https://eventos.utfpr.edu.br//sicite/sicite2019

Segurança em ambientes SCADA: Uma simulação de criptografia de eventos críticos com máquina de estados.

Security on SCADA environments: A simulation of critical events cryptography with state machines.

Alex Bender
alexbender@alunos.utfpr.edu.br
Universidade Tecnológica Federal do Paraná, Pato Branco, Paraná, Brasil
Marcelo Teixeira
Marceloteixeira@utfpr.edu.br
Universidade Tecnológica Federal do Paraná, Pato Branco, Paraná, Brasil

RESUMO

O sistema de controle supervisório e aquisição de dados (do inglês Supervisory Control and Data Acquisition - SCADA) desenvolvido em meados do séc. XX, tem como objetivo monitorar uma planta, ou seja, o processo de fabricação de algum produto ou até mesmo a distribuição de energia e água. Um dos problemas gerados na atualidade são agentes mal-intencionados que pretendem corromper ou modificar dados que são vitais para o funcionamento destas plantas. Este trabalho tem como objetivo aumentar o nível de segurança nesses sistemas, buscando simular a criptografia desses dados que são recebidos e enviados apenas em momentos críticos classificados através de uma máquina de estados. O trabalho obteve êxito em suas simulações mostrando que o atraso provocado pela criptografia não foi prejudicial, mas a diferença entre criptografar todos os estados e o estado crítico não foi alcançado.

PALAVRAS-CHAVE: Computadores – Medidas de Segurança. Computadores – Controle de Acesso. Controle Automático.

ABSTRACT

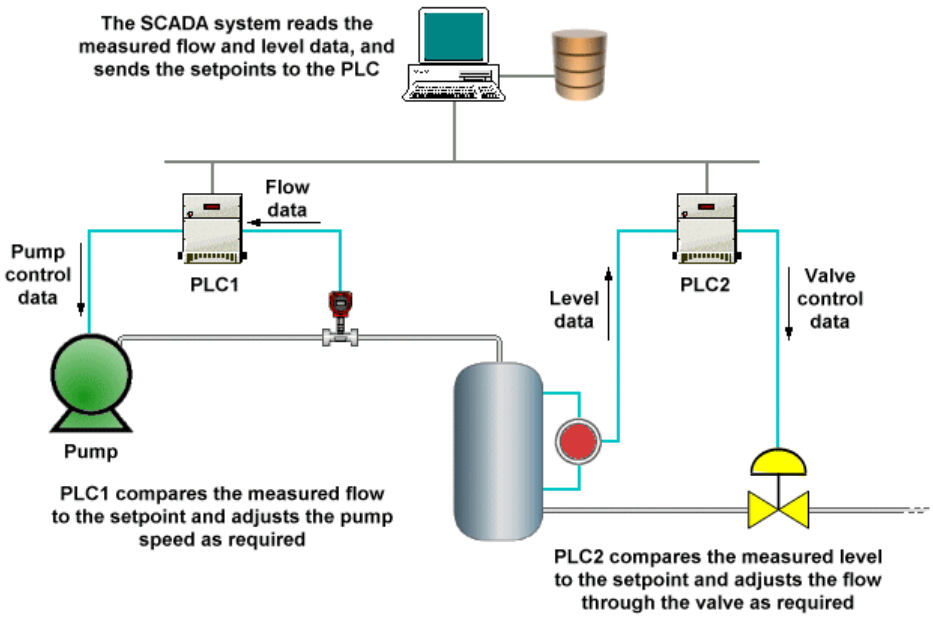
The security of Supervisory Control and Data Acquistion (SCADA) developed in the mid 20th century, aims monitor a plant, ie the fabrication process of a product or even water and energy distribuition. One of the problems that currently happens are malicious agents that intend to corrupt or modify data that is vital to the operation of this plants. This work has as objetive ensure the security level of this systems, seeking to simulate the cryptography of this data that are received and sent just in critical moments classified through a state machine. This work succeeded in its simulations showing that the delay caused by the cryptography was not harmful, but the difference between encrypt all states and just the critical state was not achived.

KEYWORDS: *Computers – Security measures. Computers – Access control. Automatic control.*

Recebido: 19 ago. 2019.
Aprovado: 01 out. 2019.

INTRODUÇÃO

A necessidade de controlar ambientes fabris ou sistemas críticos como o abastecimento de água ou distribuição de energia elétrica além de diminuir custos, fez com que, nos anos de 1970, isso fosse possível através de um sistema de controle supervisório e aquisição de dados (do inglês *Supervisory Control and Data Acquisition* – SCADA)(ANTÓN, 2017) que funciona de uma forma simplificada conforme a Figura 1: dados físicos (nesse exemplo o nível de um tanque) são lidos por um Controlador Lógico Programável (CLP ou *Programavel Logic Controller* – PLC). Esses dados são enviados para o SCADA que supervisiona todo o processo e o controlador pode controlar toda a planta sem necessidade da presença física no local. Quando necessário alguma mudança no processo físico, o controlador do sistema faz certa ação no SCADA que modifica o funcionamento da planta pelos CLPs.



Fonte: https://br.pinterest.com/pin/466896686340360073/, acessado 06/08/19 as 11:30.

Com a evolução da tecnologia, o sistema SCADA que iniciou seus trabalhos sem a preocupação com segurança, começa a ter problemas com softwares mal-intencionados que através da internet e *exploits* em seus sistemas operacionais, deixaram brechas para ataques (KRUTZ, 2005). Alguns desses sistemas SCADA ainda não conseguiram melhorar a segurança de seus sistemas e continua-se a ter brechas de segurança.

Desta forma, este trabalho tem como objetivo adicionar uma camada de segurança as que já existem, mas de uma forma específica: assegurando que mensagens enviadas e recebidas em momentos críticos do sistema não poderão ser acessadas ou modificadas neste momento. A abordagem será criptografar essas mesmas mensagens utilizando-se de uma máquina de estados já desenvolvida, garantindo que sejam criptografadas.

Trabalhos como os problemas de segurança do SCADA (IGURO, 2006) são exemplos de trabalhos relacionados

MATERIAIS E MÉTODOS

Para que este trabalho fosse desenvolvido foram necessários os seguintes materiais:

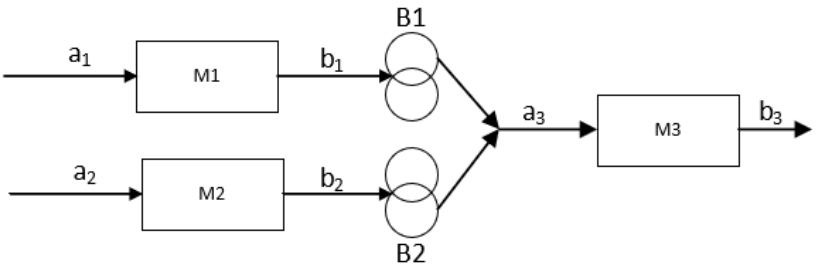
a) Um computador com sistema operacional UNIX;

b) A plataforma Anaconda para programação na linguagem python3, com a IDE de programação spyder3 inclusa na plataforma;

c) Os módulos: sys – System-specific parameters and functions 3.7.4, signal – Set handlers for asynchronous events 3.7.4, time – Time access and conversions, cryptography em especial o pacote fernet.

d) A máquina de estados (Bianchi, 2019) (Figura 2) para tratar de eventos críticos.

Figura 2 - Máquina de Estados



Fonte: Felipe Bianchi (2019)

Os materiais acima proporcionam a possibilidade de desenvolver o seguinte algoritmo: alguns eventos aleatórios são gerados para que a máquina de estados entre em funcionamento, o estado crítico mostrado em M3 inicia o processo de criptografia do dado recebido, após os acontecimentos de M1 e M2. Ao fim da criptografia o programa simula o envio do dado à um microcontrolador que seria o responsável pela descriptografia dos dados, simulando o tempo de atraso de envio e recebimento de dados.

Para testar a eficiência do algoritmo, foi medido o tempo de execução com 7 eventos aleatórios, 50 vezes, em 3 situações:

a) Algoritmo sem criptografia: O tempo é medido a partir do início da execução do algoritmo sem criptografia em nenhum nível, ou seja, sobre nenhum evento, levando em conta também os atrasos de envio e recebimento dos dados, para que exista uma base de tempo para a futura comparação com os métodos abaixo descritos;

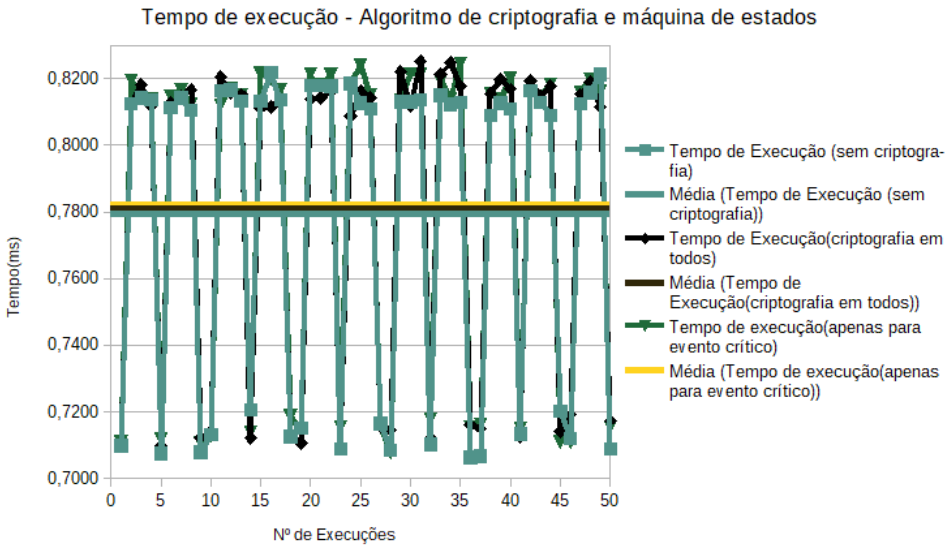
b) Algoritmo com criptografia em evento crítico: O tempo é medido a partir do início da execução do algoritmo com criptografia apenas sobre o evento crítico, medindo o tempo de execução do algoritmo e dos atrasos de envio e recebimento de dados

c) Algoritmo com criptografia: O tempo é medido a partir do início da execução do algoritmo com criptografia em todos os eventos, medindo o tempo de execução do algoritmo e dos atrasos de envio e recebimento

RESULTADOS E DISCUSSÃO

Apresenta-se o da simulação de execução da forma apresentada a cima, conforme a figura 3:

Figura 3 – Tempo de execução - Algoritmo de criptografia e máquina de estados



Fonte: Autor (2019)

Constata-se que os tempos de execução com as três variações do algoritmo são muito próximas, mas pequenos, sendo assim, os atrasos não seriam significativos no tempo de execução do processo completo aonde está implantado o SCADA.

Por outro lado, não temos ganhos significativos, segundo a simulação, na comparação entre a variação do algoritmo usando a criptografia em todos os estados em relação a apenas o estado crítico.

Numa aplicação real, teríamos outros atrasos não levantados neste trabalho ou mal levantados: o tempo de atraso da via de comunicação, o tempo de atraso da comunicação em si, ou seja, envio e recebimento. Outro grande problema é: como apresentado na introdução deste trabalho, é necessário um CLP para comunicar o que está acontecendo no processo físico para o SCADA. Sendo assim, é necessário descriptografar os dados no CLP, e isso pode acarretar atrasos pois o nível de processamento de um CLP não é comparável a um computador, com vários núcleos de processamento, que aceleram todo o processo.

CONCLUSÃO

O sistema SCADA criada em meados do SÉC. XX pode controlar grandes processos industriais, mas teve problemas com a segurança pois não foi desenvolvido prevendo problemas com pessoas e softwares mal-intencionados que poderiam modificar ou atrapalhar a boa execução.

Este trabalho tem como objetivo melhorar a segurança deste software, mas não somente isso, busca aumentar a segurança em ambientes indispensáveis para o ser humano como a distribuição de energia elétrica, água potável, grandes indústrias.

Foi conseguido atingir com êxito a execução do algoritmo e o funcionamento da criptografia e da máquina de estados, mas infelizmente não foi possível atestar a melhoria significativa entre criptografar eventos críticos e todos os eventos, mas já é possível aplicar este algoritmo, com algumas adaptações a realidade, para que seja possível atestar, no mundo físico, a melhora ou não, desta simulação.

AGRADECIMENTOS

Agradeço a instituição CNPq (Conselho Nacional de Desenvolvimento Científico e Tecnológico), ao professor Doutor Marcelo Teixeira, ao colega Felipe Bianchi e a toda a Universidade Tecnológica Federal do Paraná(UTFPR) - Câmpus Pato Branco pela estrutura.

REFERÊNCIAS

Fernet (symmetric encryption). Version: Release 2.8.dev1. Individual Contributors. Disponível em: <https://buildmedia.readthedocs.org/media/pdf/cryptography/latest/cryptography.pdf>. Acesso em: 12/05/2018 as 22:47

SHAW, William T.. **Cybersecurity for SCADA Systems.** Pennwell, 2006. 300 p.

BIANCHI, Felipe. **Máquina de estados para eventos críticos.** Disponível em: < https://sites.google.com/view/mtmca/downloads?authuser=0 >. Acesso em: 16/08/2019 as 14:00.

S. D. Antón, D. Fraunholz, C. Lipps, F. Pohl, M. Zimmermann and H. D. Schotten, Two decades of SCADA exploitation: A brief history**. IEEE Conference on Application, Information and Network Security (AINS)**. Miri. 2017. pp. 98-104.

KRUTZ, Ronald L.. **Securing Scada Systems.** John Wiley & Sons. 2005 .

IGURE, Vinay M.; LAUGHTER Sean A.; WILLIAMS Ronald D. Security issues in SCADA networks. **Computers & Security,** v. 25, n. 7, p. 498-506, 2006. Disponível em <https://www.sciencedirect.com/science/article/pii/S0167404806000514>. Acesso em: 16 set. 2019.