Designação do Projeto|	mIDR: Usable Intrusion Detection & Response on Personal Mobile Devices
Código do Projeto|	LISBOA-01-0145-FEDER-030347
Objetivo Principal|	Reforçar a investigação, o desenvolvimento tecnológico e a inovação
Região de Intervenção|	Lisboa
Entidade Beneficiária|	FCiências.ID – Associação para a Investigação e Desenvolvimento de Ciências
Data de Aprovação|	03-05-2018
Data de Início|	01-06-2018
Data de Conclusão|	28-052-2022
Custo Total Elegível|	239.826,13€
Apoio Financeiro da União Europeia|	FEDER – 95.930,45€
Apoio Financeiro Público Nacional/ Regional|	OE – 143.895,68€

Formatada: Inglês (Estados Unidos)

Objetivos

O objetivo deste projeto foi desenvolver e avaliar modos passivos de segurança que possam acomodar as relações sociais entre as partes. Em oposição à autenticação para desbloqueio, que é uma defesa ativa contra acesso físico, as defesas passivas têm como objetivo primário oferecer informação, rastreio e recuperação; e apenas subsidiariamente lançar contramedidas. Para cumprir este objetivo, teve-se como sub-objetivos: 1) caracterizar a ameaça de acesso a dispositivos por pessoas próximas; 2) desenhar e desenvolver um sistema de deteção e resposta a intrusões que acomode as necessidades dos diferentes utilizadores; 3) avaliar a adequação da abordagem com utilizadores finais.

Atividades

Numa etapa formativa, o objetivo foi caracterizar o fenómeno de intrusões em dispositivos móveis por pessoas próximas. Para atingir esse objetivo, realizamos estudos qualitativos para recolher relatos pessoais e reais de intrusões sociais

internas, relatados tanto por vítimas quanto por atacantes. Utilizamos uma abordagem de métodos mistos para analisar os dados, tanto para quantificar quanto para qualificar as intrusões, seus detalhes e consequências. Um resultado importante desses estudos foi a avaliação da gravidade desses ataques, revelando que, na maioria das vezes, causavam um impacto significativo na vida pessoal e nos relacionamentos sociais. Essa caracterização permitiu, conforme planeado, diferenciar a ameaça social do modelo de ameaça normalmente utilizado em segurança da computação.

Baseando-nos nesse conhecimento e conforme delineado na proposta, o projeto visava projetar, desenvolver e avaliar um sistema de deteção e resposta a intrusões (IDR) para dispositivos móveis, baseado em *plug-ins*, que englobaria um conjunto de mecanismos de deteção e resposta, ativos e passivos, capazes de lidar com as idiossincrasias dos contextos sociais. Para atingir esse objetivo, desenvolvemos uma plataforma IDR móvel flexível e extensível que pode ser parametrizada para cada contexto. Em paralelo, construímos mecanismos de recolha de dados para alimentar e informar os outros módulos na plataforma: módulos de deteção móvel para rastrear o uso de aplicativos, informações contextuais de sensores, dinâmica de uso de teclado virtual.

Toda a informação coletada possibilitou o enriquecimento de nossa plataforma com diferentes deteções e respostas ativas e passivas. Primeiramente, explorámos a auditoria de intrusões como uma opção à autenticação. Nessa abordagem, os usuários conseguiam visualizar um registo usável de utilização do seu telemóvel, onde podiam ver aplicações usadas, fotos da câmara frontal, juntamente com uma pontuação automática de possível intrusão (usando reconhecimento facial). Em segundo lugar, desenvolvemos uma solução em que um *smartwatch* funcionaria em conjunto com o telefone móvel para aumentar o controlo do seu utilizador: desenvolvemos mecanismos de deteção onde o telefone poderia alterar sua resposta automaticamente - por exemplo, distância do telefone - ou por solicitação - por exemplo, uma seleção do proprietário ao partilhar o telefone. As respostas também eram diversas, desde bloquear automaticamente o telefone quando afastado do proprietário, simular a perda de bateria, ou até permitir que o proprietário monitorizasse o uso do telefone no relógio. As respostas poderiam ser parametrizadas com diferentes gatilhos contextuais (localização, tempo, distância, uso). Em terceiro lugar, para maximizar as capacidades de registo de utilização e deteção, desenvolvemos um módulo semântico que constrói representações de alto nível a partir de dados de uso de baixo nível.

Para avaliar a viabilidade e usabilidade dessas abordagens, vários estudos com utilizadores foram conduzidos tanto remota quanto presencialmente. Um resultado específico desses estudos foi o uso indesejado que as pessoas consideraram ao serem fornecidas com as ferramentas, como utilizar as ferramentas de registo para monitorizar ou testar a confiança de outra pessoa. O valor de um registo também não

é negligenciável; o aumento da pesquisa em vigilância entre parceiros íntimos chamou a nossa atenção para as preocupações éticas de fornecer ferramentas que poderiam ser prejudiciais em vez de protetoras. Isso mudou a nossa abordagem de registo para detecção, especialmente nos casos comuns de falsificação de identidade

Resultados Esperados / Atingidos

Os principais resultados do projeto foram:

- A caracterização da ameaça de acesso a dispositivos móveis por pessoas próximas;
- Um conjunto de dados anonimizado de histórias reais de acesso não autorizado a dispositivos móveis, contadas por vítimas ou atacantes;
- Uma biblioteca de registo de dados de utilização de telemóveis Android, reutilizável noutros contextos;
- Um teclado Android para estudos de padrões de escrita;
- Conceito e um sistema protótipo de deteção e resposta a intrusões em dispositivos móveis;
- Publicações científicas em algumas das mais relevantes conferências da área de HCI e privacidade usável: CHI, ACSAC, SOUPS, INTERACT.
- Exposição mediática significativa, nacional e internacional, incluindo canais mediáticos de alto impacto como CBS, Daily Show, entre muitos outros.