Proposta de Projeto de Doutoramento a Desenvolver no Âmbito do 1º Concurso para Atribuição de Bolsas de Investigação na Área de Engenharia Informática

1. Título do projeto

Título: Deteção e prevenção de ataques em aplicações IoT críticas

Palavras-chave: IoT, segurança, deteção de anomalias, prevenção de ataques, aplicações críticas

Referência: CEE_EI_UC2

2. Instituições envolvidas

Instituição onde o doutoramento será realizado: FCTUC

Outras instituições participantes no projeto de investigação: Universidade Lusíada de Angola, com a coordenação do Prof. Doutor Fernando Osmar Pombal Ribeiro, responsável pela área de Pós-Graduações.

3. Equipa de Orientação

Orientador: Prof. Doutor António Jorge da Costa Granjal (https://www.cisuc.uc.pt/people/show/226)

4. Descrição do Projeto

As comunicações 5G irão permitir suportar aplicações verticais em diversas áreas da indústria, entre as quais as aplicações críticas tais como no controlo industrial e aplicações de telemedicina, entre outras. Até à data, tais aplicações são normalmente suportadas por sistemas e infraestruturas de comunicação fechadas e isoladas, sendo que a utilização de comunicações por radiofrequência irá diminuir dramaticamente os custos de instalação e operação de tais aplicações. Este aspeto é particularmente relevante em países que, por fatores socioeconómicos e históricos, não puderam apostar na instalação de uma infraestrutura de comunicações fixa de forma alargada. Por outro lado, é importante considerar que, dado o carácter crítico de tais aplicações, a utilização de mecanismos de cibersegurança adequados reveste-se da maior importância. Em tais ambientes, a segurança é, na realidade, um fator crítico para a viabilização da utilização de comunicações por radiofrequência, com os ganhos de escala atrás referidos.

É importante considerar que os dispositivos sensores e atuadores utilizados no contexto das aplicações IoT são caracterizados por limitações ao nível das suas capacidades computacionais e energéticas, podendo igualmente estar expostos a ameaças físicas e lógicas, quer internas quer externas ao ambiente de operação e comunicação. Assim, a utilização de soluções para a deteção e prevenção atempada de anomalias e ataques à sua segurança e estabilidade reveste-se de particular importância. É neste contexto que irão decorrer os esforços de investigação a levar a cabo ao longo do Projeto, de acordo com os seguintes objetivos de investigação:

- Criação de uma arquitetura para a deteção e prevenção de anomalias e intrusões em ambientes IoT críticos, com particular enfoque nas comunicações de baixa energia e ambientes de controlo industrial SCADA.
- Investigação e validação de modelos de deteção e prevenção de ataques baseados na deteção de anomalias, com recurso a técnicas de aprendizagem computacional.

- Validação das propostas com dados reais e em contexto laboratorial, com vista à implementação e validação dos modelos criados no contexto da arquitetura proposta.

A investigação a desenvolver visará aferir a viabilidade da construção e utilização de modelos de detecção e prevenção de anomalias e ataques externos em ambientes IoT críticos. Existem atualmente diversos desafios aos quais a investigação terá que responder. Por um lado, pretende-se estudar a viabilidade da utilização de técnicas de aprendizagem computacional para detecção, com precisão adequada, de ataques em ambientes e comunicações críticas. Por outro lado, pretende-se avaliar experimentalmente a viabilidade da utilização de tais técnicas nos dispositivos de controlo e atuação utilizados em tais aplicações, considerando as restrições computacionais e energéticas dos sensores e atuadores utilizados. Como resultados expectáveis da investigação a desenvolver ao longo do Projeto, pretende-se publicar em revistas e conferências internacionais de referência na área, bem como contribuir diretamente ao nível da investigação desenvolvida na área no contexto do grupo de Comunicações e Telemática do CISUC (Centro de Informática e Sistemas da Universidade de Coimbra). O orientador, bem como o grupo de investigação no qual se insere, dispõem de alargada experiência na área, atestada por diversas publicações recentes [1-3], bem como pela sua participação em Projetos de Investigação tais como o Projeto Mobilizador 5G [4] e o Projeto H2020 Athena [5].

5. Referências Bibliográficas

[1] Granjal, J., & Pedroso, A. (2018). Intrusion Detection and Prevention with Internet-integrated CoAP Sensing Applications. In IoTBDS (pp. 164-172)

[2] Granjal, J., Silva, J. M., & Lourenço, N. (2018). Intrusion detection and prevention in CoAP wireless sensor networks using anomaly detection. Sensors, 18(8), 2445

[3] Granjal, J., Monteiro, E., & Silva, J. S. (2015). Security for the internet of things: a survey of existing protocols and open research issues. IEEE Communications Surveys & Tutorials, 17(3), 1294-1312

[4] Projeto Mobilizador 5G - Components and Services for 5G Networks (5G - Componentes e Serviços para Redes 5G), https://5go.pt

[5] Atena H2020 Project, Advanced Tools to assEss and mitigate the criticality of ICT compoNents and their dependencies over Critical InfrAstructures, https://cordis.europa.eu/project/id/700581