Controle de Autenticação e Acesso para Sistemas Ciber-Físicos

Doutorado

Vilmar Abreu Junior, Altair Olivo Santin

Contexto: Sistemas Ciber-Físicos (*Cyber-Physical Systems* – CPS) são sistemas de larga escala, geograficamente distribuídos, federados, heterogêneos e de aplicação crítica. Tipicamente são compostos por sensores, atuadores, sistemas de controle e componentes de redes. O CPS pode ser utilizado em diversos segmentos que necessitam de coleta de informações e tomada de decisões em tempo real, como cirurgia robótica, controle aéreo de tráfego, sistemas militares e redes inteligentes de energia. A cyber segurança de um CPS emergiu como interesse crítico de organizações governamentais, principalmente após o Stuxnet deteriorar uma usina nuclear no Irã em poucos segundos. **Objetivo Geral:** Este trabalho propõe um modelo de controle de autenticação e acesso que atenda aos requisitos críticos de um CPS. **Questão de Pesquisa:** A heterogeneidade dos elementos que compõem a arquitetura de um CPS aumenta a complexidade de uma solução de segurança integral. É possível conceber uma solução de controle de autenticação e acesso que contemple desde os dispositivos da Internet das Coisas (*Internet of Things* – IoT) até os Sistemas de Sistemas (*Systems of Systems* – SoS)? **Método de Pesquisa:** Para garantir a solução integral de um CPS, a segurança deve ser concebida *by design*. Devido a criticidade de um CPS, propomos um mecanismo de autenticação multifator, composto por técnicas de autenticação por biometria, georreferenciamento, QR code, entre outros. Para atender a necessidade de interoperabilidade e compartilhamento de informações entre os diversos sistemas do SoS, propomos um controle de acesso distribuído baseado em atributos e papéis, que preserva a autonomia do administrador de cada aplicação para definir os direitos de acesso aos seus recursos protegidos. Finalmente, para garantir a segurança fim-a-fim da comunicação dos dispositivos da IoT com os sistemas de controle mestre (*Master Terminal Unit* – MTU), propomos um esquema baseado em chaves que utiliza um sistema de Gestão de Identidades e Acesso (*Identity and Access Management* – IAM) da Internet para garantir a integração da IoT com a Internet. Dessa maneira, a solução permite que um operador utilize as mesmas credenciais para acessar diversos dispositivos da IoT, sem criar uma brecha de segurança na comunicação. **Resultados Preliminares:** O protótipo que garante a segurança fim-a-fim da comunicação dos dispositivos da IoT com a MTU apresentou que a proposta é viável para proteção da comunicação.

Palavras-chave: Sistemas Ciber-Físicos; Controle de Autenticação Multifator; Controle de Acesso Distribuído; Gestão de Identidades; Internet das Coisas.

Publicações do aluno no período do Doutorado (03/2016 – Atual)

1. **ABREU, VILMAR** ; Santin, Altair O. ; XAVIER, A. S. ; LANDO, Alison Luis ; WITKOVSKI, ADRIANO ; RIBEIRO, R. C. ; STIHLER, M. ; ZAMBENEDETTI, V. C. ; CHUEIRI, I. J. . A Smart Meter and Smart House Integrated to an IdM and Key-based Scheme for Providing Integral Security for a Smart Grid ICT. MOBILE NETWORKS AND APPLICATIONS, 2017. (Aceito para publicação)
2. **ABREU, VILMAR**; SANTIN, A. O. ; VIEGAS, E. K. ; STIHLER, M. . A Multi-domain Role Activation Model. In: IEEE International Conference on Communications, 2017, Paris. IEEE International Conference on Communications, 2017.
3. VIEGAS, E. K. ; SANTIN, A. O. ; **ABREU, V**. ; OLIVEIRA, L. E. S. . Stream Learning and Anomaly-based Intrusion Detection in the Adversarial Settings. In: IEEE Symposium on Computers and Communications, 2017, Crete. 2017 IEEE Symposium on Computers and Communications (ISCC) - 22th IEEE Symposium on Computers and Communications, 2017.
4. RIBEIRO, R. C. ; SANTIN, A. O. ; **ABREU, V**. ; MARYNOWSKI, J. ; VIEGAS, E. K. . Providing Security and Privacy in Smart House Through Mobile Cloud Computing. In: Latin-American Conference on Communications, 2016, Medelin. IEEE 8th Latin-American Conference on Communications, 2016.