câmaras ocultas, uma pessoa observa intencionalmente o utilizador a inserir o método para posteriormente o reutilizar e obter acesso ao dispositivo e aos dados sensíveis [18, 42].

Em contexto social e organizacional cada autenticação poderá ser facilmente observada por pessoas socialmente próximas do utilizador. Este, normalmente, negligencia a adoção de práticas de segurança simples que possam prevenir estes ataques, como por exemplo tapar o ecrã enquanto insere o método de autenticação, por considerar que esta sua atitude poderá ser conotada como uma atitude de desconfiança [18]. Torna-se, assim, um alvo particularmente vulnerável a este tipo de ataques – *shoulder surfing* – de ameaça à privacidade do utilizador.

Embora a autenticação seja um passo crucial para a segurança, quando o utilizador insere o método de autenticação no ecrã tátil [2], deixa resíduos de gordura que possibilitam, através da sua análise, deduzir o "segredo" com as pistas deixadas pelas dedadas na superfície do ecrã (ataque de *smudge*) (Figura 2.3b). Estes vestígios são persistentes no tempo, difíceis de ocultar ou apagar. Mesmo limpando o ecrã, são facilmente identificados com recurso a equipamentos acessíveis a qualquer pessoa (câmaras e computadores) [6].

(a) Ataque de *shoulder surfing*.[4] (b) Ataque de *smudge*.[5]

Figura 2.3: Ataques de observação.

Apesar dos métodos de autenticação garantirem a segurança e serem uma barreira contra o acesso não autorizado à informação, verificamos, contudo, que a sua eficácia nem sempre está assegurada [13]. Primeiro, porque o utilizador tenderá a não os adotar se o esforço despendido com os processos de autenticação for elevado (segurança *vs.*

[4] Fonte: http://i2.cdn.turner.com/cnnnext/dam/assets/150521150533-snooping-large-169.jpg [Online; 10-Novembro-2015].

[5] Fonte: https://dlcdnimgs.asus.com/websites/global/products/3HzHuNmdcAgeMhJ1/img/design/memopad-anti-finger.png [Online; 19-Novembro-2015].

usabilidade); segundo, porque são vulneráveis a ataques simples de observação facilmente perpetrados por pessoas socialmente próximas; finalmente, porque não impedem o acesso aos conteúdos quando o dispositivo é partilhado.

2.4 Partilha de Dispositivos Móveis Pessoais

Os utilizadores partilham os seus dispositivos, por diversas razões, normalmente com pessoas em quem confiam. Contudo, não controlam o acesso não autorizado a determinados dados e funcionalidades, pelo que muitos receiam que a sua privacidade seja invadida. De facto, os métodos de autenticação existentes, assentes na abordagem *all-or-nothing*, não permitem que o utilizador controle e limite esse acesso e, consequentemente, não possibilitam a partilha *segura* do *smartphone* [23].

As principais motivações, apontadas no estudo efetuado por Velho *et al.* [51], para partilhar o dispositivo com outra pessoa relacionavam-se com tarefas específicas e estavam limitadas a certas funcionalidades, tais como fazer ou receber chamadas telefónicas, enviar mensagens, visualizar fotografias, jogar, entre outras. Cerca de 80% dos participantes, neste estudo, afirmaram que apenas partilhavam o *smartphone* com pessoas em quem confiavam. No entanto, adotavam algumas medidas preventivas, tais como serem os próprios a segurar e/ou manusear o dispositivo, terminarem sessões de aplicações com dados sensíveis, abrirem previamente a aplicação a partilhar, manterem-se próximos e supervisionarem o que a outra pessoa fazia no *smartphone*.

Ainda em outro estudo [34], os autores concluíram que as atitudes, relativamente às preocupações com a partilha, se manifestavam de três formas distintas. Assim, 56% dos participantes não partilhavam o seu dipositivo; 86% supervisionavam o dispositivo e 60% vigiavam as atividades executadas pelo convidado; 54% revelaram que, antes de partilharem o seu dispositivo, apagavam ou alteravam o local de armazenamento dos seus dados privados, (des)ativavam certas funcionalidades e/ou abriam a aplicação desejada. Estes resultados são indicativos das preocupações que os utilizadores têm antes e durante o processo da partilha. Contudo, e independentemente das medidas de prevenção adotadas, a barreira de autenticação é sempre ultrapassada, não existindo qualquer mecanismo de segurança adicional.

As manifestações de preocupação, referidas anteriormente, poderão ter implicações sociais. A recusa e a adoção de medidas explícitas de vigilância denotam atitudes de desconfiança e de desconforto que podem comprometer as relações interpessoais. Assim, o utilizador poder-se-á sentir forçado a assumir uma atitude de confiança total e ficar exposto a diversas ameaças [19].

As preocupações de partilha dependem ainda do nível de confiança entre o dono e o

convidado. A confiança é evidenciada pelas medidas adotadas pelo dono do dispositivo. Se esta for elevada, o dono poderá deixar o convidado sozinho com o seu *smartphone*, ou, pelo contrário, ficar próximo para poder observar a sua interação e intervir se necessário [23].

Num estudo recente [52] os participantes concordaram que o grupo de pessoas em quem mais confiavam incluía os pais e os amigos próximos. No entanto, discordaram quanto aos dados que aceitariam partilhar com esse grupo, o que sugere que a partilha de dispositivos móveis pessoais não é apenas uma questão de confiança, mas também é influenciada pelos dados que irão ser partilhados com o convidado.

Os diversos estudos relacionados com esta temática reforçam que, apesar de as necessidades de privacidade serem subjetivas, os participantes expressaram uma preocupação maior com o acesso aos seus dados privados, tais como mensagens e fotografias, ou a outro tipo de informação pessoal, por parte de pessoas do seu círculo social (amigos, familiares e colegas). Contudo, consideraram como pouco relevante que pessoas completamente estranhas o fizessem, receando apenas que estas, eventualmente, pudessem roubar o dispositivo [23, 30, 39]. Estes resultados sugerem que as pessoas próximas são também consideradas uma ameaça nas situações de partilha do dispositivo.

As preocupações de partilha não estão somente relacionadas com questões de privacidade, mas também com aspetos de segurança. Os utilizadores receiam que os outros, intencionalmente ou não, comprometam a segurança da informação alterando e/ou eliminando dados importantes, configurações, efetuem tarefas abusivas, como por exemplo escreverem e enviarem mensagens de texto, acedam a redes sociais, entre outras situações [23, 30, 52].

Em suma, os utilizadores dividem-se entre preocupações com a privacidade e o desejo de partilharem os seus *smartphones*. Consequentemente, consideram que se possuíssem um modo inconspícuo que permitisse controlar e limitar os dados e aplicações que deveriam estar (in)disponíveis durante e com quem a partilha é efetuada, isso torná-la-ia por um lado mais espontânea e por outro mais segura [34]. No entanto, os métodos de autenticação existentes não respondem a estas necessidades.

2.4.1 Partilha de Dispositivos Móveis Pessoais – Soluções Existentes

As soluções *xShare* [34] e *FaceProfiles* [24] visam solucionar os problemas da partilha de *smartphones*, colocando o dispositivo, no momento em que é partilhado, num modo restrito.

O *xShare* é um *software* que permite ao dono do *smartphone*, através da configuração de uma política de acessos, definir os ficheiros, aplicações, pastas, recursos e definições

que pretende partilhar. Quando o dispositivo móvel é partilhado, o perfil definido é ativado explicitamente pelo utilizador. Consequentemente, o *xShare* não fornece qualquer proteção no caso de a partilha ocorrer de forma não intencional (e.g., numa situação em que "alguém" se apodera do *smartphone* enquanto o dono o utiliza). Além disso, a ativação do perfil poderá ser observada pela pessoa com quem o dispositivo é partilhado, podendo causar desconforto e sentimentos de desconfiança.

Hang *et al.* propuseram um conceito chamado *FaceProfiles* [24]. Este permite, ao dono do *smartphone*, definir perfis através da gestão de permissões para cada utilizador ou grupo de utilizadores (e.g., família, amigos ou colegas de trabalho). Os perfis são ativados, de forma inconspícua, através do reconhecimento facial dos utilizadores. As fotografias necessárias para o reconhecimento facial são recolhidas a partir dos contactos telefónicos ou de redes sociais como, por exemplo, o *Facebook*. A gestão de permissões permite ao dono do dispositivo definir as funcionalidades que cada aplicação deverá disponibilizar, no caso de partilhar o seu dispositivo. Os autores consideram que o melhor conceito de privacidade apenas será bem-sucedido se o esforço entre o processo de configuração e os benefícios for aceitável. No entanto, o método apresentado é demasiado complexo, não sendo apropriado para utilizadores "preguiçosos".

2.5 Sistemas de Deteção e Respostas a Intrusões

Os mecanismos de controlo e segurança existentes para *smartphones* têm-se focado essencialmente no desenvolvimento de métodos de autenticação, de antivírus e de *firewalls*, assim como na salvaguarda de dados na *cloud*. Contudo, o incremento das funcionalidades de conetividade dos *smartphones*, proporcionadas por múltiplas ligações de redes e canais de comunicação cada vez mais complexos, exigem novos sistemas de controlo e segurança mais sofisticados, tais como os sistemas de deteção de intrusões, que acompanhem esta evolução e que também respondam às ameaças perpetradas por adversários socialmente próximos da vítima [32, 33].

Conforme já mencionado anteriormente, uma intrusão é um conjunto de ações que representam um incidente de segurança que afeta um sistema ou um recurso [48] e os sistemas de deteção e resposta a intrusões (*Intrusion Detection and Response Systems* – IDRSs) são uma ferramenta (*software* ou *appliance*) composta por três componentes principais: sensores – responsáveis pela recolha de dados; módulo de deteção – que monitoriza, analisa os dados recolhidos e deteta esses incidentes, isto é, as atividades maliciosas ocorridas, neste caso concreto, no *smartphone* [38]; e o componente de resposta que desencadeia mecanismos de segurança [5, 45].

Os sistemas de deteção de intrusões dividem-se, geralmente, em duas categorias,

uma baseada na rede (*Network based* IDS – NIDS) e a outra baseada na máquina-hóspede (*Host based* IDS – HIDS). A primeira monitoriza o tráfego da rede para detetar se os eventos estão ou não dentro de padrões pré-determinados, enquanto a segunda é executada no próprio sistema que protege, ou seja, monitoriza e analisa os eventos ocorridos no próprio dispositivo onde atua, detetando eventuais tentativas de intrusão [46, 50].

Consideramos que os sistemas de deteção baseados na rede (NIDS), por estarem mais orientados para a monitorização de ameaças vindas do exterior, não se enquadram no âmbito do nosso trabalho, afastando-se do nosso objetivo pelo facto não terem em consideração os dados armazenados no dispositivo móvel (como ativos a proteger) nem os adversários fisicamente próximos [38].

Assim, iremos efetuar a abordagem dos sistemas de deteção de intrusões para *smartphones* com base na aproximação concetual dos sistemas baseados na máquina-hóspede (HIDS).

As técnicas de deteção de intrusões mais comuns dividem-se em duas categorias: a de deteção de assinaturas (ou baseada no conhecimento) – baseada nas regras e padrões que definem uma intrusão – verifica se a assinatura de uma determinada aplicação coincide, por exemplo, com uma de *malware* pré-definida. Por outro lado, a de deteção de anomalias (ou baseada no comportamento) – baseada num modelo ou padrão comportamental do utilizador ou de atividades consideradas normais (legítimas) – monitoriza os eventos e deteta os desvios à normalidade [22, 31].

Algumas desvantagens poderão ser apontadas às técnicas descritas. As primeiras não detetam outras intrusões para além das que estão definidas nas regras e padrões pré-estabelecidos. As segundas emitem um elevado número de falsos alarmes devido à grande diversidade de atividades, de mobilidade e/ou de perfis de comportamentos dos utilizadores de *smartphones*, o que dificulta a implementação e a eficácia desta técnica [50].

Os sistemas de deteção devem integrar sistemas de resposta às tentativas de intrusões para mitigar os seus efeitos – sistema de deteção e resposta a intrusões. As respostas são, tipicamente, agrupadas em ativas e passivas.

As respostas ativas são acionadas automaticamente pelo sistema, ou pelo utilizador/administrador. Estas respostas incluem contramedidas tais como bloquear funções, terminar uma sessão, cancelar ligações, simular uma falha, entre outras. As respostas passivas, por seu lado, reportam informações da ocorrência do evento (alarmes e notificações) e aguardam a resposta do utilizador ou administrador do sistema. Este processo é impercetível para o atacante e/ou utilizador porque apenas monitoriza os eventos, não interferindo nos mesmos [4, 41].

Contudo, a eficácia das respostas apresenta algumas limitações. As respostas ativas estão associadas a um determinado tipo de ataque específico. Portanto, se a intrusão não tiver uma solução configurada o sistema poderá ficar sem resposta, o que exige que o modelo de medidas a aplicar tenha de ser permanentemente atualizado [4, 7]. Nas respostas passivas, o sistema está dependente da reação humana, originando um intervalo de tempo entre a deteção da intrusão e o início da reação, durante o qual o intruso pode continuar a operar. A Figura 2.4 apresenta a visão geral do processo de prevenção, deteção e resposta a intrusões em *smartphones*.

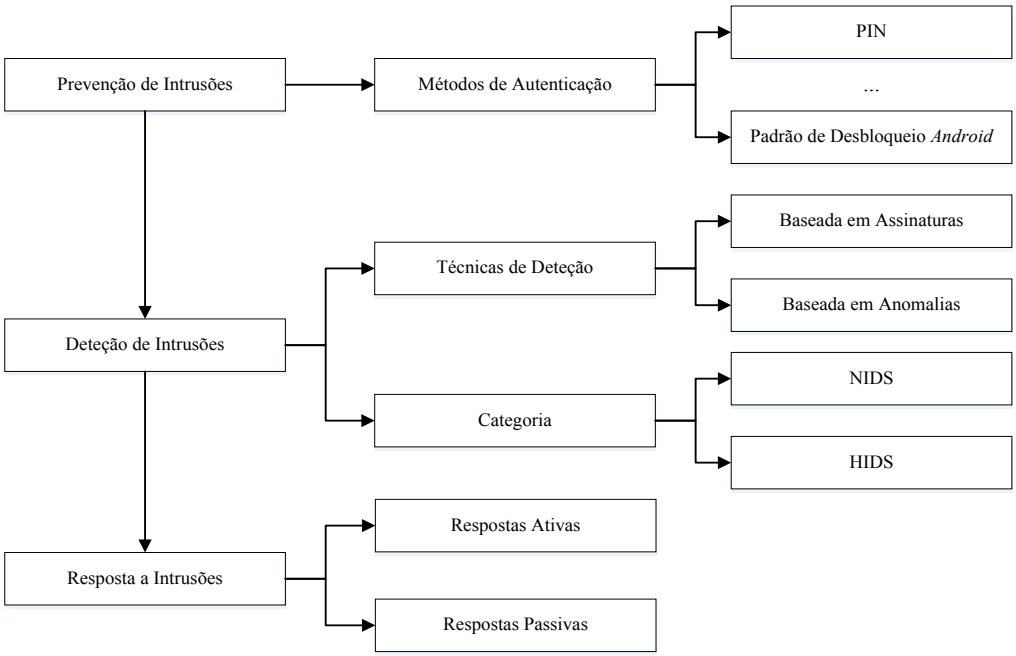


Figura 2.4: Visão geral do processo de prevenção, deteção e resposta a intrusões.

2.5.1 Sistemas de Deteção e Resposta a Intrusões – Soluções Existentes

Diferentes tipos de mecanismos de sistemas de deteção e resposta de intrusões têm vindo a ser desenvolvidos ao longo dos últimos anos. Neste contexto, iremos analisar alguns sistemas propostos para deteção de intrusões para *smartphones*, baseados na *máquina-hóspede* (HIDS). Serão destacadas as suas principais características, métodos de análise e de deteção e tipos de respostas.

O sistema *Andromaly* [47], proposto por Shabtai *et al.*, baseia-se na técnica de deteção de anomalias em plataformas com o sistema operativo *Android*. O *Andromaly* é uma ferramenta – *framework* – instalada no próprio dispositivo, concebida para detetar *malware*. Esta aplicação monitoriza continuamente os eventos e funcionalidades do *smartphone* classificando-os, com a utilização de técnicas de *Machine Learning*, em nor-

mais (benignos) ou anormais (maliciosos). O processo de deteção de *malware* deste sistema, consiste na recolha, monitorização e análise, em tempo real, de dados relativos a diferentes métricas do sistema (como a utilização da CPU, a quantidade de dados enviados através de *Wi-Fi*, número de processos ativos, o consumo da bateria, entre outras). Os dados, depois de analisados, são avaliados e é apresentado um alerta ao utilizador sempre que uma aplicação é maliciosa. Adicionalmente, são apresentadas opções de resposta, tais como, remover a aplicação maliciosa, parar a sua execução ou bloquear o dispositivo.

Apesar do *Andromaly* ser uma ferramenta eficaz na deteção de *malware* (taxa de sucesso de 94% nos testes realizados), apresenta limitações uma vez que não considera os adversários com acesso físico ao dispositivo.

O sistema proposto por Velho *et al.* [51], tal como o *Andromaly*, baseia-se na técnica de deteção de anomalias em *smartphones* com o sistema operativo *Android*. No entanto, este sistema tem como objetivo detetar e responder a intrusões físicas, perpetradas por adversários com acesso físico ao dispositivo.

Este sistema autentica continuamente o utilizador, através do reconhecimento facial. No caso de ser detetada uma intrusão, é acionada uma resposta passiva, de forma inconspícua, que regista as ações e fotografa o intruso. As informações podem ser consultadas mais tarde pelo dono do dispositivo. No entanto, este sistema apresenta limitações: a eficácia do reconhecimento facial depende das condições de luminosidade e da qualidade da câmara do dispositivo, possibilitando a produção excessiva de falsos positivos comprometendo a sua adoção; não inclui respostas ativas que impeçam a progressão do ataque e, consequentemente, assegurem a segurança da informação armazenada no dispositivo e a privacidade do utilizador. Além destas limitações, o sistema apresenta problemas de usabilidade relacionados com a configuração.

2.6 Apreciação Crítica

A massificação dos *smartphones* originou um crescimento de adversários que, através do acesso indevido aos dispositivos, ameaçam a privacidade dos utilizadores.

Nos vários estudos realizados, tem-se concluído que as pessoas, quando têm oportunidade, tendem a "bisbilhotar" (*snooping*) e/ou utilizar os dispositivos alheios sem autorização [35, 53]. A crescente adoção destes dispositivos poderá aumentar a motivação e a capacidade de pessoas comuns para efetuarem ataques e explorarem diversas vulnerabilidades [20, 21, 36, 38].

Os principais mecanismos de segurança existentes são os métodos de autenticação. Os estudos empíricos efetuados nesta área dão a indicação de que se são percecionados

como pouco seguros e complexos, o utilizador tenderá a não os adotar (segurança *vs.* usabilidade). De facto, os métodos de autenticação, apesar de serem uma barreira contra o acesso indevido aos dispositivos móveis, não garantem, no entanto, uma segurança total, e apresentam sérias limitações. Destas, destacamos a vulnerabilidade a que estão sujeitos, no caso, por exemplo de ataques de observação, facilmente realizados por pessoas socialmente próximas e ainda o facto de não impedirem o acesso e o controlo dos conteúdos quando o dispositivo é partilhado.

Embora os utilizadores afirmem que só partilham o dispositivo com pessoas em quem confiam, receiam que os convidados acedam à sua informação pessoal, confidencial e privada. Independentemente das medidas de supervisão adotadas, a barreira de autenticação é sempre ultrapassada.

As propostas analisadas para a partilha dos dispositivos móveis baseiam-se em políticas de acesso e na gestão de permissões para utilizadores. No entanto, não permitem a partilha espontânea do dispositivo, não fornecem proteção em situações de partilha não autorizada, ou são demasiado complexas.

Os sistemas de deteção e de resposta a intrusões apresentados baseiam-se na deteção de assinaturas e de anomalias. No entanto, não consideram os adversários com acesso físico ao dispositivo, apresentam problemas relacionados com a usabilidade, geram um número de elevado de falsos positivos e não incluem respostas ativas que impeçam a progressão de um ataque.

Explorar soluções que mitiguem as lacunas apontadas foi o desafio a que nos propusemos. Com o sistema desenvolvido, pretendemos solucionar alguns dos problemas e falhas apresentadas, e propor um método de segurança acessível, versátil e facilmente adaptável às mais diversas situações do quotidiano e interesses do utilizador comum.

Capítulo 3

Desenho do Sistema

Como vimos anteriormente, os *smartphones* estão cada vez mais presentes na nossa vida pessoal, social e profissional. Atendendo ao grande volume de dados sensíveis que contêm [9, 23], torna-se essencial a sua proteção contra o acesso indevido, preservando a sua confidencialidade e privacidade. No entanto, a necessidade de estarmos sempre ligados, aceder à informação em qualquer lado e a todo o momento e a interação constante com o *smartphone*, a qual tipicamente exige processos de autenticação constantes, – tornou os dispositivos vulneráveis a intrusões físicas. Estas são, em particular, perpetradas por pessoas que nos estão próximas e que, de alguma forma, conseguem ter acesso físico ao dispositivo, criando a possibilidade de explorarem os nossos dados sensíveis.

Atualmente, os principais mecanismos de segurança são os métodos de autenticação. No entanto, vários estudos revelam que a maioria dos utilizadores opta pela usabilidade dos *smartphones* em detrimento da segurança dos seus dados [9, 14, 25]. Acresce ainda que os métodos de autenticação existentes são poucos eficazes nas situações em que o intruso que estamos a considerar, por ser uma pessoa socialmente próxima, possa facilmente observar a interação do utilizador com o *smartphone*.

Os utilizadores dividem-se entre preocupações com a privacidade e o desejo de partilharem os seus *smartphones*. Consideram, contudo, que medidas de vigilância explícitas denotam atitudes desconfiança que podem comprometer as relações sociais. O facto de poderem, de modo discreto, controlar e limitar os dados que deverão estar (in)disponíveis, possibilitaria por um lado a partilha mais espontânea e por outro mais segura.

Conforme referimos no capítulo anterior, as soluções de partilha analisadas não respondem às necessidades citadas, como também não impedem a partilha não autorizada. Os sistemas de deteção e resposta a intrusões não consideram, por um lado, os adversários socialmente próximos, comprometem a usabilidade e, por outro, apenas integram respostas passivas que não impedem a progressão da intrusão.

Assim, o nosso propósito foi o de conceber um sistema simples, fiável e seguro, de *deteção* e *resposta*, que permita eliminar o risco de intrusões físicas quando a barreira de autenticação é ultrapassada. Neste sistema, a deteção consiste na monitorização do sistema de modo a determinar quando ocorreu o incidente e quem foi o responsável pelo mesmo. E a resposta consiste num processo de respostas ativas e passivas que permitam eliminar o risco sem comprometer a usabilidade do dispositivo.

Efetuado o levantamento dos diferentes problemas, o desenho da nossa solução foi orientado para a necessidade da conceção de um sistema de deteção e resposta a intrusões físicas, sustentado num novo leque de mecanismos de segurança que:

- Permitam controlar o acesso indevido ao *smartphone*;
- Permitam a partilha segura, simples e espontânea do dispositivo;
- Permitam desencadear respostas em tempo real;
- Não comprometam a usabilidade do dispositivo;
- Tenham opções adequadas a diversas situações do quotidiano, de forma a serem acessíveis a utilizadores comuns.

3.1 Cenários do Problema

Os cenários que apresentamos permitem, através da sua análise, enquadrar para cada um dos problemas descritos as soluções do sistema de deteção e resposta a intrusões físicas que foi desenvolvido. Assim, a partir de três cenários distintos, são relatadas as intrusões físicas ocorridas nos *smartphones*, os riscos e as ameaças decorrentes. Face a cada problema e consoante as situações "vividas", são exploradas as diferentes necessidades de resposta.

Em cada cenário iremos considerar dois intervenientes – um utilizador comum de *smartphones* e um intruso (atacante) – e um contexto relacional e físico.

3.1.1 Cenário 1: Intrusão Física – acesso não autorizado

A Alice, administrativa numa grande empresa, é uma pessoa muito prática, que considera que os métodos de autenticação são uma perda de tempo e como não garantem uma segurança 100% eficaz, optou por desativá-los no seu smartphone.

O Bob, colega de trabalho da Alice, é uma pessoa bastante intrometida e os colegas de escritório consideram-no um grande bisbilhoteiro.

Um dia, a Alice foi almoçar fora com as amigas de infância e, como saiu apressadamente do escritório, não se apercebeu que deixou o seu smartphone em cima da sua

mesa de trabalho.

O Bob, assim que viu o smartphone da Alice esquecido em cima da secretária, considerou que ganhara o dia, pois esta oportunidade permitir-lhe-ia descobrir os segredos que ela guardava. Acedeu à galeria de fotografias e visualizou algumas bastante "comprometedoras".

O Bob voltou a colocar o smartphone no mesmo sítio, sem deixar quaisquer pistas.

A Alice, assim que se apercebeu que se tinha esquecido do smartphone, pensou que o Bob não iria desperdiçar a oportunidade de explorar a sua informação mais pessoal e regressou rapidamente ao escritório. Ao chegar, o seu colega Bob cumprimentou-a com um sorriso comprometedor. Embora não tendo como o provar, a Alice ficou bastante desconfiada de que este tivesse acedido ao seu smartphone e ficou receosa do que ele pudesse ter descoberto e dos rumores que pudesse divulgar.

3.1.2 Cenário 2: Intrusão Física – partilha autorizada

O James e a Mary são um jovem casal. A Mary considera que o marido é um pouco ciumento e ansioso, e bem poderá ter razão.

Ultimamente, o James anda intrigado com o tempo excessivo que a Mary tem dedicado ao smartphone. De facto, ela, às escondidas, tem estado muito ocupada a preparar uma festa surpresa para o aniversário do James e tem trocado várias mensagens com diversos convidados.

Na noite anterior à festa de aniversário, enquanto estavam na sala a ver televisão, o James lembrou-se repentinamente que não enviara um email urgente para um dos seus clientes mais importantes. Como o smartphone pessoal estava sem bateria e o computador tinha ficado no escritório, ficou nervoso e pediu à Mary que lhe emprestasse o smartphone.

A Mary, para não revelar uma atitude de desconfiança que pudesse comprometer a relação do casal, inseriu o PIN do método de autenticação no smartphone e partilhou-o com o marido sem qualquer vigilância. No entanto, o James, após enviar o email, aproveitou a oportunidade para ler as mensagens trocadas pela Mary com os convidados e descobriu todos os planos que estavam a preparar.

A Mary considerou que o marido demorou muito tempo para enviar o email e ficou receosa que ele tivesse lido as mensagens trocadas, o que iria estragar a surpresa que estava a preparar. A festa, apesar de se ter realizado, não teve o impacto desejado. O efeito surpresa tinha sido perdido.

3.1.3 Cenário 3: Intrusão Física – partilha não autorizada

A Anne e a Sophia são jovens estudantes universitárias. A Anne é uma rapariga conservadora e pouco dada a brincadeiras. Ela e a sua amiga Sophia planearam efetuar uma viagem no verão, pelo estrangeiro, para comemorar o final do curso que terminaram com sucesso.

Numa tarde, enquanto estavam a conversar ao telefone sobre os países que queriam visitar, o Charlie, irmão mais novo da Sophia e um miúdo bastante traquina, tirou-lhe o smartphone e fechou-se no quarto.

Apesar de muitas tentativas, a Sophia não conseguiu que o Charlie lho devolvesse. O Charlie resolveu enviar várias mensagens ofensivas à Anne. Quando a Sophia recuperou o smartphone, tentou explicar à amiga o que se tinha passado. No entanto, a Anne ficou muito aborrecida com o teor das mensagens, e afirmou que não iria frequentar mais a sua casa nem iria viajar com ela.

3.2 Modelo Adversarial

As intrusões físicas implicam que o adversário tenha acesso físico ao *smartphone* da vítima. De acordo com os estudos empíricos que já referimos [36, 40], essas intrusões são frequentemente perpetradas por pessoas comuns e socialmente próximas da vítima, nas quais se englobam os familiares, amigos e colegas de trabalho.

O nosso modelo adversarial assume que um adversário deve ter, pelo menos, um dos seguintes objetivos:

- Ler dados sensíveis (e.g., fotografias, vídeos, mensagens de texto, entre outros);
- Apagar ou modificar dados sensíveis (e.g., apagar *emails*, alterar números de contactos telefónicos, entre outros);
- Ocultar as pistas do acesso não autorizado.

O nosso modelo adversarial parte ainda de alguns pressupostos. O adversário:

- É um utilizador comum, ao nível das competências e conhecimentos em termos de utilização de *smartphones*;
- Tem acesso físico ao dispositivo;
- Consegue ultrapassar a barreira de segurança imposta pelos métodos de autenticação;
- Repõe o dispositivo no local e estado iniciais, ou seja, não tem como objetivo roubar o dispositivo.

3.3 Abordagem Proposta

No desenho da nossa solução optámos por adotar, como dispositivo auxiliar, o *smartwatch* (*wearable*) que, contrariamente ao *smartphone*, está em contacto físico com o utilizador, no seu pulso. Este dispositivo permite ao utilizador a interação inconspícua com o *smartphone*, integrar e aceder rapidamente à informação, monitorizar as atividades ocorridas no *smartphone* e, desta forma, responder remotamente e em tempo real a situações de ameaça, sem comprometer a usabilidade dos dispositivos, assim como permite a partilha segura, espontânea e simples do *smartphone*.

O sistema de deteção e resposta a intrusões físicas deverá ser instalado nos dois dispositivos (*smartphone* e *smartwatch*), deverá ser configurado no *smartphone* e os mecanismos de deteção e resposta deverão ser concebidos com base nas características da comunicação *Bluetooth* a partir das quais serão estruturadas diferentes respostas (independentes – não mutuamente exclusivas) a intrusões físicas:

- Quando os dispositivos não têm ligação *Bluetooth* (isto é, estão afastados) e ocorre o acesso não autorizado ao *smartphone*:
    - O sistema ativa, automaticamente no *smartphone*, o conjunto de respostas, previamente configurado pelo utilizador, para impedir o acesso não autorizado à informação sensível no *smartphone* como, por exemplo, ocultar ficheiros e adicionalmente recolher elementos relevantes sobre as atividades de intrusão ocorridas, gerando um relatório detalhado dessas atividades e/ou obtendo elementos identificativos do intruso (e.g., fotografa o intruso).
- Quando os dispositivos têm ligação *Bluetooth* (isto é, estão próximos) e ocorre a partilha consentida e/ou a partilha não autorizada do dispositivo:
    - O utilizador, em consonância com diferentes situações/contextos, ativa, através do seu *smartwatch*, diversos mecanismos de deteção e resposta. Por exemplo, numa situação de partilha autorizada (ou consentida) poderá monitorizar as atividades efetuadas no *smartphone* pelo convidado e desencadear discretamente – através do *smartwatch* – o conjunto de respostas de segurança, configurado previamente, que permitirá restringir o acesso a informação sensível (e.g., ocultar ficheiros), desativar aplicações ou bloquear o dispositivo, entre outras;
    - Numa situação de partilha não autorizada, o utilizador poderá ativar, em tempo real, no *smartwatch* a resposta que considera mais apropriada (e.g., bloquear de imediato o *smartphone*).

Em síntese:

Ligação *Bluetooth*	**Cenários de Intrusão Física**	**Configuração Prévia**	**Utilizador**	**Dispositivo Auxiliar**	**Respostas**
Sem ligação	Acesso não autorizado	Sim	Sem intervenção direta	*Smartwatch*	Ativadas automaticamente, no *smartphone*
Com ligação	Partilha autorizada	Sim	Com intervenção direta	*Smartwatch*	Ativadas, pelo utilizador, de forma inconspícua através do *smartwatch*
	Partilha autorizada e Partilha não autorizada	Não			Ativadas no *smartwatch*, pelo utilizador, em tempo real

Tabela 3.1: Síntese da abordagem proposta.

3.4 Propostas de Solução

Nesta secção são apresentadas propostas de solução, segundo a abordagem sugerida, para os cenários de intrusões físicas apresentados anteriormente. Assim, iremos considerar que o utilizador possui um *smartwatch* com diversas funcionalidades básicas, tais como relógio, notificação de mensagens e *emails*, entre outras aplicações mais sofisticadas.

É de realçar que os cenários de respostas apresentados descrevem apenas as três situações definidas anteriormente, no entanto o sistema desenvolvido permite que a sua aplicação seja direcionada para um conjunto mais alargado de situações.

3.4.1 Resposta Cenário 1: Intrusão Física – acesso não autorizado

A Alice, administrativa numa grande empresa, sabe que o seu colega Bob é muito intrometido e bisbilhoteiro e que não perde uma oportunidade de divulgar os segredos alheios. Apesar de não utilizar métodos de autenticação no seu smartphone, possui o nosso sistema no smartphone e smartwatch. Este sistema possui um vasto conjunto de potencialidades de deteção e resposta a intrusões físicas, que a Alice considera bastante útil, porque no âmbito das suas funções tem que se deslocar com frequência entre os diferentes departamentos da empresa e, por vezes, esquece-se do smartphone em cima da secretária. Assim, sempre que a distância de transmissão entre o smartphone e o smartwatch for excedida (equivalente à do alcance do sinal de Bluetooth), o smartphone entra no modo de segurança e desta forma impede o acesso à informação sensível.

Um dia, a Alice foi almoçar com as amigas de infância. Como saiu apressadamente do escritório, não se apercebeu que deixou o seu smartphone em cima da sua secretária.

Quando a Alice se apercebeu que deixara o smartphone no escritório, ficou tranquila, porque havia configurado previamente os seguintes mecanismos de resposta no

smartphone: ocultar álbuns de fotografias, registar atividades e fotografar intruso. Estes mecanismos seriam ativados sempre que a distância de transmissão entre os dispositivos fosse ultrapassada, colocando o smartphone no modo de segurança pretendido.

O seu colega Bob, assim que viu o smartphone da Alice esquecido na secretária, não desperdiçou a oportunidade e acedeu à galeria de fotografias, procurando as mais comprometedoras, mas não encontrou qualquer álbum de fotografias. Deixou o smartphone no mesmo sítio, sem deixar pistas (ou, pelo menos, assim o pensava).

Quando a Alice regressou, os dois dispositivos voltaram a estar próximos e com ligação Bluetooth. No smartphone recebeu a notificação "ocorreu uma intrusão", acedeu ao sistema, analisou o relatório da intrusão e visualizou a fotografia do Bob.

Confrontado com as provas recolhidas, o Bob perguntou-lhe: "Não farias o mesmo?".

3.4.2 Resposta Cenário 2: Intrusão Física – partilha autorizada

A Mary, casada com o James, reconhece que o marido é uma pessoa um pouco ciumenta e ansiosa. Por vezes, o marido pede-lhe o smartphone com o intuito de efetuar chamadas urgentes e/ou consultar a sua conta de email. A Mary, apesar de partilhar o smartphone, sente algum desconforto por recear que o marido aceda à sua informação pessoal.

A Mary adquiriu um smartwatch e por sugestão das suas amigas instalou o nosso sistema. Este sistema permite-lhe, através do smartwatch, ativar mecanismos de segurança no smartphone e desta forma restringir o acesso de terceiros à informação armazenada.

Nos últimos dias, a Mary tem andado muito ocupada com os preparativos da festa de aniversário que pretende que seja uma surpresa para o James.

Numa noite, enquanto estavam na sala a ver televisão, o James lembrou-se que não enviara um email urgente para um seus dos clientes mais importantes. Como o seu smartphone estava sem bateria e o computador no quarto, pediu à Mary que lhe emprestasse o smartphone.

A Mary, após inserir o PIN do método de autenticação no smartphone e de o ter partilhado com o marido, ativou de forma discreta, no smartwatch, um mecanismo de segurança que lhe permitia visualizar as atividades que ele estava a efetuar no smartphone, assegurando-se, desta forma, que ele não iria descobrir qualquer informação relativa à festa surpresa. Além deste mecanismo de segurança, a Mary também tinha configurado previamente uma outra funcionalidade adicional que, depois de ativada discretamente com um conjunto de toques no smartwatch, permitia simular que o dispositivo

estava sem bateria.

O James, após enviar o email, tentou aceder às mensagens trocadas pela Mary. A Mary visualizou, no smartwatch, a ação do marido e efetuou, discretamente, o conjunto de toques no seu smartwatch. O James devolveu o smartphone à Mary e informou-a que este estava sem bateria.

O James adorou a festa de aniversário e a surpresa que a Mary lhe preparara.

3.4.3 Resposta Cenário 3: Intrusão Física – partilha não autorizada

A Sophia e a Anne são estudantes universitárias. Embora boas amigas, a Sophia sabe que a Anne é uma rapariga conservadora e pouco dada a brincadeiras. A Sophia já passou por alguns dissabores, provocados pelas partidas que o seu irmão mais novo, Charlie, gosta de fazer. Numa dessas partidas, o Charlie apoderou-se do smartphone da irmã e enviou várias mensagens disparatadas às amigas dela.

A Sophia tem um grande fascínio por relógios de pulso de todos os géneros, pelo que os pais lhe ofereceram, no final do curso, um smartwatch. A Sophia quis de imediato instalar diversas aplicações, mas houve uma que mereceu especial destaque: o sistema que oferecia um conjunto de funcionalidades bastante interessantes e, acima de tudo, aquelas que impediriam, em tempo real, que o seu irmão Charlie acedesse ao seu smartphone sem autorização.

Numa tarde, enquanto estava a conversar, no jardim, ao telefone com a sua amiga Anne sobre os países que iriam visitar na viagem de finalistas, o Charlie aproximou-se e num ápice tirou-lhe o smartphone e fechou-se no seu quarto.

A Sophia, através do smartwatch, ativou no sistema a opção que lhe permitiu, em tempo real, selecionar a resposta que lhe permitiu bloquear de imediato a utilização do smartphone.

O irmão da Sophia, ao aperceber-se que não podia utilizar o smartphone, nem enviar mensagens disparatadas à amiga da irmã, saiu do quarto, bastante frustrado, e devolveu o smartphone à irmã.

A Sophia suspirou de alívio e depois de contar à Anne o incidente ocorrido, continuaram, calmamente, a fazer planos para a viagem de finalistas.

3.5 Requisitos do Sistema

Os requisitos do sistema integram os requisitos funcionais (funções do sistema) e os requisitos não-funcionais (propriedades do sistema).

Requisitos funcionais do sistema:

- **Proteção de dados sensíveis –** garantir a segurança e privacidade da informação;
- **Capacidade de deteção de intrusões físicas –** monitorizar continuamente o *smartphone* de modo a determinar a ocorrência de uma intrusão física;
- **Capacidade de resposta a intrusões físicas:**
    - Quando os dispositivos não têm comunicação *Bluetooth* – o sistema ativa automaticamente, no *smartphone*, o modo seguro;
    - Quando o dispositivo é partilhado – no momento da partilha, o utilizador ativa, de forma inconspícua no *smartwatch*, o conjunto de respostas previamente configurado no *smartphone*;
    - Quando o dispositivo é partilhado com ou sem autorização – o utilizador ativa, no *smartwatch*, o modo seguro em tempo real.
- **Identificação do intruso –** disponibilizar elementos que permitam, ao utilizador, identificar o intruso;
- **Registo das atividades do intruso –** gerar um relatório detalhado das atividades de intrusão efetuadas no *smartphone*;
- **Monitorização das atividades do intruso em tempo real –** permitir a monitorização no *smartwatch*, em tempo real, das atividades efetuadas no *smartphone*.

Requisitos não-funcionais do sistema:

- **Usabilidade –** facilmente configurável, com uma interface simples e intuitiva, apropriada a qualquer tipo de utilizador;
- **Extensibilidade –** integração fácil e compatível com novas funcionalidades e aplicações;
- **Transparência –** não perturbar a utilização dos dispositivos, isto é, opera em *background*;
- **Modificabilidade –** poderá ser modificado de forma simples e fácil;
- **Disponibilidade –** resistente a falhas que possam impedir o seu funcionamento;
- **Fiabilidade –** robusto e à prova de erros de modo a garantir a sua boa utilização;
- **Eficiência –** utilização adequada dos recursos (bateria, memória, entre outros);
- **Safety –** mantém o funcionamento normal dos dispositivos em situações adversas (e.g., caso o *smartwatch* fique sem bateria ou o utilizador perder o dispositivo, o *smartphone* manterá o seu funcionamento normal).

3.6 Apreciação Crítica

Neste capítulo foi descrito um conjunto de três cenários ilustrativos de situações e contextos (cenários do problema) a partir dos quais foram propostas soluções para as seguintes intrusões físicas: acesso não autorizado, partilha autorizada e partilha não autorizada.

O sistema de deteção e resposta a intrusões físicas em *smartphones* a implementar permite ao utilizador, através do uso de um dispositivo secundário – *smartwatch* – a interação inconspícua com o *smartphone*, integrar e aceder rapidamente à informação, monitorizar as atividades ocorridas e, desta forma, responder remotamente e em tempo real a situações de ameaça.

Os mecanismos de deteção e resposta serão estruturados com base nas características da comunicação *Bluetooth* baseadas na distância entre os dois dispositivos, de modo a permitir detetar e responder a possíveis intrusões.

O sistema oferece uma panóplia de configurações de respostas para cenários de partilha explícita ou de deteção de intrusões, que vão do bloqueio imediato do *smartphone* à monitorização de ações realizadas no dispositivo primário.

Capítulo 4

Implementação

Neste capítulo apresentamos o sistema de deteção e resposta a intrusões – *Smart Intrusion Detection and Response* – *SmartIDR* e os detalhes e decisões tomadas na sua implementação.

4.1 Visão Geral do Sistema – SmartIDR

O sistema *SmartIDR* é composto por uma aplicação para *smartphone* e uma aplicação para *smartwatch*. Na aplicação do *smartphone*, o utilizador poderá efetuar as configurações dos modos de proteção que contêm as respostas a intrusão e consultar informações relativas às intrusões que ocorreram. Na aplicação do *smartwatch*, o utilizador poderá monitorizar as atividades efetuadas no *smartphone* e ativar respostas a intrusão em tempo real.

4.1.1 Modos de Proteção

O sistema *SmartIDR* é composto por três modos de proteção distintos que vão ao encontro da abordagem proposta no capítulo anterior:

Proteção – Acesso não autorizado

- **"Modo Sem Ligação" –** neste modo o sistema ativa automaticamente, sem intervenção do utilizador, o conjunto de respostas previamente configurado na aplicação do *smartphone*, quando os dispositivos não têm ligação *Bluetooth* (estão afastados). Para o *SmartIDR* detetar a interação de um intruso com o *smartphone* recorremos à `API` – *Application Programming Interface* – do serviço de acessibilidade (`AccessibilityService`) do *Android* (*vide* Secção 4.5);

Proteção – Partilha do smartphone

- **"Modo de Partilha Controlada" –** o utilizador (des)ativa de forma inconspícua através do *smartwatch* o conjunto de respostas previamente configurado na aplicação do *smartphone*. Para implementarmos o mecanismo de (des)ativação inconspícuo recorremos ao sensor de luminosidade do *smartwatch* (*vide* Secção 4.7);
- **"Modo de Resposta em Tempo Real" –** permite que o utilizador monitorize as atividades efetuadas no *smartphone* e ative respostas a intrusão em tempo real através do *smartwatch*. Este modo requer que os dispositivos comuniquem entre si (*vide* Secção 4.4).

Na Figura 4.1 apresentamos o fluxograma do *SmartIDR*.

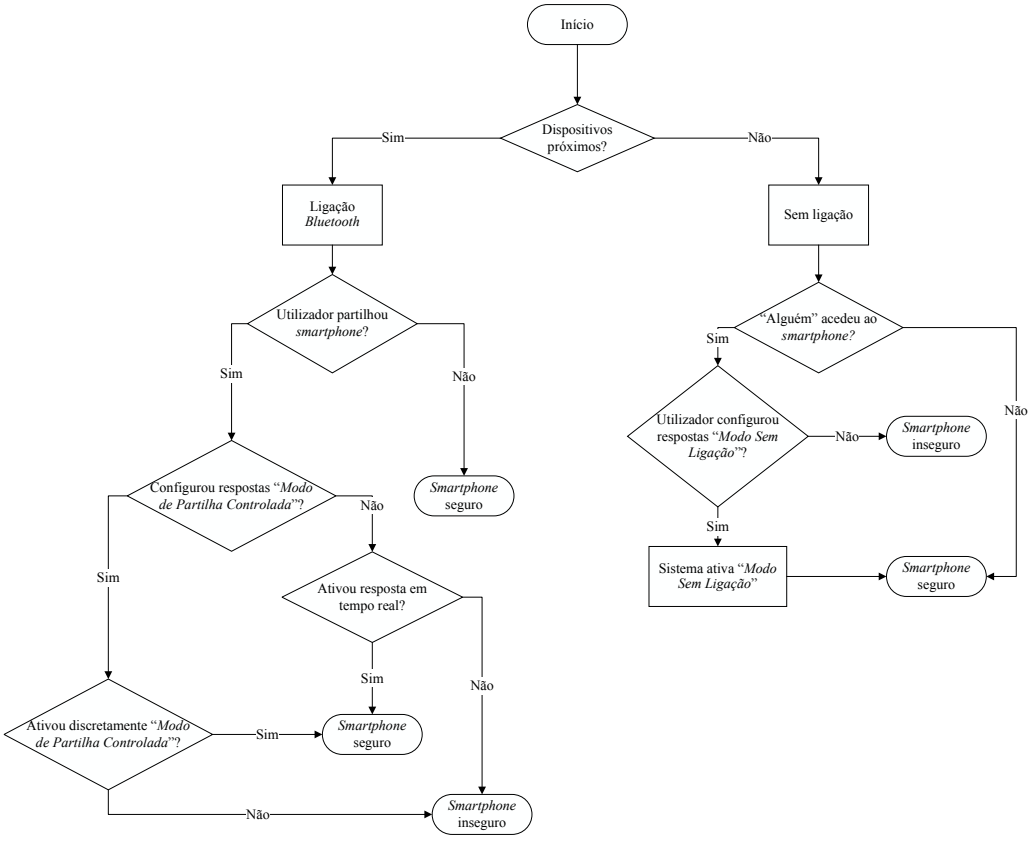
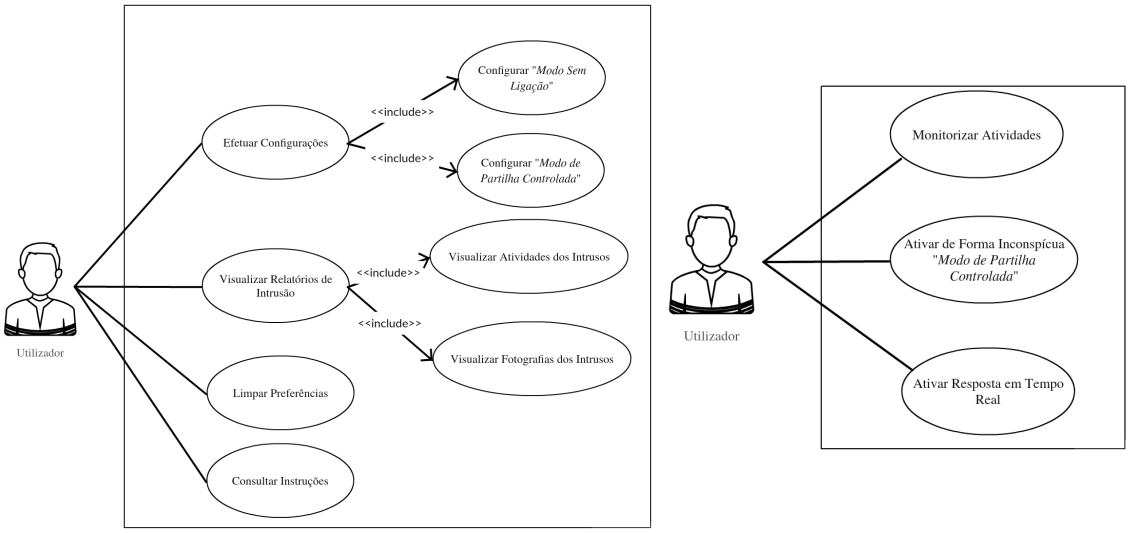


Figura 4.1: Fluxograma do *SmartIDR*.

Após a análise cuidada dos requisitos funcionais do *SmartIDR*, podem ser representados os diagramas de casos de uso correspondentes. Estes diagramas permitem ter uma visão geral da aplicação do *smartphone* (Figura 4.2a) e do *smartwatch* (Figura 4.2b), em termos de funcionalidades e interações do utilizador com o sistema.



(a) Diagrama de casos de uso da aplicação do *smartphone*.

(b) Diagrama de casos de uso da aplicação do *smartwatch*.

Figura 4.2: Diagramas de casos de uso do *SmartIDR*.

4.2 Sistemas Operativos e Linguagens

O sistema foi desenvolvido para *smartphones* com sistema operativo *Android* e *smartwatches* com sistema operativo *Android Wear*.

A linguagem de programação utilizada para a implementação da aplicação foi o `Java`. Os *layouts* da interface do utilizador foram especificados em `XML` (`eXtensible Markup Language`).

4.3 Arquitetura do Sistema

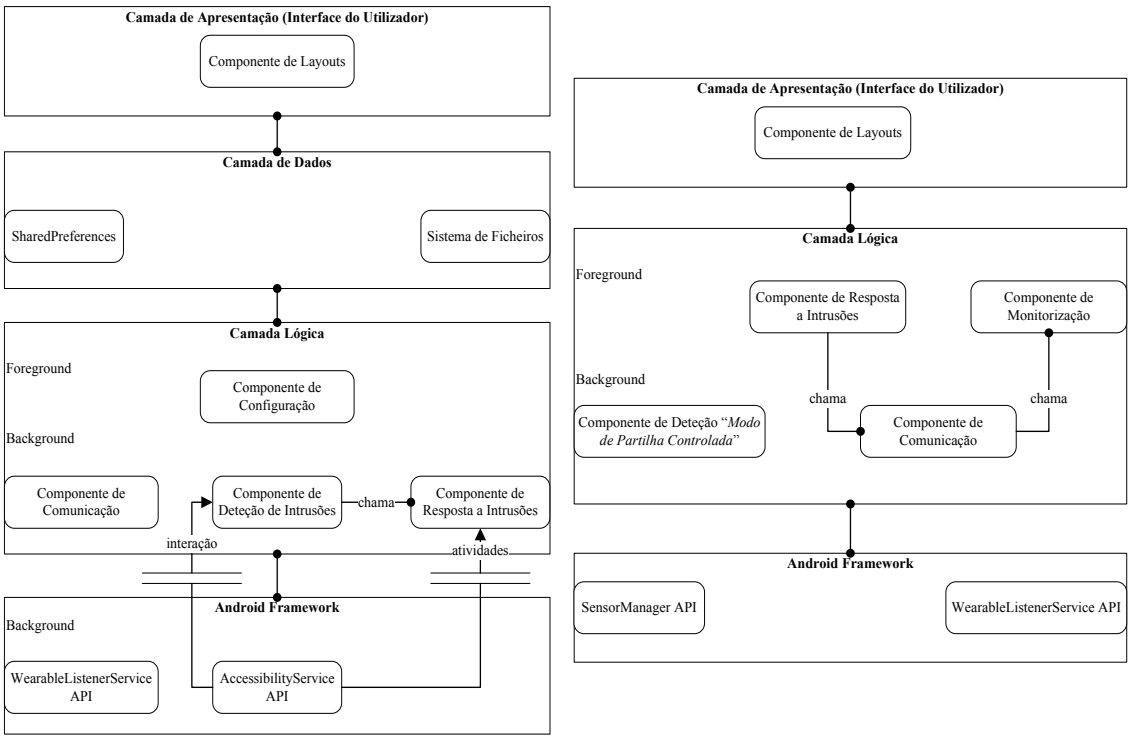
A arquitetura do sistema está dividida em três camadas (Figura 4.3): *Camada de Apresentação*, *Camada de Dados* e *Camada Lógica*.

A *Camada de Apresentação* é composta pelos *layouts* `XML` que incluem os componentes que fazem parte da interface do utilizador (e.g., as listas de respostas – `ListView`, os botões – `Button`, entre outros).

A *Camada de Dados* é responsável pelo armazenamento dos dados do *SmartIDR* (*vide* Secção 4.8).

A *Camada Lógica* é constituída por classes `Java` que representam os componentes da aplicação executados em *foreground* e *background*. Os componentes executados em *foreground* são do tipo `Activity` e estão associados a um *layout* da *Camada de Apresentação* (e.g., submenus de configurações). Estes componentes fornecem uma interface com que o utilizador pode interagir para efetuar as configurações (na aplicação do *smartphone*), ativar uma resposta em tempo real e monitorizar as atividades do intruso (na aplicação do *smartwatch*). Os componentes executados em *background* são do tipo `Service` e desempenham operações de longa-execução (comunicação entre os diposi-tivos, deteção e resposta a intrusões), não fornecem interface e são transparentes para o utilizador.

A *Android Framework* contém todas as `APIs` do *Android*.



(a) Arquitetura *SmartIDR – smartphone*. (b) Arquitetura *SmartIDR – smartwatch*.

Figura 4.3: Arquitetura do sistema.

4.3.1 Respostas a Intrusão

Para que a aplicação permita a integração simples e compatível com novas respostas (requisito não-funcional – extensibilidade), adotámos uma arquitetura de sistema baseada em *plug-ins*. A grande vantagem é que, no futuro, será possível adicionar, atualizar e/ou remover *plug-ins* que permitam responder aos mais diversos cenários de intrusão.

A aplicação principal (`SmartIDRSmartphone.apk`) é responsável por carregar todos os *plug-ins* de resposta (Figura 4.4).

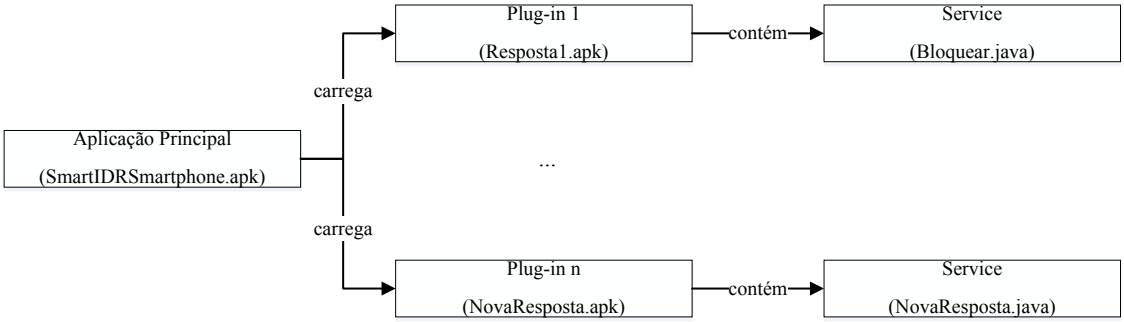


Figura 4.4: Sistema de *plug-ins* de respostas a intrusão.

Cada resposta é composta por um nome, o nome do pacote a que pertence (*package*) e um ícone:

```
public class Resposta{

    private String nomeResposta;
    private String nomePacote;
    private Drawable iconeResposta;

    public Resposta(String nomeResposta, String nomePacote, Drawable iconeRes-
posta){
        this.nome = nomeAplicacaoResposta;
        this.nomePacote = nomePacote;
        this.iconeResposta = iconeResposta;
    }
}
```

Figura 4.5: Código Java – Estrutura respostas a intrusões físicas.

Cada *plug-in* de resposta deverá obedecer aos seguintes requisitos:

- Ser uma aplicação (ficheiro com a extensão `.apk` – *Android application package*);
- Conter um componente do tipo `Service`. Desta forma, a resposta a intrusão é executada em *background* e é transparente para o utilizador e/ou intruso;
- Associar, no ficheiro `AndroidManifest.xml`, o `Service` da resposta à categoria (`smartidr.resposta.PLUG-IN`).

O sistema operativo *Android* requer que as aplicações descrevam explicitamente os seus conteúdos num ficheiro `XML` designado `AndroidManifest.xml`. É neste ficheiro que as aplicações declaram os componentes do tipo `Activity`, do tipo `Service`, as permissões requeridas pela aplicação, entre outros.

O ficheiro `AndroidManifest.xml` dos *plug-ins* de resposta do *SmartIDR* deverá apresentar a seguinte estrutura:

```
<service
    android:name="NovaResposta"
    android:icon="@drawable/iconenovaresposta"
    android:label="Nova Resposta">
    <intent-filter>
        <action android:name="android.intent.action.MAIN" />
        <category android:name="smartidr.resposta.PLUG-IN" />
    </intent-filter>
</service>
```

Figura 4.6: Código XML – Ficheiro AndroidManifest.xml plug-ins de resposta.

O menu de configurações contém listas (`ListView`) de respostas para cada modo de proteção. Estas listas são compostas apenas pelos *plug-ins* que obedeçam aos requisitos apontados:

```
private void iniciaListaRespostas(){
    listaRespostas = new ArrayList<Resposta>();
    PackageManager gestorPacotes = getActivity().getPackageManager();
    Intent servicosRespostas = new Intent(Intent.ACTION_MAIN, null);

    servicosRespostas.addCategory("smartidr.resposta.PLUG-IN"); //Adiciona
apenas à lista os plug-ins de resposta do SmartIDR

    List<ResolveInfo> listarespostas = gestorPacotes.queryIntentServices(ser-
vicosRespostas, 0); //A lista contém, apenas, plug-ins de resposta do SmartIDR


    for (ResolveInfo ri : respostas) {
            Resposta resposta = new Resposta((String) ri.loadLabel(gestorPaco-
tes), ri.serviceInfo.name, ri.serviceInfo.loadIcon(gestorPacotes));
            listaRespostas.add(resposta);
    }
}
```

Figura 4.7: Código Java – Composição da lista de respostas a intrusões físicas.

Nos modos "*Sem Ligação*" e "*Partilha Controlada*" implementámos *plug-ins* de resposta a intrusões com o objetivo de:

Impedir o acesso ao smartphone

- **"Bloquear" –** simula que o *smartphone* está bloqueado. Para tal, são alteradas as definições do *smartphone*, diminuindo o volume do som e a luminosidade do ecrã para o nível 0. Além disso, é adicionada uma janela (`View`) que ocupa todo o ecrã e se sobrepõe às janelas de outras aplicações ou partes da interface, impedindo que o intruso interaja com o dispositivo.

  Uma resposta alternativa que poderia atingir os mesmos objetivos seria desligar o *smartphone*; no entanto, esta ação requer que o dispositivo tenha permissões de administrador (*root*), o que faria com que muitos utilizadores não a adotassem;

- **"Pedir Autenticação" –** faz um pedido de autenticação. Esta resposta só será eficaz se o utilizador tiver configurado no *smartphone* um método de autenticação (e.g., PIN) e se o intruso não conhecer o "segredo" do método.

Recolher informações relativas à intrusão

- **"Registar Atividades" –** gera relatórios de intrusão que incluem as atividades efetuadas no *smartphone* pelos intrusos. Para registar as atividades/interações do intruso com o dispositivo é necessária a utilização do serviço de acessibilidade (*vide* Secção 4.5);
- **"Fotografar Intruso" –** fotografa o intruso com a câmara frontal do dispositivo. Esta resposta impôs alguns desafios de implementação (*vide* Secção 4.6).

Proteger os dados sensíveis

- **"Ocultar Álbuns de Fotografias" –** oculta os álbuns de fotografias configurados pelo utilizador. Para tal, é adicionado, na pasta do álbum correspondente, um ficheiro em branco designado "`.nomedia`". Desta forma, impedimos que os álbuns de fotografias sejam apresentados na Galeria e noutras aplicações;
- **"Ocultar Álbuns de Vídeos" –** oculta os álbuns de vídeos configurados pelo utilizador. Esta resposta foi implementada de forma análoga à resposta "*Ocultar Álbuns de Fotografias*";
- **"Desativar Aplicações" –** desativa as aplicações configuradas pelo utilizador. A implementação desta resposta recorre ao serviço de acessibilidade (*vide* Secção 4.5).

Dissuadir o intruso

- **"Emitir Alarme Sonoro" –** emite um alarme sonoro que tem como objetivo dissuadir o intruso. Para tal, o volume do som é aumentado para o nível máximo e é reproduzido o alarme;
- **"Exibir Mensagem de Texto" –** exibe uma mensagem de texto (`Toast`) previamente configurada pelo utilizador.

O "*Modo de Resposta em Tempo Real*" é composto pelos *plug-ins* de resposta que têm como objetivo:

Impedir o acesso ao smartphone em tempo real

- **"Bloquear" –** análoga à resposta "*Bloquear*" dos modos "*Sem Ligação*" e "*Partilha Controlada*";
- **"Pedir Autenticação" –** análoga à resposta "*Pedir Autenticação*" dos modos

"*Sem Ligação*" e "*Partilha Controlada*".

Recolher informações relativas à intrusão em tempo real

- **"Monitorizar Atividades" –** permite que o utilizador monitorize as atividades efetuadas no *smartphone*, através do *smartwatch*. Para monitorizar as atividades/interações do intruso com o dispositivo, recorremos ao serviço de acessibilidade (*vide* Secção 4.5).

4.4 Comunicação entre Dispositivos

Para que seja possível ativar o "*Modo de Partilha Controlada*", "*Monitorizar Atividades*" e ativar respostas a intrusão em tempo real, é necessário que os dispositivos comuniquem entre si.

O *Android Wear* fornece `APIs` que possibilitam a comunicação entre os dispositivos: a `Message API` e a `Node API`.

A `Message API` fornece um mecanismo de comunicação *one-way* (apenas numa direção, do transmissor para o recetor da mensagem). A `Node API` permite saber quais são os nós/dispositivos que têm ligação com o dispositivo transmissor.

Enviar Mensagens

Para enviar mensagens, é necessário obter uma referência para a `Wear API`, através do `GoogleApiClient` e implementar a interface `GoogleApiClient.ConnectionCallbacks`:

```
GoogleApiClient clienteApi = new GoogleApiClient.Builder(aplicacao.getApplica-
tionContext())
    .addApiIfAvailable(Wearable.API)
    .build();
clienteApi.blockingConnect(CONNECTION_TIME_OUT_MS, TimeUnit.MILLISECONDS);
```

Figura 4.8: Código Java – Referência Wear API.

Antes de enviar a mensagem é necessário saber se os dispositivos têm ligação. Para tal, obtemos a lista de nós/dispositivos (`NodeApi.getConnectedNodes()`) que têm ligação com o dispositivo transmissor, utilizando a `Node API`:

```
NodeApi.GetConnectedNodesResult listaNos = Wearable.NodeApi.getConnected-
Nodes(clienteApi).await();
if (listaNos.getNodes().isEmpty())
    Log.i("Sem Ligação!", "Sem Ligação!");
else {
    Wearable.MessageApi.sendMessage(clienteApi, no.get(0).getId(), mensagem,
mensagem.getBytes()).await();
}
```

Figura 4.9: Código Java – Envio de mensagens entre dispositivos.

Receber Mensagens

Para que o dispositivo recetor receba mensagens do outro dispositivo, implementámos um `Service` (`RecebeMensagem.class`) que estende o serviço `WearableListenerService`. O `WearableListenerService` permite que o dispositivo receba mensagens em *background*. Para tal, utilizámos o método `onMessageReceived`. Este método é invocado cada vez que uma mensagem é enviada de um dispositivo para outro.

Proximidade Dispositivos

Para sabermos se os dispositivos estão próximos, implementámos um `TimerTask` que obtém, de 5 em 5 segundos, a lista de nós/dispositivos que têm ligação ao dispositivo. Se a lista estiver vazia assumimos que os dispositivos estão afastados.

4.5 Interações com o Smartphone

O serviço de acessibilidade (`AccessibilityService`) do *Android* é executado em *background* e "captura" eventos de acessibilidade (`AccessibilityEvents`) que contêm informações relativamente às interações do utilizador/intruso com a interface do dispositivo (e.g., botões selecionados).

Este serviço foi fundamental para a implementação das seguintes funcionalidades:

- **Deteção de Intrusões no "Modo Sem Ligação" –** para decidir se está a ocorrer uma intrusão no "*Modo Sem Ligação*", este serviço permite saber se "alguém" está a interagir com o *smartphone* quando os dispositivos não têm ligação. Nesse caso, serão ativadas as respostas previamente configuradas pelo utilizador;
- **Resposta "Desativar Aplicações" –** os eventos de acessibilidade permitem-nos saber quais são as aplicações executadas pelo intruso. Se a aplicação executada corresponder a uma das aplicações configuradas pelo utilizador para serem desativadas, é executada uma ação que faz com que o *smartphone* regresse ao ecrã inicial:

```
Intent ecraInicial = new Intent(Intent.ACTION_MAIN);
ecraInicial.addCategory(Intent.CATEGORY_HOME);
ecraInicial.setFlags(Intent.FLAG_ACTIVITY_NEW_TASK);
```

Figura 4.10: Código Java – Ação regressar ao ecrã inicial.

  Outra implementação possível seria ocultar os ícones das aplicações desativadas;
- **Respostas "Registar Atividades" e "Monitorizar Atividades" –** os eventos de acessibilidade permitem, na resposta "*Registar Atividades*", gerar os relatórios de

intrusão que detalham as atividades efetuadas pelo intruso no *smartphone*. Na resposta "*Monitorizar Atividades*", as atividades são enviadas do *smartphone* para o *smartwatch*.

O *SmartIDR* "captura" os seguintes eventos de acessibilidade:

- `TYPE_VIEW_SELECTED` – indica os componentes da interface que são selecionados pelo intruso;
- `TYPE_VIEW_CLICKED` – indica os componentes da interface que são clicados pelo intruso;
- `TYPE_VIEW_TEXT_CHANGED` – indica o texto escrito pelo intruso e o campo em que foi escrito;
- `TYPE_NOTIFICATION_STATE_CHANGED` – representa o evento de apresentação de uma notificação.

4.6 Fotografar Intruso

O primeiro desafio na implementação da resposta "*Fotografar Intruso*" foi fotografar o intruso de forma inconspícua. Segundo a documentação do *Android*, para uma aplicação tirar uma fotografia é necessário que o utilizador pré-visualize o que irá ser fotografado pela câmara do dispositivo [17]. Para ultrapassarmos este requisito imposto pelo sistema operativo, utilizámos uma `View` com altura e largura 1 (definidas em pixéis). Desta forma, a pré-visualização da fotografia não fornece *feedback* visual ao intruso:

```
windowManager = (WindowManager) getSystemService(WINDOW_SERVICE);
parametros = new WindowManager.LayoutParams(
        WindowManager.LayoutParams.TYPE_PHONE,
        WindowManager.LayoutParams.FLAG_NOT_FOCUSABLE);
parametros.width = 1; // 1 pixel
parametros.height = 1; // 1 pixel
parametros.x = 0;
parametros.y = 0;
parametros.screenOrientation = ActivityInfo.SCREEN_ORIENTATION_PORTRAIT;
windowManager.addView(fotografia, parametros);
```

Figura 4.11: Código Java – `View` pré-visualização fotografia intruso.

Outro desafio na implementação desta resposta foi mitigar as limitações que poderia apresentar, no caso de a fotografia tirada não conter a face do intruso, existir pouca luminosidade no local onde está a decorrer a intrusão ou a câmara do dispositivo ter pouca qualidade.

De forma a mitigar estas limitações implementámos um mecanismo que permite:

- **Detetar faces numa fotografia –** permite detetar se a fotografia tirada contém pelo menos uma face. Para atingirmos este objetivo utilizámos a `API FaceDetector`: criámos um detetor de faces (`FaceDetector(int width, int height, int maxFaces)`) configurado com a altura e largura da fotografia tirada e um inteiro com o número máximo de faces que podem ser detetadas (neste caso 1). Foi ainda utilizado o método `findFaces(Bitmap bitmap, Face [] faces)` que devolve o número de faces detetadas no `Bitmap` que contém a fotografia;
- **Aferir a qualidade da fotografia –** no caso de não ser detetada uma face durante a intrusão, é armazenada a fotografia que contém maior detalhe e que pode fornecer informações relevantes ao utilizador (e.g., o local onde ocorreu a intrusão). Para selecionarmos a melhor fotografia, comparámos o tamanho em `bytes` da fotografia tirada com o da melhor fotografia que foi tirada anteriormente. No caso de a fotografia atual ser mais detalhada (com tamanho superior) é armazenada e a fotografia anterior é eliminada.

Na Figura 4.5 descrevemos o pseudo-código do algoritmo que permite selecionar a melhor fotografia:

Algoritmo 1 Resposta Fotografar Intruso

```
1:function FOTOGRAFAINTRUSO()
2:     f ← fotografia tirada com a camara frontal do smartphone
3:     n ← indica numero de faces detetadas na fotografia f
4:     tMaisDetal ← indica o tamanho (em bytes) da fotografia mais detalhada
5:     if n = 1 then
6:         apagafotografiaantiga()
7:         guardafotografia(f)
8:         parafotografarintruso()
9:     else
10:        tAtual ← indica o tamanho (em bytes) da fotografia f
11:        if tMaisDetal < tAtual then
12:            apagafotografiaantiga()
13:            guardafotografia(f)
14:            tMelhor ← tAtual
15:        end if
16:        FOTOGRAFAINTRUSO()
17:    end if
18:end function
```

Figura 4.12: Pseudo-código – Fotografar Intruso.

4.7 Des(ativação) Inconspícua Modo de Partilha Controlada

Para implementarmos o mecanismo de (des)ativação inconspícua do "*Modo de Partilha Controlada*", através do *smartwatch*, utilizámos o sensor de luminosidade.

```
SensorManager sensorManager = (SensorManager) getSystemService(Context.SEN-
SOR_SERVICE);
sensorManager.registerListener(this, sensorManager.getDefaultSensor(Sen-
sor.TYPE_LIGHT), SensorManager.SENSOR_DELAY_FASTEST);
```

Figura 4.13: Código Java – Aceder ao sensor de luminosidade do *smartwatch*.

Para que uma aplicação possa aceder a um sensor ou a um conjunto de sensores, o *Android* fornece o serviço do sistema `SensorManager`. Este é acedido através do método `getSystemService()` com o argumento `Context.SENSOR_SERVICE`. Com o serviço `SensorManager` é possível obter um sensor específico através do método `getDefaultSensor()`. Na nossa implementação, este método recebe o sensor de luminosidade (`Sensor.TYPE_LIGHT`).

Para iniciar a recolha de dados do sensor é necessário registar um `Listener`. Os dados são recolhidos a uma taxa definida no argumento da função `registerListener`. Para os dados do sensor serem recolhidos da forma mais rápida possível utilizámos a constante `SENSOR_DELAY_FASTEST`.

O método `onSensorChanged(SensorEvent event)` é chamado quando os dados do sensor de luminosidade estão disponíveis. Este sensor fornece um valor único (`event.values[0]`) que representa o nível de luminosidade ambiente em unidades do SI (lx).

No entanto, a simples alteração da luminosidade do meio ambiente não é suficiente. É necessário garantir com um certo nível de confiança que o utilizador tem a intenção de desempenhar esta ação. Para tal, terá de efetuar três sequências tapando e destapando o sensor de luminosidade do *smartwatch*, num intervalo de 10 segundos.

O mecanismo de (des)ativação do "*Modo de Partilha Controlada*" segue o seguinte pseudo-código:

Algoritmo 2 Mecanismo para (des)ativar o Modo de Partilha Controlada

```
1:function ATIVAPARTILHACONTROLADA()
2:     v ← valor de luminosidade obtido
3:     altLumi ←indica se foram detetadas alteracoes na luminosidade
4:     numAltLumi ←indica o numero de transicoes na luminosidade
5:     if v = 0 & !altLumi then
6:         if numAltLumi = 0 then
7:             contasegundos(10)
```

```
8:              end if
9:              numAltLumi++
10:             altLumi ← true
11:         else if v > 0 & altLumi then
12:             numAltLumi++
13:             altLumi ← false
14:         if numAltLumi = 6 then
15:             enviaMensagemSmartphone()
16:             numAltLumi ← 0
17:             altLumi ← false
18:         end if
19:end function
```

Figura 4.14: Pseudo-código – (Des)ativação do "*Modo de Partilha Controlada*".

Após o utilizador efetuar esta sequência, o *smartwatch* envia uma mensagem para o *smartphone*. No momento em que o *smartphone* recebe a mensagem do *smartwatch* ativa o conjunto de respostas configuradas pelo utilizador. Posteriormente, o *smartphone* envia uma mensagem para o *smartwatch* que indica que a operação foi bem-sucedida. Para o utilizador ter *feedback* de que o modo foi ativado com sucesso, o *smartwatch* vibra (`VIBRATOR_SERVICE`).

A troca de mensagens entre os dois dispositivos é descrita no diagrama de sequência da Figura 4.7:

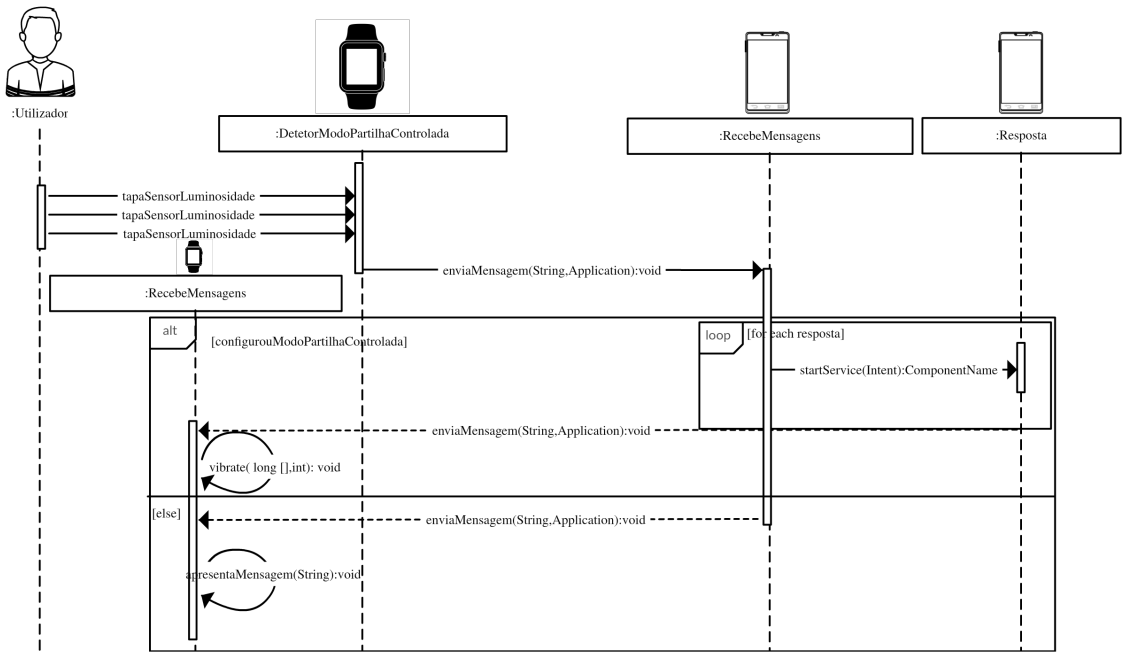


Figura 4.15: Diagrama de sequência – ativação "*Modo de Partilha Controlada*".

4.8 Armazenamento de Dados

Nesta secção discutiremos as decisões de implementação relativamente ao armazenamento dos dados da nossa aplicação.

O sistema operativo *Android* oferece várias opções de armazenamento para guardar os dados de forma persistente [16]:

- `SharedPreferences` – armazenam dados primitivos privados em pares chave-valor;
- Armazenamento interno – armazena dados privados na memória do dispositivo;
- Armazenamento externo – armazena dados públicos no armazenamento externo partilhado (por exemplo, num cartão microSD);
- Bases de dados `SQLite` – armazenam dados estruturados em bases de dados privadas.

O *SmartIDR* contém os seguintes dados:

1. **Preferências do utilizador –** incluem as respostas configuradas, pelo utilizador, para os modos "*Sem Ligação*" e "*Partilha Controlada*". Em cada modo são armazenadas as preferências das respostas que têm configurações adicionais (aplicações escolhidas para a resposta "*Desativar Aplicações*", álbuns de fotografias e vídeos para as respostas "*Ocultar Álbuns de Fotografias*" e "*Ocultar Álbuns de Vídeos*" e a mensagem de texto para a resposta "*Exibir Mensagem de Texto*");
2. **Registos de atividades dos intrusos –** os registos das atividades realizadas pelos intrusos. Os ficheiros são armazenados com a extensão (`.txt`);
3. **Fotografias dos intrusos –** o conjunto de fotografias dos intrusos armazenadas com a extensão (`.jpeg`).

SharedPreferences

Para armazenar as preferências do utilizador, optámos pela utilização da `API SharedPreferences`. Esta é a melhor opção para guardar um conjunto de dados relativamente simples de pares chave-valor. Um objeto `SharedPreferences` aponta para um ficheiro que contém pares chave-valor e fornece métodos simples para a sua leitura e escrita. Cada ficheiro `SharedPreferences` pode ser privado (`MODE_PRIVATE`) ou partilhado (`WORLD_READABLE` e/ou `WORLD_WRITEABLE`). Se o ficheiro for privado, apenas a nossa aplicação tem acesso a este ficheiro. Se o ficheiro for partilhado, todas as aplicações podem aceder-lhe, podendo criar falhas de segurança [16]. Por estas razões, optámos por armazenar estes ficheiros de forma privada.

Armazenamento interno – sistema de ficheiros Android

Os ficheiros podem ser armazenados diretamente no armazenamento interno do dispositivo. Por omissão, os ficheiros armazenados no armazenamento interno são privados (`MODE_PRIVATE`) e as outras aplicações não podem aceder-lhes (nem o próprio utilizador). Quando o utilizador desinstala a aplicação, todos os ficheiros que lhe estão associados são removidos [16]. Por estes motivos, optámos por armazenar as fotografias e registos de atividades dos intrusos no armazenamento interno do dispositivo (Figura 4.8).

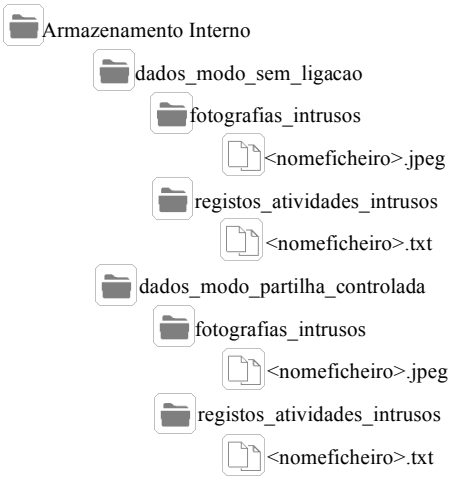


Figura 4.16: Visão geral do armazenamento dos ficheiros da aplicação.

4.9 Permissões

O utilizador, no momento em que instala a aplicação, tem de aceitar ou rejeitar as permissões requeridas, escolhendo desta forma se confia, ou não, na aplicação. A menos que o utilizador concorde com todas as permissões, esta não pode ser instalada. Sendo o *SmartIDR* um sistema que tem como objetivo garantir a privacidade do utilizador, tivemos como princípio utilizar o menor número de permissões possível. As permissões utilizadas (declaradas no ficheiro `AndroidManifest.xml`) pelo nosso sistema são as seguintes:

Aplicação Smartphone

```
<uses-permission android:name="android.permission.CAMERA"/>
```

Permite que a aplicação aceda à câmara do dispositivo. Esta permissão é necessária para a resposta "*Fotografar Intruso*".

```
<uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE"/>
```

Permite que a aplicação leia os dados armazenados no dispositivo.

```
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE"/>
```

Permite que a aplicação escreva, modifique ou apague os dados armazenados no dispositivo.

```
<uses-permission android:name="android.permission.WRITE_SETTINGS"/>
```

Permite que a aplicação leia ou modifique as definições do sistema. Esta permissão é necessária para: aumentar o volume do som do *smartphone* na resposta "*Emitir Alarme Sonoro*"; diminuir o volume do som e a luminosidade do ecrã do *smartphone* na resposta "*Bloquear*".

```
<uses-permission android:name="android.permission.RECEIVE_BOOT_COMPLETED"/>
```

Permite que a aplicação reinicie os serviços (`Service`) de deteção e resposta, automaticamente, quando o sistema é iniciado.

```
<uses-permission android:name="android.permission.SYSTEM_ALERT_WINDOW"/>
```

Permite que a aplicação crie janelas por cima de todas as outras aplicações ou partes de interfaces do utilizador. Esta permissão é necessária para a resposta "*Bloquear*".

```
<uses-permission android:name="android.permission.BIND_ACCESSIBILITY_SER-
VICE"/>
```

Permite que a aplicação utilize o serviço de acessibilidade. Esta permissão é necessária para: detetar intrusões no "*Modo Sem Ligação*" e para as respostas "*Desativar Aplicações*", "*Registar Atividades*" e "*Monitorizar Atividades*".

```
<uses-permission android:name="android.permission.BIND_DEVICE_ADMIN"/>
```

Permite que a aplicação controle programaticamente funcionalidades de segurança do dispositivo. Esta permissão é necessária para a resposta "*Pedir Autenticação*".

Aplicação Smartwatch

```
<uses-permission android:name="android.permission.WAKE_LOCK"/>
```

Impede que a CPU do dispositivo entre em inatividade. Esta permissão é necessária para que o sensor de luminosidade continue em execução, mesmo que o dispositivo esteja inativo. A utilização desta permissão poderá gastar a bateria rapidamente.

```
<uses-permission android:name="android.permission.VIBRATE"/>
```

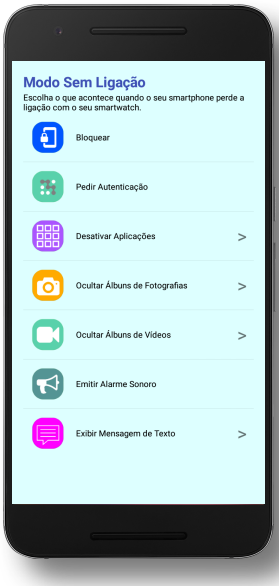
Permite à aplicação controlar o vibrador do dispositivo. Esta permissão é necessária para fornecer ao utilizador *feedback* da (des)ativação do "*Modo de Partilha Controlada*".

4.10 Interface do Utilizador

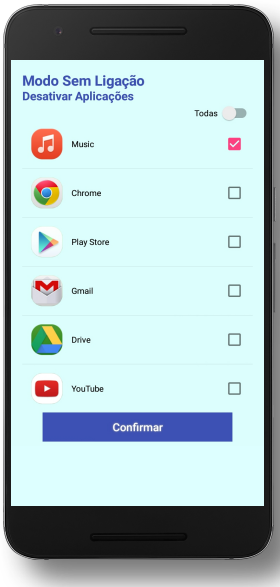
Configuração dos modos da aplicação – *Smartphone*

(a) Ecrã inicial.

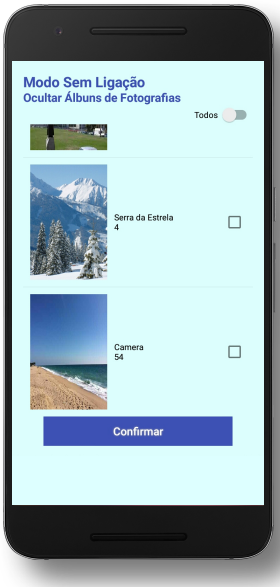
(b) Submenu de configurações.



(c) Excerto lista de respostas a intrusão.



(d) Configuração da resposta "*Desativar Aplicações*".



(e) Configuração da resposta "*Ocultar Álbuns de Fotografias*".

Figura 4.17: Menu principal e submenus de configuração do *SmartIDR*.

A conceção da interface do *SmartIDR* teve como principal objetivo permitir, através de menus intuitivos, uma interação simples, eficiente, atrativa e acessível a qualquer tipo de utilizador.

No *smartphone*, o utilizador poderá aceder à aplicação, sendo-lhe apresentado o ecrã inicial (Figura 4.9a) com os submenus: "*Configurações*", "*Relatório de Intrusões*", "*Limpar Preferências*" e "*Instruções*".

No submenu "*Configurações*" (Figura 4.9b) o utilizador poderá selecionar o modo da aplicação ("*Modo Sem Ligação*" ou "*Modo de Partilha Controlada*") para o qual pretende efetuar as configurações. Para qualquer um dos modos o utilizador poderá escolher as opções de resposta que serão ativadas (Figura 4.9c). Os procedimentos de configuração poderão ser efetuados uma única vez ou, pelo contrário, poderão ser efetuados um número ilimitado de vezes.

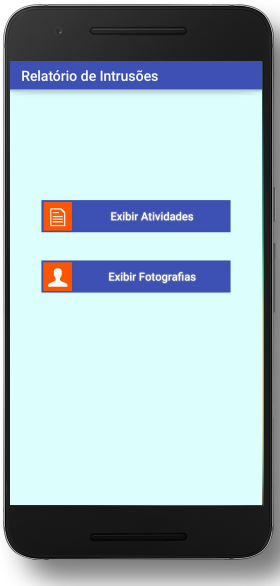
As respostas que necessitam de configurações adicionais estão assinaladas com o símbolo ">" como, por exemplo, no caso de a resposta "*Desativar Aplicações*" e "*Ocultar Álbuns de Fotografias*". No caso de a resposta "*Desativar Aplicações*", são listadas as aplicações instaladas no *smartphone* (Figura 4.9d). No caso de a resposta "*Ocultar Álbuns de Fotografias*", são listados os álbuns de fotografias armazenados (Figura 4.9e) no *smartphone*. Nestes menus o utilizador poderá selecionar, através de caixas de confirmação (`CheckBox`), as aplicações que pretende desativar ou os álbuns que pretende ocultar. Para facilitar o processo de seleção adicionámos um botão (`Switch`) "*Todo(a)s*" que permite marcar/desmarcar rapidamente todas as opções.

O submenu "*Limpar Preferências*" permite apagar todas as configurações que tenham sido efetuadas, os relatórios de atividades e as fotografias dos intrusos.

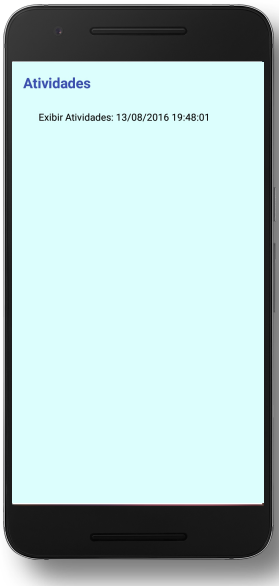
Se o utilizador selecionar "*Instruções*", ser-lhe-ão apresentadas informações relativamente à configuração dos modos e utilização da aplicação.

Visualização dos relatórios de intrusão – Smartphone

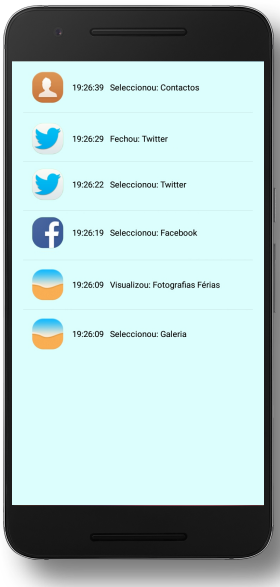
(a) Notificação "*Ocorreu uma Intrusão!*".



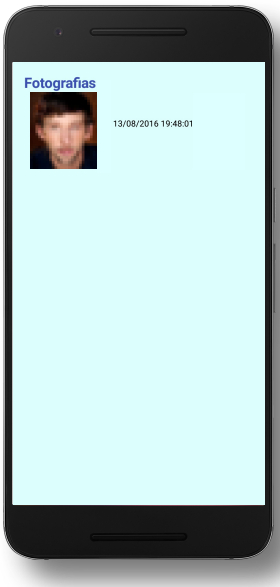
(b) Submenu de relatório de intrusões.



(c) Lista de relatórios de atividades.



(d) Lista de atividades.



(e) Lista de fotografias.

Figura 4.18: Visualização dos relatórios de intrusão.

No caso de ocorrer uma intrusão enquanto os dispositivos estão sem ligação *Bluetooth*, o *smartphone* exibe a notificação "*Ocorreu uma Intrusão!*" no momento em que os dispositivos restabelecem a ligação (Figura 4.10a). Se o utilizador selecionar a notificação, será reencaminhado para o submenu "*Relatório de Intrusões*" (Figura 4.10b).

No submenu "*Relatório de Intrusões*" estão disponíveis as opções "*Exibir Atividades*" e "*Exibir Fotografias*", bastando ao utilizador selecionar a opção pretendida.

Caso tenha sido selecionada a opção "*Exibir Atividades*" (Figura 4.10c), será exibida a lista dos relatórios de atividades efetuadas durante as intrusões. Ao aceder a um dos relatórios serão apresentadas detalhadamente e cronologicamente – da mais recente para a mais antiga – todas as atividades efetuadas pelo intruso. A cada elemento da lista está associado o ícone da aplicação utilizada, a hora (num formato `HH:mm:ss`) e a descrição da atividade efetuada (Figura 4.10d).

Caso o utilizador escolha a opção "*Exibir Fotografias*", será apresentada uma lista com as fotografias dos intrusos (Figura 4.10e). Tal como na lista de atividades, as fotografias são apresentadas cronologicamente – da mais recente para a mais antiga – e a cada elemento da lista estão associadas a data (num formato `dd:MM:yyyy`) e a hora (num formato `HH:mm:ss`) a que o intruso foi fotografado.

Lista de respostas e monitorização de atividades – Smartwatch

(a) Excerto lista de respostas a intrusões.

(b) Lista de atividades.

(c) Mudança da cor do fundo da aplicação.

Figura 4.19: Lista de respostas e lista de atividades.

No ecrã inicial do *smartwatch*, ao aceder à aplicação, é apresentada ao utilizador uma lista com as respostas a intrusões que poderá ativar em tempo real (Figura 4.11a). Caso o utilizador selecione a opção "*Monitorizar Atividades*", serão exibidas, no *smartwatch*, as atividades efetuadas no *smartphone*. As atividades são apresentadas cronologicamente – da mais recente para a mais antiga – e as mais recentes são adicionadas ao topo da lista (Figura 4.11b). A cada elemento da lista está associados o ícone da aplicação utilizada, a

hora (num formato `HH:mm:ss`) e a descrição da atividade efetuada.

No caso de os dispositivos perderem a ligação *Bluetooth*, o fundo da aplicação muda de cor (azul para vermelho) (Figura 4.11c). No caso de os dispositivos restabelecerem a ligação, o fundo será alterado, novamente, para a cor inicial (vermelho para azul).

Capítulo 5

Avaliação

Um sistema só será útil se os utilizadores forem capazes de atingir os objetivos estabelecidos. Um sistema ineficaz provavelmente será abandonado [29].

Para maximizar o sucesso do nosso sistema e identificar eventuais problemas, recorremos aos métodos baseados em grupos de foco e testes de usabilidade com o objetivo de avaliar a nossa solução. O nosso desafio, nesta fase, foi o de tornar a nossa aplicação mais eficaz, eficiente e ir ao encontro das necessidades e expetativas dos potenciais utilizadores.

Numa primeira etapa, procedeu-se à avaliação da qualidade do sistema desenvolvido, com a realização de sessões de grupos de foco presenciais, recolheram-se dados qualitativos e sugestões de melhoria. A análise dos resultados obtidos conduziu-nos a uma reflexão aprofundada acerca das sugestões que considerámos mais pertinentes e levou-nos a reestruturar algumas das funcionalidades do sistema desenvolvido.

Após a implementação das propostas (e consequente reestruturação da aplicação), concluímos esta fase com a avaliação da usabilidade do sistema.

5.1 Grupos de Foco

Os grupos de foco são comumente utilizados como um método de investigação qualitativa e baseiam-se fundamentalmente numa discussão, ou seja, procede-se à reunião de um conjunto de pessoas do público-alvo com o objetivo de trocarem e comentarem opiniões e pontos de vista entre si (em discussão aberta) sobre os tópicos que interessam ao investigador.

Os grupos de foco realizados forneceram-nos uma perspetiva multifacetada sobre as funcionalidades do sistema e a identificação de problemas.

5.1.1 Objetivos

Os principais objetivos dos grupos de foco foram:

- Identificar medidas e práticas de segurança com a proteção dos dados armazenados nos *smartphones*;
- Conhecer motivações, preocupações e precauções adotadas durante a partilha;
- Avaliar qualitativamente a aplicação *SmartIDR*;
- Obter e analisar propostas/sugestões de melhoria;
- Melhorar a aplicação.

5.1.2 Procedimento

Foram realizadas três sessões presenciais, cada uma com três participantes, um moderador e um anotador. Estas sessões decorreram nas instalações da Faculdade de Ciências da Universidade de Lisboa (Portugal) e tiveram uma duração aproximada de setenta e cinco minutos cada.

Foram utilizados os seguintes dispositivos: *smartphone Huawei* ALE-L21, com sistema operativo *Android* 5.0.1, e *smartwatch Moto 360* com sistema operativo *Android Wear* 1.4.0.

O método de seleção da amostra foi o de "por conveniência". Procurou-se a heterogeneidade em termos demográficos e socioprofissionais, privilegiando-se a diversidade de competências ao nível de sistemas informáticos para, assim, ser possível obter elementos relevantes para a temática em debate.

As sessões foram conduzidas de acordo com a sequência de tópicos abordados (*vide* Apêndice A: Guião – Grupos de Foco): apresentação da aplicação desenvolvida (*SmartIDR*); objetivos do estudo; recolha dos dados identificativos dos participantes (*vide* Apêndice B: Formulário – Dados Identificativos); abertura do debate sobre as medidas de segurança adotadas e relato de situações de acesso indevido aos dispositivos móveis pessoais; motivações, preocupações sentidas e medidas de segurança adotadas durante a partilha do *smartphone*.

Seguidamente, foram demonstrados os diferentes modos da aplicação. Procedeu-se, em cada um dos modos, à descrição de um cenário ilustrativo de uma intrusão física e à demonstração das diferentes respostas/soluções propostas pela aplicação. Após esta breve introdução, foi solicitado aos participantes que procedessem às configurações necessárias no *smartphone* e no *smartwatch* e, através da sua intervenção ativa, foram simuladas, novamente, situações de intrusões físicas e de respostas com recurso às funcionalidades

da aplicação. Nesta etapa, os participantes foram incentivados a manifestar a sua opinião e a dar contributos de melhoria.

As questões foram colocadas de forma aberta, tendo sido adaptadas consoante o desenrolar da discussão; no entanto, o moderador guiou a conversa no sentido de gerar e estimular o debate de ideias sobre os tópicos relevantes para este estudo.

5.1.3 Participantes

Os grupos foram repartidos em três sessões distintas, cada uma com três elementos, num total de nove participantes, seis do género masculino e três do género feminino, com idades compreendidas entre os 21 e os 49 anos ($\bar{x} \approx 29$, $s \approx 8{,}4$). Os participantes foram recrutados na Faculdade de Ciências da Universidade de Lisboa (Portugal), são estudantes de Engenharia Informática com um grau académico de nível superior e utilizadores de *smartphones* – Tabela 5.1.

Grupo	**Participante**	**Género**	**Idade**	**Habilitações Literárias**	**Profissão**	**Dispositivo(s) Móvel(eis)**	**Sistema(s) Operativo(s) do(s) *Smartphone(s)***	**Método(s) de Autenticação no(s) *Smartphone(s)***
GF1	P1	Masculino	27	Mestrado	Estudante	*Smartphone*	*Android*	PIN
	P2	Feminino	23	Licenciatura	Estudante	*Smartphone* e *Tablet*	*Android*	Padrão de Desbloqueio *Android*
	P3	Feminino	30	Mestrado	Estudante	*Smartphone* e *Tablet*	*Android*	*Knock Code*[6]
GF2	P1	Masculino	24	Licenciatura	Estudante	*Smartphone* e *Tablet*	*iOS*	PIN e Impressão Digital
	P2	Feminino	21	Licenciatura	Estudante	*Smartphone*	*Android*	Nenhum
	P3	Masculino	36	Mestrado	Trabalhador Estudante	*Smartphone* e *Tablet*	*Android*	PIN
GF3	P1	Masculino	49	Mestrado	Trabalhador Estudante	*Smartphone*	*Android*	Nenhum
	P2	Masculino	26	Licenciatura	Estudante	*Smartphone*	*Android*	Padrão de Desbloqueio *Android*
	P3	Masculino	22	Licenciatura	Estudante	*Smartphone*	*Android*	Padrão de Desbloqueio *Android*

Tabela 5.1: Caracterização dos participantes dos grupos de foco.

[6] Padrão de segurança por toques que define o código pessoal. Os toques são personalizados e podem ser criados em qualquer zona do ecrã do dispositivo.

5.1.4 Resultados

No final de cada sessão, procedeu-se à análise dos dados, complementando-os com as gravações de áudio e das notas tomadas, o que nos permitiu ter presente o contexto em que decorreu cada uma das sessões e, desta forma, proceder a um tratamento mais consistente dos dados recolhidos, de modo a identificar as propostas de melhoria a implementar.

Medidas e práticas de segurança adotadas

A maioria dos participantes (6/9) utiliza apenas um método de autenticação (baseado num PIN ou num padrão de desbloqueio *Android*), um dos participantes utiliza dois métodos complementares (PIN e impressão digital) e dois não adotam qualquer método de autenticação.

Como medida de segurança adicional, todos os participantes afirmaram que mantêm o *smartphone* por perto (em cima da mesa ou no bolso), sob o seu controlo e inacessível a outras pessoas. No entanto, alguns dos participantes admitiram que, por vezes, se esquecem do dispositivo e/ou se afastam do mesmo, o que lhes causa alguma apreensão e receio que alguém possa aceder à sua informação sem a sua autorização e/ou conhecimento. Para que a sua privacidade não possa ser invadida, os elementos GF1P2, GF3P1 e GF3P3 acrescentaram que não armazenam dados sensíveis no *smartphone*.

Como razão para não adotar qualquer método de autenticação, o participante GF2P2 referiu que os métodos disponíveis são pouco seguros pelo facto de serem vulneráveis a ataques de observação. Justificou que, de acordo com a sua experiência, os seus amigos observavam a inserção do método de autenticação e facilmente o ficavam a conhecer. O elemento GF3P1 revelou que não adota métodos de autenticação porque considera que impedem o acesso rápido aos dados que não considera sensíveis, prejudicando a usabilidade do dispositivo.

Relativamente a experiências negativas com o acesso não autorizado ao *smartphone*, a maioria dos participantes (7/9) não relatou qualquer situação deste tipo, no entanto, o participante GF3P1 assinalou que, provavelmente, algum dos familiares já o teria feito. O participante GF2P2 (que não utiliza método de autenticação) revelou que, quando se esquece do *smartphone* em casa, o seu irmão mais novo tem por hábito utilizá-lo para jogar. Embora já lhe tenha pedido para não o fazer, ele continua a utilizá-lo, o que lhe causa algumas preocupações com a segurança dos dados armazenados.

Os elementos GF2P3 e GF3P2 referiram que, apesar das preocupações de segurança, consideravam que os seus familiares mais próximos deveriam saber o "segredo" de autenticação, de modo a poderem utilizar os seus dispositivos, principalmente em situações

de emergência.

Partilha de dispositivos móveis pessoais

As principais razões destacadas para partilhar os dispositivos foram: as aplicações lúdicas (jogos); a visualização de vídeos e de fotografias; as aplicações de *email*, de mensagens de texto (SMS) e chamadas telefónicas.

A maioria dos elementos revelou preocupações com a privacidade e confidencialidade dos dados. Os participantes salientaram, entre outros motivos, que receavam que os outros lessem as suas mensagens, visualizassem fotografias de índole pessoal, removessem e/ou alterassem contactos e acedessem a contas e serviços que acarretassem custos. Também referiram aspetos relacionados com a má utilização e os danos no dispositivo.

Todos os participantes afirmaram que só partilham o seu *smartphone* com pessoas em que confiam plenamente. No entanto, os elementos do GF1 admitiram que, independentemente da confiança e do grau de desconforto causado, vigiavam sempre o dispositivo e ficavam alerta se o tempo, considerado razoável para a realização da atividade, fosse ultrapassado. Assim como no GF2, a generalidade dos participantes referiu, como medida de precaução adicional à supervisão, o facto de serem os próprios a manusear o *smartphone* nesta situação.

Assinalamos que apenas dois dos participantes – GF2P3 e GF3P2 – assumiram que depositavam confiança total nas pessoas, pelo que não adotavam qualquer medida de proteção; ao contrário, o GF3P3 referiu que se sentiria muito desconfortável e embaraçado com o facto de supervisionar a interação da pessoa com o seu *smartphone* pelo que preferia não o partilhar com ninguém.

Aplicação SmartIDR

Na generalidade, os diversos elementos consideraram que a aplicação apresentada permitiria mitigar alguns pontos fracos apontados nos métodos de autenticação existentes e/ou adotados, assim como colmatar algumas das preocupações sentidas com a partilha do dispositivo. A interface foi considerada bastante intuitiva, de fácil utilização e acessível.

Como resultado da experiência de utilização e das opiniões emitidas para os diferentes modos da aplicação concluímos que:

"Modo Sem Ligação"

Este modo foi considerado bastante interessante, principalmente nas situações em que os participantes se esquecem do *smartphone* em algum local ou este está fora do seu alcance.

Os elementos (GF2P2 e GF3P1) que não adotam qualquer método de autenticação reconheceram que este modo, por ser um obstáculo ao acesso indevido, lhes seria muito conveniente.

Do conjunto das nove opções de resposta analisadas pelos participantes, os grupos consideraram, na generalidade, a resposta "*Emitir Alarme Sonoro*" como "divertida", mas excessivamente intensa (alarmante) o que poderia conduzir o intruso a querer livrar-se impulsivamente do dispositivo; a resposta "*Bloquear*" foi considerada, pelo participante GF2P1, como a menos conveniente por poder sugerir que o utilizador teria algo a esconder da outra pessoa o que poderia comprometer as suas relações sociais; quanto à opção "*Pedir Autenticação*", o membro GF2P2 referiu que a sua eficácia estaria dependente da adoção ou não de métodos de autenticação.

Como propostas de melhoria foram apresentadas algumas sugestões que, pela sua pertinência, foram posteriormente equacionadas.

Assim, a opção "*Fotografar Intruso*" foi destacada como bastante relevante, embora alguns elementos do GF1 tivessem assinalado, no entanto, que a possibilidade de tapar a câmara do dispositivo exigiria que a sua adoção devesse estar integrada com outras respostas. A sugestão apresentada pelo GF2 para a opção "*Exibir Mensagem de Texto*" vai ao encontro da anterior, na medida em que este grupo considerou que esta resposta, para ser mais inibidora, deveria também ter associada a fotografia do intruso.

Por considerar que as informações relativas à resposta "*Registar Atividades*" representa um dos pontos fortes do *SmartIDR*, o GF1 indicou que o ecrã inicial da aplicação (no *smartphone*) deveria exibir os relatórios de intrusão.

Os grupos referenciaram que consideravam uma mais-valia que as funcionalidades oferecidas pela aplicação também pudessem ser utilizadas por pessoas que não possuíssem um *smartwatch*.

Destacaram-se pela sua utilidade as opções "*Registar Atividades*", "*Fotografar Intruso*", "*Bloquear*" e "*Pedir Autenticação*".

Embora não enquadrado no âmbito das funcionalidades desta aplicação, referimos que o elemento GF3P3 considerou que as respostas "*Registar Atividades*" e "*Fotografar Intruso*" poderiam ser utilizadas para atrair/espiar intrusos e saber em quem pode confiar.

"Modo de Partilha Controlada"

Este modo foi alvo de algumas opiniões divergentes e ambíguas por parte do GF1 que questionou, por um lado, a sua utilidade, fundamentando que por não conseguir prever as

especificidades de situações futuras e o seu risco, a configuração prévia de respostas poderia ficar aquém do pretendido. Por outro lado, considerou que a resposta "*Desativar Aplicações*" seria bastante adequada para controlo parental, nomeadamente para bloquear jogos e/ou impedir o acesso a aplicações que acarretassem custos.

Os elementos GF2 afirmaram que, independentemente do constrangimento provocado, alertariam a pessoa, com quem partilhassem o *smartphone*, que possuíam uma aplicação que registaria todas as ações que efetuassem. Os participantes GF2P1 e GF2P2 assinalaram que este modo lhes permitiria partilhar o dispositivo com maior segurança e evitaria que as atitudes de supervisão e/ou outras que indiciassem desconfiança, que referiram anteriormente, tivessem de ser tomadas.

Os participantes GF1P1 e GF3P1 afirmaram que o mecanismo de ativação do "*Modo de Partilha Controlada*" era impercetível e muito prático. Os elementos do GF1 sugeriram que, além deste mecanismo, fosse adicionado um botão na aplicação do *smartwatch*, que permitisse também ativar este modo.

A opção "*Registar Atividades*" foi a resposta considerada como a de maior utilidade neste modo, assim como "*Desativar Aplicações*", "*Ocultar Álbuns de Fotografias*" e "*Ocultar Álbuns de Vídeos*" que também foram consideradas bastante importantes e adequadas aos objetivos pretendidos.

"Modo de Resposta em Tempo Real"

Este modo foi considerado como mais apropriado do que o modo anterior ("*Modo de Partilha Controlada*"), principalmente nas circunstâncias em que não se deseja perder tempo com configurações. O GF1 realçou que, neste caso, os aspetos assinalados no ponto anterior como menos positivos, eram superados. A maior flexibilidade e a capacidade de adaptabilidade que este modo faculta, em termos de contexto concreto de partilha e de atuação/resposta em conformidade com a situação real, torna-o mais completo e adequado às diferentes situações do quotidiano.

Os participantes GF1P1 e GF2P3 assinalaram que a opção "*Monitorizar Atividades*", embora pudesse ser considerada um pouco intrusiva e causar alguns constrangimentos, permitiria abandonar atitudes de controlo e vigilância, que por si só também denotam desconfiança e podem comprometer as relações sociais. No entanto, o GF3 concluiu que, uma vez que a partilha tem um propósito estabelecido e consentido, a monitorização das atividades não poderia ser considerada intrusiva ou abusiva.

Foram sugeridas algumas propostas de melhoria que pela sua pertinência, foram posteriormente equacionadas. Assim, relativamente à interface, o elemento GF3P1 mencio-

nou que a designação dos comandos de resposta da aplicação no *smartwatch* deveria refletir o estado oposto do *smartphone*. Por exemplo, após ativar a resposta "*Bloquear*" no *smartwatch*, a designação do comando deveria assumir a ação oposta, ou seja, "*Desbloquear*" e vice-versa.

À semelhança do mencionado anteriormente relativamente ao *smartphone*, o GF1 reiterou que também o *smartwatch* deveria exibir no ecrã inicial da aplicação as atividades monitorizadas.

Destacaram-se, pela sua utilidade e relevância, as opções "*Monitorizar Atividades*", "*Bloquear*" e "*Pedir Autenticação*".

5.1.5 Implicações – Propostas Implementadas

Equacionadas e ponderadas as diversas sugestões apresentadas, considerámos seis propostas que, pela sua relevância e pertinência, deveriam ser alvo de implementação. Assim, a aplicação *SmartIDR* deve:

- **Proposta 1 –** Associar a resposta "*Fotografar Intruso*" a outra(s) resposta(s) de modo a suprir ações e/ou interferências que limitem a sua eficácia, tais como tapar a câmara fotográfica do dispositivo e/ou luminosidade reduzida, entre outras;
- **Solução Proposta 1 –** Complementámos a resposta "*Fotografar Intruso*" com a opção "*Registar Atividades*" (por ser a mais destacada pelos grupos). A seleção da opção será seguida de um aviso (`AlertDialog`), informando que tem outra resposta associada ("*Registar Atividades*") (Figura 5.1);

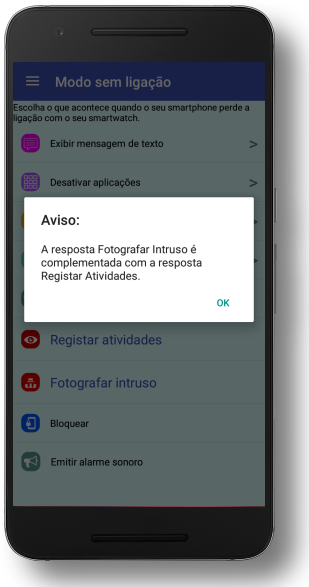
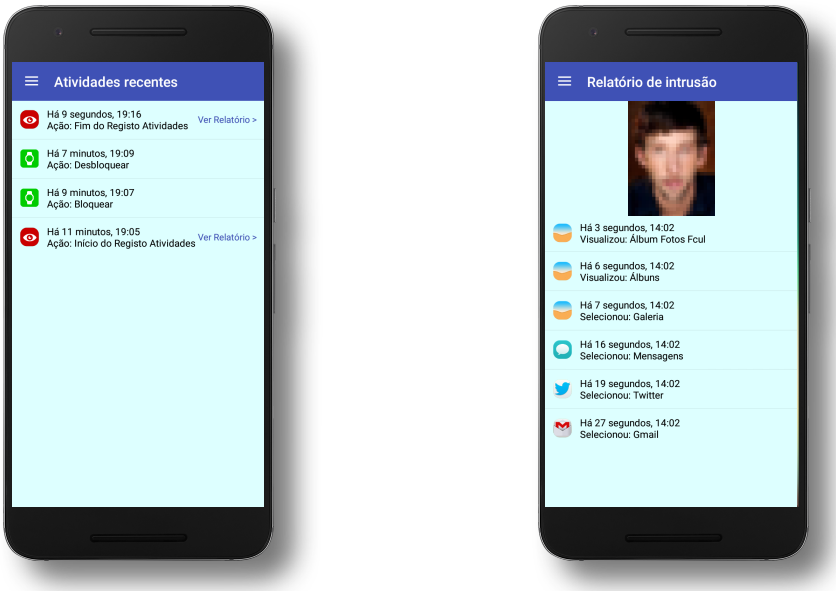


Figura 5.1: Aviso resposta complementar à resposta "Fotografar Intruso".

- **Proposta 2 –** Ter como perfil de resposta pré-selecionado, nos modos "*Sem Ligação*" e "*Partilha Controlada*", a opção "*Registar Atividades*" de forma a que a lista das atividades recentes seja exibida no primeiro ecrã sempre que a aplicação é iniciada;
- **Solução Proposta 2 –** No ecrã inicial foi incluída a lista de atividades recentes e os itens "*Início do Registo Atividades*" e de "*Fim do Registo Atividades*" por cada relatório de intrusão gerado (Figura 5.2a).

  Adicionalmente e, em conformidade com a solução para a proposta número um, incluímos no relatório de intrusão a fotografia do intruso (Figura 5.2b).

  O formato da hora das atividades também foi modificado para um formato mais legível para o utilizador (e.g., em vez de "`HH:mm:ss`", "Há `ss` segundos, `HH:mm`");



(a) Ecrã inicial da aplicação.

(b) Relatório de intrusão.

Figura 5.2: Atividades recentes e relatório de intrusão.

- **Proposta 3 –** Exibir no ecrã de abertura da aplicação do *smartwatch* as atividades efetuadas no *smartphone*;
- **Solução Proposta 3 –** O ecrã inicial da aplicação do *smartwatch* foi modificado passando a exibir as atividades efetuadas no *smartphone* (Figura 5.3a).

  Face à reduzida dimensão do ecrã do *smartwatch* considerámos pertinente que os detalhes da atividade selecionada fossem exibidos num ecrã independente (Figura 5.3b);

(a) Lista de atividades. (b) Detalhes de uma atividade.

Figura 5.3: Lista e detalhes de atividade.

- **Proposta 4 –** Abranger utilizadores que não possuam *smartwatch*;
- **Solução Proposta 4 –** Desenvolvemos o modo adicional – "*Modo de Ativação Rápida*" – que dispensará a utilização do *smartwatch*.

  A configuração do conjunto de respostas (similar ao dos modos "*Sem Ligação*" e de "*Partilha Controlada*") será efetuada no *smartphone*, através do qual poderão ser ativadas rapidamente.

  Com o objetivo de facilitar a interação do utilizador com a aplicação, implementámos um menu de navegação rápida (`NavigationView`) (Figura 5.4), através do qual poderão ser ativadas as respostas pretendidas e o acesso aos menus principais;

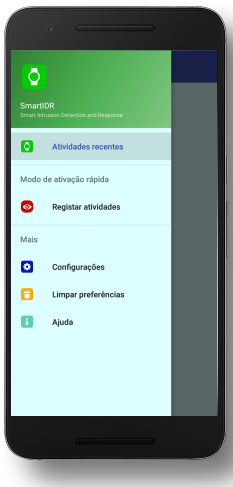


Figura 5.4: Menu de navegação rápida.

- **Proposta 5 –** Possuir um botão na aplicação do *smartwatch* que, como alternativa ao do mecanismo de ativação através do sensor de luminosidade, permita ativar o "*Modo de Partilha Controlada*";
- **Solução Proposta 5 –** Na interface do *smartwatch* foi incluído o botão "*Ativar modo partilha controlada*" (Figura 5.5);

Figura 5.5: Botão "Ativar modo partilha controlada".

- **Proposta 6 –** Assumir designações nos comandos do *smartwatch* opostas ao estado do *smartphone*;
- **Solução Proposta 6 –** Foram alteradas as designações dos botões. Por exemplo, quando for ativada a ação "*Bloquear*" o botão que passará a ser exibido tem a designação "*Desbloquear*" e vice-versa (Figura 5.6).

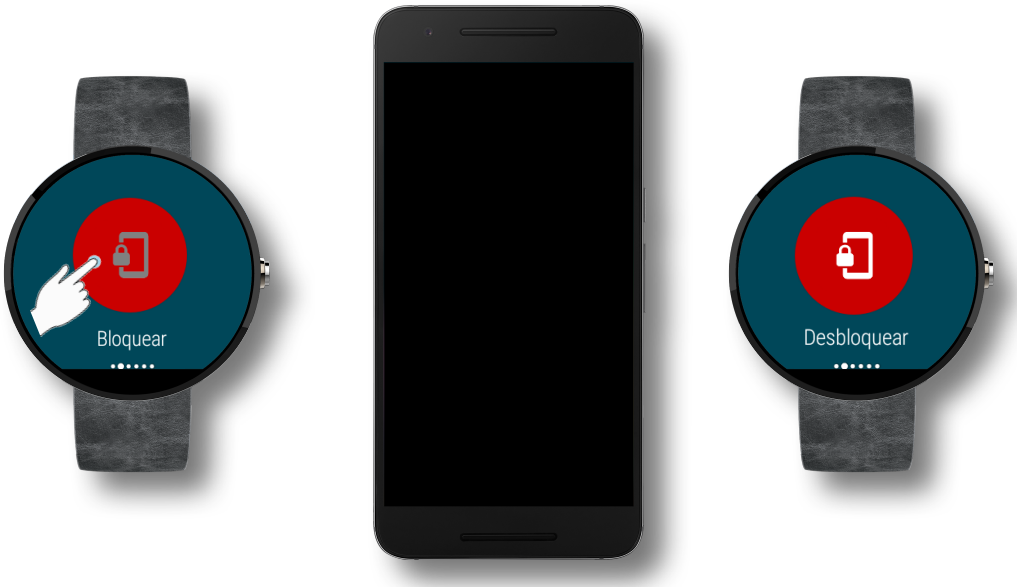


Figura 5.6: Alteração na designação dos botões.

5.2 Testes de Usabilidade

De uma forma geral, os testes de usabilidade servem para validar se as escolhas efetuadas na fase pós-reestruturação vão ao encontro do que se pretende alcançar. Para além disso, pretendeu-se medir [10, 28]:

1. Se o sistema é eficaz, ou seja, se permitiu que os utilizadores conseguissem efetuar as tarefas propostas;
2. Se o sistema é eficiente, ou seja, se o tempo de execução foi o adequado para a realização de uma determinada tarefa;
3. Se o sistema é satisfatório para o utilizador, ou seja, se o nível de experiência de interação foi suficientemente motivador.

5.2.1 Objetivos

A aplicação de testes de usabilidade teve como principais objetivos:

- Avaliar a taxa de sucesso e o tempo de execução das tarefas propostas para identificar problemas de usabilidade;
- Medir a satisfação dos utilizadores com o sistema (aplicação da "Escala de Usabilidade do Sistema");
- Recolher os pontos fortes e fracos sobre o sistema;
- Obter reações e intenções sobre a utilização da aplicação.

5.2.2 Procedimento

Foram realizadas dez sessões individuais presenciais, cada uma com um elemento facilitador, responsável por auxiliar e analisar o desempenho do participante na interação com aplicação *SmartIDR*, e um anotador (*vide* Apêndice C: Guião – Testes de Usabilidade). Estas sessões decorreram nas instalações da Faculdade de Ciências da Universidade de Lisboa (Portugal) e tiveram uma duração aproximada de quarenta minutos. Para posterior análise procedeu-se, com autorização dos participantes, à sua gravação em ficheiro áudio.

Foram utilizados os seguintes dispositivos: *smartphone Huawei* ALE-L21, com sistema operativo *Android* 5.0.1, e *smartwatch Moto 360* com sistema operativo *Android Wear* 1.4.0.

Como critérios de seleção dos participantes, procurou-se ir ao encontro das características de um utilizador comum de *smartphone*, privilegiando-se a diversidade sociopro-fissional, nomeadamente em termos de conhecimentos no ramo das tecnologias da informação e comunicação.

Cada uma das sessões teve início com a apresentação da aplicação *SmartIDR*; apresentaram-se os objetivos do estudo e procedeu-se à recolha dos dados identificativos (*vide* Apêndice B: Formulário – Dados Identificativos).

Os testes foram compostos por tarefas, pré-definidas, representativas da utilização que o *SmartIDR* poderá vir a ter e contemplaram uma bateria de dez tarefas, sete das quais (1 a 7) foram executadas no *smartphone* e as restantes três (8 a 10) com recurso ao *smartwatch* (*vide* Apêndice D: Formulário – Tarefas Testes de Usabilidade).

O participante foi informado que o tempo gasto para completar cada tarefa seria medido e que deveria fornecer *feedback*, em voz alta (*think aloud*), da interação com o *SmartIDR*.

Seguidamente, passou-se à aplicação dos testes de usabilidade atendendo aos seguintes parâmetros: o participante deveria realizar as tarefas sugeridas de modo autónomo, tendo sido feito o registo da execução com sucesso/insucesso do conjunto das tarefas propostas e a cronometragem do tempo utilizado para as completar.

Após a conclusão dos testes de usabilidade, o participante preencheu a "Escala de Usabilidade do Sistema" – *System Usability Scale* (SUS) (*vide* Apêndice E: Avaliação – Escala de Usabilidade do Sistema) [8]. Com recurso a uma pequena entrevista semiestruturada (*debriefing*), recolheram-se dados qualitativos relacionados com os pontos fortes e pontos fracos (*vide* Apêndice C: Guião – Testes de Usabilidade), reações e intenções sobre a utilização futura do *SmartIDR*. No final da secção são apresentados os resultados e as conclusões extraídas.

5.2.3 Participantes

O estudo contou com a colaboração de dez participantes, oito do género masculino e dois do género feminino, com idades entre os 22 e os 35 anos ($\bar{x} \approx 26$, $s \approx 4$). Estes elementos foram recrutados na Faculdade de Ciências da Universidade de Lisboa (Portugal) – Tabela 5.2.

Partici-pante	**Género**	**Idade**	**Habilita-ções Literárias**	**Profissão**	**Disposi-tivo(s) Móvel(eis)**	**Sistema(s) Operativo(s) do(s) *Smartphone(s)***	**Método(s) de Autenticação no(s) *Smartphone(s)***
P1	Feminino	24	Licenciatura	Estudante	*Smartphone* e *Tablet*	*Android*	*Knock Code*
P2	Masculino	23	Licenciatura	Estudante	*Smartphone* e *Tablet*	*Android* e *Windows Phone*	Padrão de Desbloqueio *Android*
P3	Masculino	25	Mestrado	Estudante	*Smartphone*	*Android*	Nenhum
P4	Masculino	27	Mestrado	Estudante	*Smartphone*	*Android*	Padrão de Desbloqueio *Android* e PIN
P5	Feminino	22	Licenciatura	Estudante	*Smartphone*	*Android*	Nenhum
P6	Masculino	27	Mestrado	Estudante	*Smartphone* e *Tablet*	*iOS* e *Windows Phone*	Nenhum
P7	Masculino	25	Licenciatura	Estudante	*Smartphone* e *Tablet*	*iOS*	PIN e Impressão Digital
P8	Masculino	22	12º Ano (Ensino Secundário)	Estudante	*Smartphone*	*Android*	Padrão de Desbloqueio *Android*
P9	Masculino	30	Mestrado	Investiga-dor	*Smartphone*, *Tablet* e *Smartwatch*	*iOS*	PIN
P10	Masculino	35	Mestrado	Investiga-dor	*Smartphone* e *Tablet*	*Android*	PIN

Tabela 5.2: Caracterização dos participantes dos testes de usabilidade.

5.2.4 Resultados

Avaliação – Testes de usabilidade

As conclusões a seguir expostas baseiam-se na análise dos resultados, evidenciados na Tabela 5.3 – taxa de sucesso – e na Tabela 5.4 – tempo de execução das tarefas – e ainda nas informações recolhidas nas gravações de áudio.

Valores expressos em percentagem

Tarefa	**Tarefa 1**	**Tarefa 2**	**Tarefa 3**	**Tarefa 4**	**Tarefa 5**	**Tarefa 6**	**Tarefa 7**	**Tarefa 8**	**Tarefa 9**	**Tarefa 10**
Taxa de Sucesso	100	70	100	100	90	70	100	100	100	100

Tabela 5.3: Taxa de sucesso na execução das tarefas.

As Tarefas 1, 3, 4, 7, 8, 9 e 10 foram executadas com sucesso. Contudo, as Tarefas 4 (Visualizar o relatório de intrusão) e 8 (Monitorizar, no *smartwatch*, as atividades efetuadas no *smartphone* e, no momento em que fosse aberta a aplicação *Facebook*, ativar a resposta "*Bloquear*"), embora tenham suscitado dúvidas a dois e a três participantes respetivamente, foram efetuadas corretamente.

Na Tarefa 2 (Ativar o "*Modo de Ativação Rápida*"), três dos participantes presumiram que esta tarefa estaria implícita na execução da anterior (Tarefa 1 – Configurar o "*Modo de Ativação Rápida*"), não a tendo concluído com sucesso. A taxa de sucesso de 70% pode indiciar algum conflito na sequência lógica das tarefas de configuração e de ativação deste modo.

Verificamos que a taxa de sucesso de 90% alcançada na Tarefa 5 (Configurar no "*Modo de Partilha Controlada*" a resposta "*Ocultar Álbuns de Fotografias*") reflete as dificuldades sentidas por um dos participantes quanto à compreensão da tarefa que foi proposta.

Na Tarefa 6 (Ativar discretamente o "*Modo de Partilha Controlada*" através do *smartwatch*) a taxa de sucesso foi de 70%, que reflete os três elementos que não taparam corretamente o sensor de luminosidade do *smartwatch*. No entanto, a demonstração posterior de como este mecanismo deveria ter sido ativado permitiu que, na tarefa subsequente, este procedimento fosse concretizado de forma correta.

As taxas de sucesso alcançadas permitiram concluir que o sistema é eficaz, na medida em que, de uma forma geral, os participantes concretizaram o conjunto de tarefas propostas.

Valores expressos em segundos

Participante	Tarefa 1	Tarefa 2	Tarefa 3	Tarefa 4	Tarefa 5	Tarefa 6	Tarefa 7	Tarefa 8	Tarefa 9	Tarefa 10
P1	10,6	27,4	11,9	43	34,1	–	3,2	20,4	6,5	1,5
P2	22,5	12,7	10,7	30,8	20,9	–	3,0	16,6	7,8	2,2
P3	13,3	9,4	12,0	29,9	18,6	7,5	3,9	21,4	5,7	1,6
P4	14,6	9,5	15,3	47,1	28,2	4,1	5,7	11,0	10,3	4,6
P5	15,3	14,4	11,5	84,1	–	6,8	5,3	18,3	12,7	1,5
P6	15,4	30,5	13,6	39,6	37,9	–	10,8	17,3	7,0	3,6
P7	13,1	–	11,4	22,5	18,2	7,3	3,3	13,7	17,8	4,6
P8	14,9	11,6	14,6	21,5	17,7	6,5	8,4	17,7	4,2	2,6
P9	16,6	–	10,9	29,1	25,4	13,3	4,9	18,3	4,6	2,3
P10	11,6	–	14,4	31,0	25,1	6,9	5,4	17,0	14,6	2,7
Média	14,8	16,5	12,6	37,9	25,1	7,5	5,4	17,2	9,1	2,7
Desvio Padrão	3,3	8,7	1,7	18,2	7,2	2,8	2,5	3,0	4,6	1,2

Tabela 5.4: Tempo de execução das tarefas.

Relativamente ao tempo utilizado na realização das tarefas, assinalamos que as tarefas cujo tempo não está assinalado se referem às que não foram concluídas.

Da análise dos tempos de execução, concluímos que a Tarefa 4, apesar da reduzida complexidade, registou um tempo médio (37,9) de execução superior. O maior desvio-padrão (18,2) pode ser explicado pelo facto de estes participantes terem tido dúvidas sobre

qual dos itens – "*Início do Registo Atividades*" ou "*Fim do Registo Atividades*" – deveriam selecionar de modo a poderem identificar a atividade mais recente e a mais antiga.

Os desvios-padrão das Tarefas 2 e 5 (8,7 e 7,2 respetivamente) decorreram do facto de dois elementos selecionarem os "álbuns" individualmente em vez de, como seria expectável, utilizarem o botão "*Todos*" que lhes permitiria marcar rapidamente todos os álbuns (na configuração dos modos "*Sem Ligação*" e de "*Partilha Controlada*").

O tempo registado na execução das restantes tarefas – 7/10 – aproximou-se do tempo médio (considerado como tempo de referência).

Os tempos de execução aproximaram-se do tempo de referência (tempo médio), o que nos permite concluir que o sistema é eficiente, na medida em que a maioria dos participantes executaram o conjunto de tarefas no tempo adequado.

Avaliação – Grau de satisfação

Após a conclusão dos testes de usabilidade e, conforme mencionado anteriormente, para avaliar o grau de satisfação do participante, utilizámos a escala SUS[7] [10], constituída por 10 afirmações (com questões de resposta fechada – alternando questões positivas e negativas) numa escala do tipo *Likert* com 5 pontos (em que 1 corresponde a – Discordo Totalmente e o 5 a – Concordo Totalmente).

A Tabela 5.5 evidencia as percentagens das respostas para cada afirmação e a medida de localização Moda (M_o).

Valores expressos em %

Afirmação	1 Discordo Totalmente	2	3	4	5 Concordo Totalmente	M_o
1. Penso que gostaria de usar este sistema frequentemente.	0	0	20	70	10	4
2. Considerei o sistema desnecessariamente complexo.	70	20	10	0	0	1
3. Considerei que o sistema foi fácil de utilizar.	0	0	10	70	20	4
4. Penso que iria precisar do suporte de alguém especializado para poder usar este sistema.	50	30	10	0	10	1
5. Considerei que as várias funcionalidades do sistema estavam bem integradas.	0	0	10	70	20	4
6. Considerei que havia demasiada inconsistência neste sistema.	80	20	0	0	0	1
7. Imagino que a maioria das pessoas iria aprender a usar este sistema rapidamente.	0	0	30	40	30	4
8. Considerei o sistema muito incómodo de utilizar.	90	10	0	0	0	1
9. Senti-me muito confiante ao utilizar o sistema.	0	0	20	50	30	4
10. Precisaria de aprender muitas coisas antes de me poder habituar a este sistema.	50	20	30	0	0	1

Tabela 5.5: Descrição dos resultados quantitativos – SUS.

[7] Tradução própria.

Da análise da Moda, concluímos que as respostas para todas as afirmações positivas estão localizadas na pontuação 4, enquanto para todas as afirmações negativas se encontram na pontuação 1. Assim, a maioria dos participantes não considerou o sistema complexo, inconsistente ou incómodo de utilizar (afirmações 2, 6 e 8), indicou não ser necessário o suporte de "alguém" especializado ou de algum tipo de aprendizagem prévia (afirmações 4 e 10), gostaria de o utilizar, considerou fácil a sua utilização, com as funcionalidades bem integradas, acessível a qualquer tipo de utilizador e sentiu-se confiante ao utilizá-lo (afirmações 1, 3, 5, 7 e 9).

A pontuação média obtida no questionário SUS foi de 82,25 (numa escala de 0 a 100 pontos), com um desvio padrão de 8,84. Esta pontuação permite concluir que a satisfação dos participantes foi positiva. Uma pontuação entre 71,4 e 85,5 [8] é um indicador positivo da satisfação dos participantes com o sistema em termos de usabilidade, correspondente ao intervalo entre o "*Bom*" e o "*Excelente*", respetivamente.

Na etapa final foi realizada uma entrevista semiestruturada com cada participante (*vide* Apêndice C: Guião – Testes de Usabilidade), com o objetivo de recolher os pontos fortes e fracos sobre o sistema e o potencial de utilização da aplicação.

Todos os participantes responderam às questões colocadas que, depois de analisadas conjuntamente com as reações obtidas no registo de áudio (*think aloud*), foram compiladas e sintetizadas. Estas respostas foram analisadas, tendo-se extraído as informações mais relevantes abaixo descritas.

Pontos Fortes vs. Pontos Fracos

Pontos fortes do sistema:

- A sua interface é bastante consistente;
- Tem uma interface simples e intuitiva;
- Contém muitas funcionalidades interessantes;
- O "*Modo de Resposta em Tempo Real*" é uma vantagem acrescida;
- O "*Modo de Ativação Rápida*" é uma solução muito positiva para quem não tem *smartwatch*;
- O botão para ativar o "*Modo de Partilha Controlada*" é uma boa alternativa ao mecanismo de ativação discreto;
- É uma boa aposta para quem não tem paciência para configurações;

- Utilizaria as funcionalidades "*Registar Atividades*" e "*Fotografar Intruso*" para saber quem tinha acedido ao meu *smartphone*;
- A execução em *background* é vantajosa por não interferir com a utilização do *smartphone*;
- Os meus filhos estão sempre a jogar no meu *smartphone* e receio que eliminem os contactos. Com o *SmartIDR* esta situação não ocorreria;
- Esta aplicação resolveria os meus problemas, porque às vezes esqueço-me de o guardar na mala e deixo-o na secretária quando vou a outra sala;
- Esta aplicação resolveria os meus problemas, pois costumo partilhar muitas vezes o meu *smartphone*;
- Ficaria menos preocupado em relação à segurança dos dados que armazeno;
- Com o *SmartIDR* não ficaria obrigado a estar próximo da outra pessoa quando partilhasse o *smartphone*;
- A possibilidade de impedir o acesso aos meus dados sensíveis no *smartphone* sem que a outra pessoa se aperceba é bastante útil e não causa embaraço.

Pontos fracos do sistema:

- Os registos de atividades deveriam ter divisórias visuais a separá-los;
- Os registos de atividades contêm demasiada informação o que os torna confusos;
- A sequência entre a configuração e a ativação do "*Modo de Ativação Rápida*" não é muito intuitiva;
- Tive algumas dificuldades com o mecanismo discreto de ativação do "*Modo de Partilha Controlada*".

Os participantes consideraram que o *SmartIDR* seria bastante útil para a segurança e privacidade dos seus dados, pelo que a sua utilização seria uma vantagem e uma boa solução a adotar no futuro.

Quando questionados sobre a possibilidade de recomendarem a aplicação a outras pessoas, todos os participantes afirmaram que, pela sua utilidade, a aconselhariam a pessoas próximas do seu círculo social, nomeadamente àquelas que tenham dados sensíveis ou que se preocupem com questões de segurança e privacidade. Mencionaram, ainda, as pessoas que por razões profissionais, por exemplo, têm de utilizar os *smartphones* em locais públicos, estando expostas a maiores riscos, assim como as pessoas que têm menor consciência das vulnerabilidades a que poderão estar expostas.

5.3 Apreciação Crítica

Neste capítulo foi apresentado um resumo alargado dos procedimentos utilizados e dos resultados da avaliação quantitativa e qualitativa do sistema de deteção e resposta a intrusões (*SmartIDR*).

As contribuições dos grupos de foco foram bastante profícuas, na medida em que nos permitiram, por um lado, constatar que o *SmartIDR* responde às necessidades sentidas pelos utilizadores quanto à segurança e privacidade dos dados que armazenam nos seus *smartphones* e, por outro, com base nas informações recolhidas, refinarmos a aplicação de forma a ir ao encontro das expetativas dos potenciais utilizadores.

Após a implementação de seis propostas de melhoria, foram realizados os testes de usabilidade que permitiram avaliar a extensão em que a aplicação pode ser utilizada por utilizadores específicos, para atingir objetivos específicos com eficácia, eficiência e satisfação num contexto específico de uso [29].

Esta avaliação permitiu concluir que o sistema foi considerado eficaz e eficiente. Os valores alcançados (entre os 70% e os 100%) evidenciaram que as tarefas propostas foram executadas, na generalidade, com sucesso. A aproximação dos tempos de execução aos tempos médios de referência demonstrou também que os utilizadores realizaram o conjunto de tarefas no intervalo de tempo aceitável.

A pontuação de 82,25 (numa escala de 0 a 100 pontos), obtida no questionário SUS, indicou que o nível de satisfação dos utilizadores com o sistema se situou entre "*Bom*" e "*Excelente*".

No que concerne às opiniões e reações, concluímos que tendencialmente foram realçados os pontos fortes do sistema. Embora a usabilidade tenha sido avaliada de forma positiva, este estudo permitiu identificar oportunidades de melhoria, que contribuirão para maximizar a sua usabilidade e potenciar a sua viabilidade no futuro.

Assim, concluímos que esta aplicação será útil, na medida em que responde às necessidades de segurança da informação e de privacidade dos utilizadores de *smartphones*, com eficácia, eficiência e com um nível de satisfação bastante positivo.

Capítulo 6

Conclusões

A evolução dos dispositivos móveis pessoais, em particular dos *smartphones*, originou o crescimento de adversários que, ao explorarem as mais diversas vulnerabilidades, ameaçam a segurança da informação e a privacidade dos utilizadores.

A área da segurança tem desenvolvido esforços consideráveis com os sistemas de segurança da informação contra riscos como o *malware* ou roubo/perda. No entanto, estes riscos, por não estarem direcionados a um alvo/pessoa concreta, não são percecionados pelo utilizador comum como tão prejudicais, quando comparados com as ameaças perpetradas por pessoas socialmente próximas.

Os métodos de autenticação são uma barreira contra o acesso indevido aos dispositivos móveis. Porém, os utilizadores tendem a não os adotar se o esforço exigido comprometer a sua usabilidade ou a optar por métodos fracos potencialmente vulneráveis a ataques de observação. Acresce ainda assinalar que a barreira de autenticação é ultrapassada quando o dispositivo é partilhado.

Esta dissertação apresenta o *SmartIDR*, um sistema de deteção e resposta a intrusões físicas em *smartphones* que, através de um dispositivo secundário – *smartwatch* –, permite, por um lado, integrar e aceder rapidamente à informação, monitorizar as atividades ocorridas no *smartphone*, e por outro, responder remotamente e em tempo real a situações de ameaça.

O *SmartIDR* foi concebido para *smartphones* e *smartwatches* com o sistema operativo *Android* e *Android Wear*, respetivamente. Os diferentes mecanismos para deteção e resposta a intrusões físicas foram estruturados com base nas características de comunicação *Bluetooth*.

Assim, quando os dispositivos não têm ligação *Bluetooth* (estão afastados), o sistema ativa automaticamente no *smartphone* o mecanismo de respostas a intrusões; quando têm

ligação (estão próximos), o utilizador, ao monitorizar em tempo real as atividades efetuadas no *smartphone*, pode optar por ativar discretamente no *smartwatch* um conjunto de respostas previamente configurado, ou ativar uma resposta específica em consonância com a ocorrência.

Para maximizar o sucesso do nosso sistema e identificar eventuais problemas, recorremos aos métodos baseados em grupos de foco e testes de usabilidade para avaliar a nossa solução. Assim, numa primeira fase, com recurso aos grupos de foco, os resultados obtidos demonstraram que o *SmartIDR* responde às necessidades de segurança e privacidade que os utilizadores têm relativamente aos dados sensíveis que armazenam nos seus *smartphones*. Os problemas identificados e as sugestões de melhoria permitiram-nos refinar a aplicação.

Numa segunda fase, foram realizados testes de usabilidade. Os resultados obtidos demonstraram que o sistema se revelou eficaz, eficiente e o nível de satisfação dos utilizadores foi bastante positivo.

Como conclusão, o *SmartIDR* caracteriza-se por ter uma interface intuitiva, ser acessível a utilizadores comuns, ser fácil de configurar, permitir a partilha segura e espontânea, disponibilizar um leque alargado de mecanismos de respostas adequadas a diferentes contextos e não comprometer a usabilidade dos dispositivos. Mais do que um sistema, o *SmartIDR* é um novo paradigma de segurança e de privacidade para dispositivos móveis pessoais que cada vez mais fazem parte integrante da nossa vida e se tornaram já uma extensão de nós próprios.

6.1 Trabalho Futuro

O trabalho futuro tem como alvo os problemas de usabilidade que foram identificados, no sentido de alargar o âmbito da aplicação, a análise do desempenho, o enquadramento legal e o impacto da aplicação na *Google Play Store*.

- Solucionar os problemas identificados nos testes de usabilidade:
    - Implementar, no menu inicial da aplicação do *smartphone*, separadores (e.g., com cores distintas ou com cabeçalhos de secção) para cada um dos relatórios de intrusão gerados;
    - Disponibilizar, num tutorial, a demonstração do mecanismo de ativação inconspícua do "*Modo de Partilha Controlada*".
- Alargar o âmbito da aplicação:

  - Incluir outros dispositivos *wearable* – explorar as potencialidades de outros *wearable* como dispositivos para deteção e resposta a intrusões que possam levar à criação de novas alternativas;
  - Expandir o leque de respostas a intrusão – recomenda-se a inclusão de novos *plug-ins* de resposta a intrusão para cenários não contemplados na aplicação;
  - Mecanismos de ativação inconspícua – propõe-se que sejam explorados novos mecanismos de ativação inconspícua recorrendo a outros sensores do *smartwatch* (e.g., o acelerómetro ou o giroscópio) e/ou permitindo que o utilizador personalize este mecanismo.

- Enquadramento legal – sugere-se a avaliação do impacto da utilização abusiva (fotografar, registar e/ou monitorizar as atividades do intruso sem o seu consentimento e conhecimento) atentatória dos direitos, liberdades e garantias da privacidade dos cidadãos;
- Avaliação do desempenho da aplicação – sugere-se a avaliação da utilização dos recursos dos dispositivos como o consumo de bateria e o armazenamento de dados;
- Análise do potencial da aplicação – propõe-se a publicação da aplicação na *Google Play Store* para validação longitudinal de utilização e impacto em ambiente real.

Acrónimos

API – Application Programming Interface.

CPU – Central Processing Unit.

HIDS – Host based Intrusion Detection System.

IDRS – Intrusion Detection and Response System.

NIDS – Network based Intrusion Detection System.

PIN – Personal Identification Number.

***SmartIDR* –** Smart Intrusion Detection and Response.

SMS – Short Message Service.

SUS – System Usability Scale.

XML – eXtensible Markup Language.

Bibliografia

[1] Alice, I. (2003). Biometric recognition: Security and privacy concerns. *IEEE Security & Privacy*.

[2] Amruth, M. D., & Praveen, K. (2016). Android Smudge Attack Prevention Techniques. In *Intelligent Systems Technologies and Applications* (pp. 23-31). Springer International Publishing.

[3] Anderson, M. (6). facts about Americans and their smartphones. *Pew Research Center Fact Tank: News in the Numbers*. `http://www.pewresearch.org/fact-tank/2015/04/01/6-facts-about-americans-and-their-smartphones/` [Online; acedido 10-Fevereiro-2016].

[4] Anuar, N. B., Papadaki, M., Furnell, S., & Clarke, N. (2010, August). An investigation and survey of response options for Intrusion Response Systems (IRSs). In *2010 Information Security for South Africa* (pp. 1-8). IEEE.

[5] Ashoor, A. S., & Gore, S. (2011, July). Difference between Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). In *International Conference on Network Security and Applications* (pp. 497-501). Springer Berlin Heidelberg.

[6] Aviv, A. J., Gibson, K., Mossop, E., Blaze, M., & Smith, J. M. (2010). Smudge Attacks on Smartphone Touch Screens. *WOOT*, *10*, 1-7.

[7] Bace, R. G. (2000). *Intrusion detection*. Sams Publishing.

[8] Bangor, A., Kortum, P., & Miller, J. (2009). Determining what individual SUS scores mean: Adding an adjective rating scale. *Journal of usability studies*, *4*(3), 114-123.

[9] Ben-Asher, N., Kirschnick, N., Sieger, H., Meyer, J., Ben-Oved, A., & Möller, S. (2011, August). On the need for different security methods on mobile phones. In *Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services* (pp. 465-473). ACM.

[10] Brooke, J. (2013). SUS: a retrospective. *Journal of usability studies*, *8*(2), 29-40.

[11] Cherapau, I., Muslukhov, I., Asanka, N., & Beznosov, K. (2015). On the impact of touch id on iphone passcodes. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)* (pp. 257-276).

[12] Chin, E., Felt, A. P., Sekar, V., & Wagner, D. (2012, July). Measuring user confidence in smartphone security and privacy. In *Proceedings of the Eighth Symposium on Usable Privacy and Security* (p. 1). ACM.

[13] Crawford, H., Renaud, K., & Storer, T. (2013). A framework for continuous, transparent mobile device authentication. *Computers & Security*, *39*, 127-136.

[14] De Luca, A., & Lindqvist, J. (2015). Is Secure and Usable Smartphone Authentication Asking Too Much?. *IEEE Computer*, *48*(5), 64-68.

[15] Developers, A. (2013). Android, the world's most popular mobile platform. *Google, USA*. `https://developer.android.com/about/android.html`. [Online; acedido 10-Abril-2016].

[16] Developers, A. (2014). Storage Options. `https://developer.android.com/guide/topics/data/data-storage.html`. [Online; acedido 3-Maio-2016].

[17] Developers, A. (2014). Controlling the Camera. `https://developer.android.com/training/camera/cameradirect.html`. [Online; acedido 18-Maio-2016].

[18] Dunphy, P., Heiner, A. P., & Asokan, N. (2010, July). A closer look at recognition-based graphical passwords on mobile devices. In *Proceedings of the Sixth Symposium on Usable Privacy and Security* (p. 3). ACM.

[19] Egelman, S., Jain, S., Portnoff, R. S., Liao, K., Consolvo, S., & Wagner, D. (2014, November). Are you ready to lock?. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (pp. 750-761). ACM.

[20] Felt, A. P., Finifter, M., Chin, E., Hanna, S., & Wagner, D. (2011, October). A survey of mobile malware in the wild. In *Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices* (pp. 3-14). ACM.

[21] Felt, A. P., Egelman, S., & Wagner, D. (2012, October). I've got 99 problems, but vibration ain't one: a survey of smartphone users' concerns. In *Proceedings of the second ACM workshop on Security and privacy in smartphones and mobile devices* (pp. 33-44). ACM.

[22] Ghorbanian, M., Shanmugam, B., Narayansamy, G., & Idris, N. B. (2013, April). Signature-based hybrid Intrusion detection system (HIDS) for android devices. In *Business Engineering and Industrial Applications Colloquium (BEIAC), 2013 IEEE* (pp. 827-831). IEEE.

[23] Hang, A., Von Zezschwitz, E., De Luca, A., & Hussmann, H. (2012, October). Too much information!: user attitudes towards smartphone sharing. In *Proceedings of the 7th Nordic Conference on Human-Computer Interaction: Making Sense Through Design* (pp. 284-287). ACM.

[24] Hang, A., Von Zezschwitz, E., De Luca, A., & Hussmann, H. (2014, May). FaceProfiles: Inconspicuous, Private and Secure Mobile Device Sharing. In *CHI'14 Workshop on Inconspicuous Interaction*. ACM.

[25] Harbach, M., von Zezschwitz, E., Fichtner, A., De Luca, A., & Smith, M. (2014). It's a hard lock life: A field study of smartphone (un)locking behavior and risk perception. In *Symposium On Usable Privacy and Security (SOUPS 2014)* (pp. 213-230).

[26] Harbach, M., De Luca, A., & Egelman, S. (2016, May). The Anatomy of Smartphone Unlocking: A Field Study of Android Lock Screens. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (pp. 4806-4817). ACM.

[27] Heady, R., Luger, G. F., Maccabe, A., & Servilla, M. (1990). *The architecture of a network level intrusion detection system*. University of New Mexico. Department of Computer Science. College of Engineering.

[28] ISO, W. (1998). 9241-11. Ergonomic requirements for office work with visual display terminals (VDTs). *The international organization for standardization*, *45*.

[29] Kainda, R., Flechais, I., & Roscoe, A. W. (2010, February). Security and usability: Analysis and evaluation. In *Availability, Reliability, and Security, 2010. ARES'10 International Conference on* (pp. 275-282). IEEE.

[30] Karlson, A. K., Brush, A. J., & Schechter, S. (2009, April). Can I borrow your phone?: understanding concerns when sharing mobile phones. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 1647-1650). ACM.

[31] Kruegel, C., Valeur, F., & Vigna, G. (2005). Computer security and intrusion detection. *Intrusion Detection and Correlation: Challenges and Solutions*, 9-28.

[32] Li, F., Clarke, N. L., & Papadaki, M. (2008). Intrusion Detection System for Mobile Devices: Preliminary Investigation. In *Proceedings of the Fourth Collaborative Research Symposium on Security, E-learning, Internet and Networking, Glyndwr University, Wrexham, 6-7 November 2008* (p. 21). Lulu.com.

[33] Li, F., Clarke, N. L., & Papadaki, M. (2009, April). Intrusion detection system for mobile devices: investigation on calling activity. In *Proceedings of the 8th Security Conference, April, Las Vegas, USA*.

[34] Liu, Y., Rahmati, A., Huang, Y., Jang, H., Zhong, L., Zhang, Y., & Zhang, S. (2009, June). xShare: supporting impromptu sharing of mobile phones. In *Proceedings of the 7th international conference on Mobile systems, applications, and services* (pp. 15-28). ACM.

[35] Marques, D., Guerreiro, T., & Carriço, L. (2014, April). Measuring snooping behavior with surveys: it's how you ask it. In *CHI'14 Extended Abstracts on Human Factors in Computing Systems* (pp. 2479-2484). ACM.

[36] Marques, D., Muslukhov, I., Guerreiro, T., Carriço, L., & Beznosov, K. (2016). Snooping on Mobile Phones: Prevalence and Trends. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*.

[37] Mednieks, Z., Dornin, L., Meike, G. B., & Nakamura, M. (2012). *Programming android*." O'Reilly Media, Inc.".

[38] Muslukhov, I. (2012). Survey: Data Protection in Smartphones Against Physical Threats. *Term Project Papers on Mobile Security. University of British Columbia*.

[39] Muslukhov, I., Boshmaf, Y., Kuo, C., Lester, J., & Beznosov, K. (2012, April). Understanding users' requirements for data protection in smartphones. In *Data Engineering Workshops (ICDEW), 2012 IEEE 28th International Conference on* (pp. 228-235). IEEE.

[40] Muslukhov, I., Boshmaf, Y., Kuo, C., Lester, J., & Beznosov, K. (2013, August). Know your enemy: the risk of unauthorized access in smartphones by insiders. In *Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services* (pp. 271-280). ACM.

[41] Ragsdale, D. J., Carver, C. A., Humphries, J. W., & Pooch, U. W. (2000). Adaptation techniques for intrusion detection and intrusion response systems. In *Systems, Man, and Cybernetics, 2000 IEEE International Conference on* (Vol. 4, pp. 2344-2349). IEEE.

[42] Roth, V., Richter, K., & Freidinger, R. (2004, October). A PIN-entry method resilient against shoulder surfing. In *Proceedings of the 11th ACM conference on Computer and communications security* (pp. 236-245). ACM.

[43] Riva, O., Qin, C., Strauss, K., & Lymberopoulos, D. (2012). Progressive authentication: deciding when to authenticate on mobile phones. In *Presented as part of the 21st USENIX Security Symposium (USENIX Security 12)* (pp. 301-316).

[44] Schechter, S., & Bonneau, J. (2015). Learning assigned secrets for unlocking mobile devices. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)* (pp. 277-295).

[45] Sen, S., & Clark, J. A. (2009). Intrusion detection in mobile ad hoc networks. In *Guide to wireless ad hoc networks* (pp. 427-454). Springer London.

[46] Shabtai, A., Fledel, Y., Kanonov, U., Elovici, Y., & Dolev, S. (2009). Google android: A state-of-the-art review of security mechanisms. *arXiv preprint arXiv:0912.5101*.

[47] Shabtai, A., Kanonov, U., Elovici, Y., Glezer, C., & Weiss, Y. (2012). "Andromaly": a behavioral malware detection framework for android devices. *Journal of Intelligent Information Systems*, *38*(1), 161-190.

[48] Shirey, R. (2000). RFC 2828: Internet security glossary. *The Internet Society*, 13.

[49] Spanceski, F. R. (2004). Politica de segurança da informação – Desenvolvimento de um modelo voltado para instituições de ensino. *Instituto Superior de Tupy–Joinville, SC–Brasil–Trabalho de Conclusão de Curso em Sistemas de Informação*.

[50] Sun, B., Yu, F., Wu, K., Xiao, Y., & Leung, V. C. (2006). Enhancing security using mobility-based anomaly detection in cellular mobile networks. *IEEE Transactions on Vehicular Technology*, *55*(4), 1385-1396.

[51] Velho, J., Marques, D., Guerreiro, T., & Carriço, L. Physical Intrusion Detection and Prevention for Android Smartphones.

[52] Von Zezschwitz, E., & Hang, A. (2012). Towards Privacy-Aware Mobile Device Sharing. In *4th International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use (IWSSI/SPMU)*.

[53] Wright, S. (2012). The symantec smartphone honey stick project. *Symantec Corporation, Mar*.

[54] Zhang, Y., Xia, P., Luo, J., Ling, Z., Liu, B., & Fu, X. (2012, October). Fingerprint attack against touch-enabled devices. In *Proceedings of the second ACM workshop on Security and privacy in smartphones and mobile devices* (pp. 57-68). AC.

Apêndice A

Guião – Grupos de Foco

Passo 1 (5 minutos) – Abertura da sessão – Explicação aos participantes do objetivo do estudo no qual irão participar.

Pretende-se desenvolver um sistema que permita detetar e responder a intrusões para *smartphones*, através da utilização de um *smartwatch*.

Esta sessão tem como objetivo, através do debate de ideias, conhecer hábitos e medidas de segurança adotados com *smartphones* e, simultaneamente, recolher opiniões sobre a aplicação que será apresentada, bem como testar a sua utilização (intuição, *design*, facilidade de interação).

Esta sessão terá as seguintes etapas:

1ª Preenchimento do formulário com os dados identificativos dos participantes;

2ª Debate sobre as medidas de segurança adotadas na proteção dos dados pessoais, guardados nos *smartphones*;

3ª Debate sobre a partilha de *smartphones*: motivações, cuidados e preocupações;

4ª Demonstração da aplicação *SmartIDR*;

5ª Obter sugestões de melhoria.

Passo 2 (5 minutos) – Entrega do formulário e recolha dos dados identificativos dos participantes.

Exemplo de intrusão – Imaginem uma situação em que alguém acede à vossa informação privada no vosso *smartphone*, sem autorização. Pensem no que essa pessoa poderia fazer para vos prejudicar.

Passo 3 (5 minutos) – Recolha de dados relativos às medidas de segurança adotadas, pelos participantes, para proteção dos dados que guardam nos *smartphones*, anotando os seguintes aspetos:

1. Quais as medidas de segurança utilizadas para protegerem dados sensíveis contra acessos indevidos ao *smartphone* por pessoas próximas.
2. Se já passaram por alguma situação em que uma pessoa próxima tenha acedido, indevidamente, aos dados sensíveis no *smartphone*.

Passo 4 (5 minutos) – Recolha de dados relacionados com a partilha de *smartphones*.

1. Quais as medidas de controlo ou segurança adotadas durante a partilha (e.g., questionar se deixam a outra pessoa manusear "à vontade" o *smartphone* ou se "vigiam" o que a outra pessoa faz, durante a partilha).
2. Se, na situação em que adotam medidas de vigilância/controlo, sentem algum desconforto por esse facto (e.g., têm receio de mostrar desconfiança).

Passo 5 (5 minutos) – Explicar aos participantes os objetivos da aplicação desenvolvida.

Como foi referido inicialmente, o objetivo é o desenvolvimento de um sistema que permita detetar e responder a intrusões em *smartphones*. Para atingir este objetivo é utilizado um *smartwatch* – Porquê um *smartwatch*? Porque está sempre no nosso pulso.

O *smartphone* e o *smartwatch* comunicam entre si, por Bluetooth, quando estão relativamente próximos.

Passo 6 (15 minutos + 10 minutos + 10 minutos) – Apresentação de 3 cenários de intrusões e demonstração da aplicação (deteção e resposta) disponibilizada.

Cenário 1 – Demonstração do "Modo Sem Ligação"

Exemplo de Intrusão:

Um dia fui almoçar, com os meus colegas, a um restaurante numa outra cidade. Saí apressadamente, da sala onde trabalho, e não me apercebi que deixei o meu *smartphone* em cima da secretária.

Está sempre muita gente na sala, incluindo o Diogo. O Diogo utiliza o meu *smartphone*, acede à galeria de fotografias e visualiza o álbum de "Fotografias Privadas".

Como se não bastasse, o Diogo conseguiu aceder e utilizar diversas funcionalidades do *smartphone* sem problemas e sem deixar pistas.

Caso de Uso:

1. O utilizador configura o perfil "*Modo Sem Ligação*", selecionando as opções "*Registar Atividades*" e "*Fotografar Intruso*";
2. O utilizador abandona a sala, deixando o *smartphone* em cima da mesa;
3. Os dispositivos deixam de ter ligação, ou seja, o utilizador não está próximo do seu *smartphone*;
4. O atacante acede ao *smartphone*, acede à galeria de fotografias e acede ao álbum de "*Fotografias Privadas*";
5. O atacante deixa o *smartphone* no seu estado inicial;
6. O utilizador regressa à sala e recebe uma notificação, no *smartphone*, que indica que ocorreu uma intrusão. O utilizador visualiza as atividades e a fotografia do atacante.

Peço que recordem, agora, algumas situações específicas em que esta opção já poderia ter sido útil.

Atendendo à demonstração realizada:

- Que limitações/problemas encontraram?
- Que outras opções de resposta deveriam estar disponíveis?
    - Quais as que considerariam mais úteis e relevantes?

Cenário 2 – Demonstração do "Modo de Partilha Controlada"

Exemplo de Intrusão:

Um dia um professor pediu-me o *smartphone* para consultar a sua conta de *email*.

Como eu não queria revelar uma atitude de desconfiança, que pudesse vir a comprometer a minha imagem, emprestei o *smartphone* ao professor sem qualquer supervisão.

O professor, inadvertidamente, acede às minhas mensagens.

Caso de uso:

1. O utilizador configura o perfil "*Modo de Partilha Controlada*" – (1) seleciona a opção "*Desativar Aplicações*" e seleciona as aplicações "Telefone" e "Mensagens"; (2) seleciona a opção "*Ocultar Álbuns de Fotografias*" e seleciona o álbum "Fotografias Privadas";
2. O utilizador partilha o seu *smartphone* com o atacante e ativa o "*Modo de Partilha Controlada*", de forma discreta, a partir do *smartwatch*;
3. O atacante tenta aceder às aplicações de "Telefone" e de "Mensagens" e visualizar o álbum de fotografias privadas do utilizador, sem sucesso.

Peço que recordem, agora, algumas situações específicas em que esta opção já poderia ter sido útil.

Atendendo à demonstração realizada:

- Que limitações/problemas encontraram?
- Que outras opções de resposta deveriam estar disponíveis?
    - Quais as que considerariam mais úteis e relevantes?

Cenário 3 – Demonstração do "Modo de Resposta em Tempo Real"

Exemplo de Intrusão:

Quando estava a trocar mensagens com o Diogo sobre a organização desta sessão, o meu irmão mais novo tirou-me o *smartphone* e fechou-se no quarto. Apesar de muitas tentativas, não consegui que ele mo devolvesse. O meu irmão enviou várias mensagens ofensivas ao Diogo.

Caso de uso:

1. O atacante apodera-se do *smartphone* sem autorização do utilizador;
2. O utilizador monitoriza as atividades do atacante através do *smartwatch*, selecionando a opção "*Monitorizar Atividades*";
3. O utilizador bloqueia o *smartphone*, através do *smartwatch*, impedindo o seu acesso.

Peço que recordem, agora, algumas situações específicas em que esta opção já poderia ter sido útil.

Atendendo à demonstração realizada:

- Que limitações/problemas encontraram?
- Que outras opções de resposta deveriam estar disponíveis?
    - Quais as que considerariam mais úteis e relevantes?

Passo 7 (15 minutos) – Obter sugestões de melhoria:

- Qual dos três modos da aplicação consideraram mais relevante em termos de utilidade e de segurança? Porquê?
- Qual dos três modos da aplicação consideraram ter uma utilidade mais reduzida? Porquê?

Além das sugestões que já referiram, que outras sugestões úteis e relevantes propõem que sejam incluídas na aplicação?

Apêndice B

Formulário – Dados Identificativos

Participante Nº ☐

Dados Pessoais

Género:

Masculino ☐ Feminino ☐

Idade: _____

Habilitações Literárias: _____

Profissão: _____

Dispositivos Móveis

Que dispositivo(s) móvel(eis) possui:

Smartphone ☐ Tablet ☐ Smartwatch ☐

Que sistema(s) operativo(s) tem no(s) seu(s) smartphone(s):

Android ☐ Windows Phone ☐

iOS ☐ Outro ☐ Qual: _____

Que método(s) de autenticação utiliza no(s) seu(s) smartphone(s):

Nenhum ☐ Padrão Android ☐

PIN ☐ Password ☐

Impressão Digital ☐ Outro ☐ Qual: _____

Apêndice C

Guião – Testes de Usabilidade

Passo 1 – Abertura da sessão – Explicar ao participante o objetivo do estudo.

Perguntar ao participante se aceita que a sessão seja gravada em formato de áudio. Se aceitar, deverá assinar o termo de consentimento.

A aplicação *SmartIDR* permite prevenir, detetar e responder a intrusões em *smartphones*, com recurso a um *smartwatch*. No entanto, a aplicação também pode ser configurada mesmo que o utilizador não possua um *smartwatch*.

Esta sessão tem como objetivo realizar um conjunto de testes de usabilidade (avaliar a facilidade de interação) da aplicação *SmartIDR – Smart Intrusion Detection and Response*.

Exemplo de intrusão – Imagine uma situação em que alguém acede à sua informação privada no seu *smartphone*, sem autorização. Pense no que essa pessoa poderia fazer para o prejudicar.

Esta sessão terá as seguintes etapas:

1ª Preenchimento do formulário com os dados identificativos do participante;

2ª Testes de usabilidade da aplicação no *smartphone*;

3ª Testes de usabilidade da aplicação no *smartwatch*;

4ª Preenchimento da "Escala de Usabilidade do Sistema" para avaliar a satisfação do utilizador;

5ª Entrevista.

Lembre-se de:

- Verbalizar as dúvidas, pois ajudará o avaliador a anotar a ocorrência e à identificação de problemas;
- É o *SmartIDR* que está a ser avaliado e não você.

Passo 2 – Entrega do formulário e recolha dos dados identificativos do participante.

Instruções

O tempo gasto a completar cada tarefa irá ser medido. No início de cada tarefa é lida a sua descrição e o participante deve confirmar se a entendeu. A medição do tempo começa após a confirmação.

O participante poderá usar a aplicação no *smartphone* durante aproximadamente 3 minutos, antes do início dos testes de usabilidade.

Passo 3 – Testes de usabilidade da aplicação no *smartphone*.

"Modo de Ativação Rápida"

Permite configurar rapidamente um conjunto de opções de proteção, sem a utilização do *smartwatch*.

(*vide* Apêndice D: Formulário –Tarefas Testes de Usabilidade)

"Modo Sem Ligação"

Permite, numa situação em que o *smartphone* está fora do seu alcance, ativar um conjunto de opções de proteção previamente configuradas.

(*vide* Apêndice D: Formulário –Tarefas Testes de Usabilidade)

"Modo de Partilha Controlada"

Permite, numa situação em que partilha o *smartphone*, ativar discretamente um conjunto de opções de proteção, previamente configuradas. Poderá fazê-lo tapando três vezes o sensor de luminosidade do *smartwatch*.

(*vide* Apêndice D: Formulário – Tarefas Testes de Usabilidade)

Saber se o participante está familiarizado com a utilização do *smartwatch*. Se não estiver, explicar como funciona.

O participante poderá usar a aplicação no *smartwatch* durante aproximadamente 2 minutos, antes do início dos testes de usabilidade.

Passo 4 – Testes de usabilidade da aplicação no *smartwatch*.

"Modo de Resposta em Tempo Real"

A aplicação também permite, no *smartwatch*, monitorizar as atividades que "alguém" está a realizar no *smartphone* e ativar um conjunto de opções de proteção em tempo real.

(*vide* Apêndice D: Formulário – Tarefas Testes de Usabilidade)

Passo 5 – Entrega e recolha da "Escala de Usabilidade do Sistema" para avaliar a satisfação do utilizador.

Passo 6 – Realização de entrevista (face a face) – recolha de dados qualitativos de acordo com os seguintes tópicos:

1. Qual a sua opinião sobre a interface da aplicação?;
2. Considera o *SmartIDR* uma boa solução para a segurança e privacidade dos dados que armazena no seu *smartphone*?;
3. Descreva as principais dificuldades e problemas associados ao *SmartIDR*;
4. Descreva situações do seu quotidiano em que a aplicação testada lhe poderia ter sido útil;
5. Utilizaria a aplicação *SmartIDR*?;
6. A quem recomendaria a aplicação *SmartIDR*?.

Nota:

Regras para apurar o resultado final do SUS [10]:

1. Nas afirmações com número ímpar (1, 3, 5, 7 e 9) – subtrair 1 à resposta do participante;
2. Nas afirmações com número par (2, 4, 6, 8 e 10) – subtrair a resposta do participante a 5;
3. Somar os resultados obtidos e multiplicar o total por 2,5.

Escala de adjetivação estabelecida por Bangor *et al.* [8] para os resultados do SUS.

Resultado Final da SUS	Desvio Padrão	Adjetivo
90,9	13,4	O Melhor Imaginável
85,5	10,4	Excelente
71,4	11,6	Bom
50,9	13,8	*Ok*
35,7	12,6	Pobre
20,3	11,3	Horrível
12,5	13,1	O Pior Imaginável

Apêndice D

Formulário – Tarefas Testes de Usabilidade

Tarefas testes de usabilidade – Smartphone

Modo	Tarefa	Sucesso (Escolher 1)	Tempo de Execução da Tarefa	Notas/Observações
"*Modo de Ativação Rápida*"	**Tarefa 1 –** Configurar o "*Modo de Ativação Rápida*": <u>Selecionar</u> **1.** "*Ocultar Álbuns de Vídeos*"	0 – Não completou 1 – Completou com dificuldade ou ajuda 2 – Completou		
	Visualizar Galeria			
	Tarefa 2 – Ativar o "*Modo de Ativação Rápida*": <u>Selecionar</u> **1.** Todos os álbuns de vídeos	0 – Não completou 1 – Completou com dificuldade ou ajuda 2 – Completou		
	Verificar Resposta			
"*Modo Sem Ligação*"	**Tarefa 3 –** Configurar o "*Modo Sem Ligação*": <u>Selecionar</u> **1.** "*Registar Atividades*" **2.** "*Fotografar Intruso*"	0 – Não completou 1 – Completou com dificuldade ou ajuda 2 – Completou		
	Simular Intrusão			
	Tarefa 4 – Relatório de Intrusão: <u>Visualizar</u> **1.** A fotografia do intruso <u>Indicar</u> **1.** Atividade mais recente **2.** Atividade mais antiga	0 – Não completou 1 – Completou com dificuldade ou ajuda 2 – Completou		

Modo	Tarefa	Sucesso (Escolher 1)	Tempo de Execução da Tarefa	Notas/Observações
"*Modo de Partilha Controlada*"	**Tarefa 5 –** Configurar o "*Modo de Partilha Controlada*": <u>Selecionar</u> **1.** "*Desativar Aplicações*" – escolher "Mensagens" **2.** "*Ocultar Álbuns de Fotografias*" – todos os álbuns de fotografias	0 – Não completou 1 – Completou com dificuldade ou ajuda 2 – Completou		
	Visualizar Galeria e Aceder à Aplicação "Mensagens"			
	Tarefa 6 – Ativar, discretamente, o "*Modo de Partilha Controlada*" no *smartwatch*	0 – Não completou 1 – Completou com dificuldade ou ajuda 2 – Completou		
	Verificar Resposta			
	Tarefa 7 – Desativar, discretamente, o "*Modo de Partilha Controlada*" no *smartwatch*	0 – Não completou 1 – Completou com dificuldade ou ajuda 2 – Completou		
	Verificar Resposta			

Tarefas testes de usabilidade – Smartwatch

Modo	Tarefa	Sucesso (Escolher 1)	Tempo de Execução da Tarefa	Notas/Observações
"*Modo de Resposta em Tempo Real*"	**Tarefa 8 –** **1.** Monitorizar no *smartwatch* as atividades efetuadas no *smartphone* **2.** Quando a aplicação do *Facebook* for aberta, ativar a resposta "*Bloquear*"	0 – Não completou 1 – Completou com dificuldade ou ajuda 2 – Completou		
	Verificar Resposta			
	Tarefa 9 – <u>Indicar</u> **1.** Qual foi a atividade mais antiga **2.** Há quanto tempo ocorreu	0 – Não completou 1 – Completou com dificuldade ou ajuda 2 – Completou		
	Tarefa 10 – **1.** Desbloquear o *smartphone* através do *smartwatch*	0 – Não completou 1 – Completou com dificuldade ou ajuda 2 – Completou		
	Verificar Resposta			

Apêndice E

Avaliação – Escala de Usabilidade do Sistema

	Discordo Totalmente				Concordo Totalmente
1. Penso que gostaria de usar este sistema frequentemente.	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
2. Considerei o sistema desnecessariamente complexo.	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
3. Considerei que o sistema foi fácil de utilizar.	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
4. Penso que iria precisar do suporte de alguém especializado para poder usar este sistema.	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
5. Considerei que as várias funcionalidades do sistema estavam bem integradas.	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
6. Considerei que havia demasiada inconsistência neste sistema.	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
7. Imagino que a maioria das pessoas iria aprender a usar este sistema muito rapidamente.	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
8. Considerei o sistema muito incómodo de utilizar.	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
9. Senti-me muito confiante ao utilizar o sistema.	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5
10. Precisaria de aprender muitas coisas antes de me poder habituar a este sistema.	☐ 1	☐ 2	☐ 3	☐ 4	☐ 5