FICHA DE PROJETO

Acrónimo: Mobitrust

Designação do projeto: Secure Communications for Next-generation PPDR

Código do projeto: CENTRO-01-0247-FEDER-003343

Objetivo Principal: Desenvolvimento de uma plataforma integrada de gestão de segurança para os terminais móveis a usar nas futuras plataformas de comunicação para aplicações de proteção pública e emergência (PPDR: Public Protection and Disaster Relief) de nova geração.

Região de intervenção: Centro (100%)

Promotor Líder: One Source, Consultoria Informática Lda

Copromotores: Instituto Politécnico de Castelo Branco e Instituto de Telecomunicações

Data de aprovação: 2015-10-16

Data de início: 2015-12-01

Data de conclusão: 2018-11-30

Investimento elegível global: 684.026,81 EUR

Apoio financeiro da União Europeia / FEDER: 512.748,20 EUR

Financiamento do IPCB: 152.803,70 EUR

Apoio FEDER (75%)**:** 114.602,77 EUR

Custo elegível: 165.926,77 EUR

Taxa de execução financeira: 108,59%

Investigador Responsável no IPCB: Paulo Marques

Objetivos

O Projeto Mobitrust teve por objetivo investigar e desenvolver uma plataforma de gestão de segurança para a terminais móveis PPDR (Public Protection and Dister Relief) de nova geração, incluindo diversas vertentes: mecanismos de segurança apropriados ao contexto dos *public safety responders*; ambientes de execução segura; ferramentas de gestão e análise forense integradas com as plataformas PPDR; mecanismos de gestão remota de aplicações; reforço da capacidade de *situational awareness* (por meio de sensores ambientais e de biossensores associados aos terminais); e uso controlado de paradigmas BYOD (Bring Your Own Device) em cenários de desastre.

Esta plataforma de gestão de segurança focou-se nos dispositivos móveis a funcionar em sistemas operativos abertos (em especial Android), com o objetivo de permitir tirar partido no contexto PPDR da evolução tecnológica e das economias de escala registadas no mercado de

consumo. Em vez de desenvolver de raiz novos terminais PPDR para LTE (à semelhança do que sucede com terminais TETRA e TETRAPOL), pressupôs que os futuros terminais pudessem reaproveitar componentes de hardware e software dos smartphones comuns, depois de devidamente adaptados. A plataforma de gestão de segurança desenvolvida no Projeto Mobitrust propôs facilitar este processo de adaptação e reaproveitamento, melhorando a privacidade e a segurança destes dispositivos e potenciando a sua utilização nas redes de emergência e segurança civil de próxima geração. Assim, poderia oferecer terminais PPDR com mais capacidades e funcionalidades, com menores custos e com uma evolução tecnológica mais rápida, sem com isso sacrificar os requisitos de segurança, robustez e operacionalidade associados ao domínio PPDR.

O projeto que correspondeu à componente nacional do projeto Europeu Eureka CATRENE/MobiTrust (CA208) http://mobitrust.av.it.pt/ propôs-se consolidar e reforçar a posição de Portugal como ator relevante europeu na economia digital, num domínio de aplicações especializado (comunicações PPDR), onde Portugal não tem ainda uma presença expressiva e com elevado potencial de exportações.

A tecnologia desenvolvida tinha como destino o mercado internacional de fabricantes, integradores e operadores de infraestruturas de comunicações de 'public protection and disaster relief' (PPDR), e agências públicas que trabalhem na área. Entre os objetivos estratégicos do TICE.PT, considerou-se o aumento do peso das TICE no produto nacional, nomeadamente através das exportações de tecnologia avançada.

Atividades/Resultados

Para atingir os **objetivos** propostos foram realizadas as seguintes **atividades**:

A1 – Estudos Preliminares

Esta atividade da responsabilidade do **Instituto Politécnico de Castelo Branco** incidiu sobre as seguintes tarefas:

- Atualização da análise de tecnologias na área do projeto, abarcando diversas vertentes técnicas relevantes para o projeto: tecnologia LTE para suporte de missões criticas (serviços *push-to-talk*); sistemas operativos para terminais móveis para PPDR (identificação de requisitos); ambientes de Execução segura (TEE) para terminais móveis PPDR; soluções de virtualização para dispositivos móveis PPDR; sistemas de deteção de intrusão para terminais móveis PPDR; sistemas de recolha/análise forense para terminais móveis PPDR; soluções de gestão e administração de terminais móveis PPDR.
- Levantamento de vulnerabilidades de segurança aplicáveis no que diz respeito ao acesso não autorizado, manipulação de dados e captura de informação transmitida em cenários PPDR e/ou de execução em ambiente seguro.
- Análise de legislação e processos de certificação relevantes para o contexto da plataforma Mobitrust.

  Esta análise foi concretizada com menor abrangência que inicialmente previsto – por se ter focado essencialmente na legislação nacional e europeia e nas iniciativas de normalização técnica em curso, dado não existirem processos de certificação específicos para esta nova geração de comunicações PPDR, esperando-se que só por volta de 2021 comecem a registar-se iniciativas nesse sentido. Os recursos não utilizados foram realocados por outras tarefas e atividades.

Instituto Politécnico de Castelo Branco

FICHA DE PROJETO

A2 - Especificações Técnicas

Esta atividade realizada pelo Instituto de Telecomunicações consistiu nas seguintes tarefas:

- Análise de Requisitos para a plataforma Mobitrust, considerando Casos de Uso, aspetos de hardware, aspetos de software, requisitos funcionais e requisitos não funcionais, tendo em conta aspetos tais como autenticação biométrica avançada, procedimentos de arranque (*boot*) seguros, ambientes de execução seguros, software de virtualização/*hypervisors*, agentes de monitorização, APIs e integração com a infraestrutura de comunicações PPDR e com o CCC.
- Definição da Arquitetura da Plataforma Mobitrust, incluindo a identificação dos blocos funcionais da arquitetura, dos serviços a suportar, dos módulos de hardware e software a usar e das respetivas interfaces.
- Especificação detalhada dos diversos componentes e interfaces da plataforma Mobitrust, em linha com a arquitetura previamente definida.

A3 - Componentes da Plataforma

- O promotor OneSource dedicou-se ao desenvolvimento dos diversos componentes da plataforma, incluindo mecanismos avançados de autenticação e criptografia, ambientes TEE, integração com sensores e periféricos, mecanismos de recolha e analise de informação forense, aplicações e APIs para integração em Centros de Comando e Controlo (CCC), componentes de integração na infraestrutura de comunicações (e.g. para suporte de mecanismos IDS ao nível de rede e para gestão do ciclo de vida dos terminais), e interfaces de utilizador especializadas em cenários de PPDR.

A4 - Integração e Validação

Nesta atividade a OneSource centrou-se nos seguintes aspetos:

- Integração dos componentes desenvolvidos a montante, na Atividade 3, no protótipo da Plataforma Mobitrust. A primeira versão do protótipo ficou disponível no mês M18, tendo sido depois objetivo de sucessivas melhorias e aumento de funcionalidades ate ao mês M30.
- Preparação do plano de testes.
- Condução dos testes de desempenho, interoperabilidade e funcionalidades da plataforma Mobitrust, de acordo com o plano de testes previamente elaborado.

A5 - Promoção, Disseminação e Exploração dos Resultados

Em termos de divulgação do projeto e dos resultados alcançados a OneSource centralizou as seguintes ações:

- Website do projeto funcional, numa primeira fase com funções de divulgação institucional do projeto (parceiros, visão, objetivos, plano de trabalhos, financiamento público, notícias do projeto, workshops e outros eventos) e no final com uma dupla vertente, mantendo um URL para a vertente institucional e criando um novo URL para exploração comercial da plataforma https://mobitrust-project.onesource.pt/
- Publicação de vários artigos científicos em revistas ISI (2), conferências com revisão de pares (5), e artigos de livro (2), além de um poster e uma apresentação oral.

- Suporte a 2 teses de doutoramento (em vias de conclusão) e uma tese de Mestrado (concluída com sucesso em 2017).
- Preparação de materiais de divulgação do projeto e dos seus resultados, incluindo logotipo e imagem gráfica, diversos *flyers*, vídeo de apresentação, posters roll-up para uso em feiras e outros eventos, faixas para uso em conferencias e stands, etc.
- Reconhecimento público dos méritos do projeto (na sua vertente internacional, por via do consorcio franco-português) com a atribuição do premio *CATRENE Innovation Award*, em dezembro de 2017. Este premio e atribuído anualmente ao projeto EureKa! CATRENE que melhor demonstre um alto nível de inovação, impacto de Mercado, potencial de exploração e benefícios para Europa.
- Organização de 2 workshops dedicados ao projeto, um deles aproveitando a vinda a Portugal dos parceiros internacionais do projeto (projeto Mobitrust CATRENE), com uma primeira apresentação integrada em cenários de PPRD, e outro focado na apresentação da plataforma Mobitrust a *stakeholders* relevantes a nível nacional.
- Presença no Critical Communications Europe 2017 com apresentação oral convidada.
- Presença no Japan IT Week, com apresentação de um poster.
- Presença no *Critical Communications Middle East & North* Africa 2018, com um *stand* dedicado ao projeto Mobitrust.
- Condução de contatos diretos com diversos parceiros potenciais de comercialização da plataforma, incluindo grandes integradores (e.g. Nokia, Gemalto, Airbus), agencias de *lobbying* envolvidas nos processos de *procurement* transeuropeu (PSCE) e potenciais parceiros locais para vendas e suporte no medio oriente, incluindo a participação em processos de *bidding* e a discussão de acordos de colaboração.
- Prémio *CATRENE Innovation Award* 2017 (atribuído ao projeto internacional onde este projeto nacional em copromoção se enquadra).

Para além dos três promotores do projeto, houve uma participação substancial do Instituto Pedro Nunes (IPN) neste processo de divulgação científica, na qualidade de entidade externa contratada pela OneSource. No total, em termos de eventos científicos *peer-reviewed*, registaram-se 2 artigos publicados em revistas ISI, 2 capítulos de livro e 5 artigos em conferencias da área, além de um poster apresentado num evento de carater misto (científico-industrial).

A6 - Gestão Técnica do Projeto

Gestão Técnica do Projeto foi realizada pela OneSource

Execução Financeira do Projeto

Relativamente à execução financeira, registaram-se os seguintes desvios setoriais face previsto e aprovado na candidatura:

- Menor investimento na Atividade 1, devido a menor profundidade com que foi executada a "Analise de Legislação e Processos de Certificação na Área de Projeto", por motivos já enunciados.
- Acréscimos pouco significativos no investimento em pessoal técnico nas Atividades 2, 3 e 4 (sempre abaixo de 3%).

- Acréscimo de 23% na Atividade 5, devido ao um esforço maior que o previsto nas atividades de disseminação e exploração (produção de diversos artigos científicos, preparação dos workshops, produção de vídeos e *flyers* adicionais, preparação de demos para abordagem de potenciais parceiros comerciais, preparação de diversas demos para CCMENA e para os posteriores contatos de *follow-up*, reformulação do website para focar mais a exploração dos resultados, na fase final do projeto).
- Acréscimo de 9% na Atividade 6, devido a extensão do projeto e a inerente necessidade de preparação de mais um relatório intercalar.
- Maior investimento que o previsto em equipamentos (servidores, terminais móveis), devido a variações de preços entre a fase de candidatura e o momento de aquisição e a revisão das especificações técnicas dos servidores a adquirir.
- Menos despesas com viagens que o previsto (25%).
- Mais custos que o previsto com o aluguer e preparação do stand na CCMENA 2018 (acréscimo de 21%).
- Menos despesas que o previsto com TOC/ROC e avaliador na auditoria intercalar.

No que se refere à execução financeira por parte dos promotores salientamos:

- **One Source, Consultoria Informática Lda**

O investimento executado pelo promotor líder foi ligeiramente superior ao previsto (102%). Tendo em conta a natureza das despesas e os desvios em geral pouco significativos, compensaram-se as rúbricas onde o investimento não foi totalmente executado pelas rúbricas onde o investimento excedeu o previsto (e.g. entre viagens e despesas com preparação de stand; entre pessoal técnico da Atividade 1 e pessoal técnico das restantes atividades).

- **IPCB – Instituto Politécnico de Castelo Branco**

O investimento executado por parte do IPCB foi 9% superior ao investimento previsto, justificando-se este acréscimo por um esforço maior que o previsto no desenvolvimento das diversas atividades técnicas (em especial Atividades 2 e 3, com a vertente de segurança), e por ter sido possível obter poupanças nas viagens para participação na vertente internacional do projeto e para apresentação de resultados do projeto em conferências e workshops científicos.

- **IT – Instituto de Telecomunicações**

De modo geral registou-se uma execução financeira abaixo do previsto, devido a questões administrativas (impossibilidade de imputação de algum do pessoal técnico envolvido no projeto) e ao facto de as viagens para participação em conferências e na vertente Eureka do projeto terem sido asseguradas por outros parceiros do consórcio).

Considerações Finais

O projeto ajudou a OneSource a manter e reforçar a equipa de investigação, assegurando a existência de um núcleo de *know-how* e competências avançadas essenciais para identificar e desenvolver soluções inovadoras.

Sumariamente, os trabalhos realizados no âmbito do projeto permitiram obter os seguintes resultados:

- Especificação, desenvolvimento e integração da Plataforma Mobitrust para cenários PPDR, com enfoque especial no suporte de *Situational Awareness* nos Centros de Comando e Controle (informação de sensores, suporte para comunicações voz, vídeo e mensagens seguras).
- Especificação, desenvolvimento e integração de diversas soluções de segurança para tornar os terminais moveis PPDR mais seguros.
- Integração dessas soluções na plataforma Mobitrust, e condução com sucesso dos trabalhos de validação e demonstração da plataforma integrada.
- Realização de várias atividades de divulgação e pré-exploração comercial, de que são exemplo os dois workshops *Mobitrust*.
- Publicação de artigos científicos em conferências, revistas e capítulos de livro.
- Presença no evento industrial CC MENA 2018 (*Critical Communications Middle East and North Africa 2018*, Dubai 23-25 de setembro de 2018).
- Consolidação de relações com parceiros do consórcio nacional e francês (e.g. IT, Gemalto, Trustonic) e com outras organizações na área de 5G e PPDR (e.g. NOKIA, Airbus, Telefonica, Altice Labs, Universidade de Malaga, Fraunhofer) para as vertentes de investigação em consórcio e de negócio (potenciais clientes e parceiros comerciais).

Considera-se que o projeto cumpriu todos os objetivos inovadores propostos e identificados no momento da candidatura, ainda que a relevância relativa de alguns deles – do ponto de vista de mercado – tenha mudado significativamente durante o decorrer do projeto.

Artigos Científicos Publicados/Links oficiais das diversas publicações disponíveis online

- Conference Paper: Ribeiro J., Mantas G., Saghezchi F.B., Rodriguez J., Shepherd S.J., Abd-Alhameed R.A. Towards an Autonomous Host-Based Intrusion Detection System for Android Mobile Devices. Broadband Communications, Networks, and Systems. BROADNETS 2018. Springer.
  http://dx.doi.org/10.1007/978-3-030-05195-2_14

- Journal Paper: K. Barmpatsalou, T. Cruz, E. Monteiro and P. Simoes, "Mobile Forensic Data Analysis: Suspicious Pattern Detection in Mobile Evidence," in IEEE Access, vol. 6, pp. 59705-59727, 2018.
  https://ieeexplore.ieee.org/document/8492342

- Book Chapter: Book Chapter: A. Lima, P. Borges, B. Sousa, P. Simoes, T. Cruz, "Security of Mobile Devices and Applications", in Mobile Apps Engineering, (Eds. G. Mostefaoui, F. Tariq), CRC Press, ISBN 9781138054356, 2018
  https://www.crcpress.com/Mobile-Apps-Engineering/Mostefaoui-Shukla-Tariq/p/book/9781138054356

- Journal papel: K. Barmpatsalou, T. Cruz, E. Monteiro, and P. Simoes. 2018. Current and Future Trends in Mobile Device Forensics: A Survey. ACM Comput. Surv. 51, 3, Article 46 (May 2018), 31 pages. DOI:
  https://doi.org/10.1145/3177847

- Conference Paper: P. Borges, B. Sousa, L. Ferreira, F. Saghezchi, G. Mantas, J. Ribeiro, J. Rodriguez, L. Cordeiro, P. Simoes, "Towards a Hybrid Intrusion Detection System for Android-based PPDR terminals," 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM), Lisbon, Portugal, 2017, pp. 1034-1039. doi: 10.23919/INM.2017.7987434
- https://ieeexplore.ieee.org/document/7987434

Instituto Politécnico de Castelo Branco

FICHA DE PROJETO

- Conference Paper: A. Lima, B. Sousa, P. Simões, T. Cruz, Security monitoring for mobile device assets: a survey, Proc. of the 12th Int. Conf. on Cyber Warfare and Security (ICCWS-2017), pp. 227-236, Dayton, Ohio, US, 2-3 March 2017.
https://www.researchgate.net/publication/312070802_Security_monitoring_for_mobile_device_assets_a_survey

- Conference Paper: Bruno Sousa, Hugo Marques, Luís Cordeiro, Edmundo Monteiro, Jonathan Rodriguez, Paulo Simões, Sistemas de Comunicação de Próxima Geração para Segurança Pública, Proceedings of CLME2017/VCEM, 8º Congresso Luso-Moçambicano de Engenharia / V Congresso de Engenharia de Moçambique, Maputo, 4-8 September 2017; Ed: J.F. Silva Gomes et al.; Publ: INEGI/FEUP (2017).

- Conference Paper: Barmpatsalou K., Cruz T., Monteiro E., Simoes P. (2017) Fuzzy System-Based Suspicious Pattern Detection in Mobile Forensic Evidence. In: Matoušek P., Schmiedecker M. (eds) Digital Forensics and Cyber Crime. ICDF2C 2017. LNICST, vol 216. Springer. doi: 10.1007/978-3-319-73697-6_8
https://www.researchgate.net/publication/322272367_Fuzzy_System-Based_Suspicious_Pattern_Detection_in_Mobile_Forensic_Evidence

- Book Chapter: K. Barbatsalou, T. Cruz, E. Monteiro, P. Simões, "From fuzziness to criminal investigation: An inference system for Mobile Forensics". In Intrusion Detection and Prevention for Mobile Ecosystems (Eds. G. Kambourakis, A. Shabtai, K. Kolias, D. Damopoulos), CRC Press, July 2017. ISBN 9781138033573.
https://www.researchgate.net/publication/322272367_Fuzzy_System-Based_Suspicious_Pattern_Detection_in_Mobile_Forensic_Evidence

- Tese de Mestrado: A. Lima, Anomaly Detection in Mobile Devices, Univ. de Coimbra (2017)
https://estudogeral.sib.uc.pt/handle/10316/83277

Websites

Website institucional do projeto: https://mobitrust-project.onesource.pt/

Website focado nos resultados do projeto: https://mobitrust.onesource.pt/

Website do projeto Eureka!: http://mobitrust.av.it.pt/