26 Jan 2017

Consumer Privacy vs Data Mining: Issues with Smart Meter Data (1:10-1:50 pm ET)

and

Defeating Malware Packing and Code Obfuscation Techniques (2:00-2:40 pm ET)

Mark your calendars and come join your friends in the CAE community for a Tech Talk. We are a warm group that shares technical knowledge. CAE Tech Talks are free and conducted live in real-time over the Internet, so no travel is required. You can attend from just about anywhere (office, home, etc.) Capitol Technology University (CTU) hosts the presentations using their online delivery platform (Adobe Connect) which employs slides, VOIP, and chat for live interaction. Just log in as “Guest” and enjoy the presentation(s).

Below is a description of the presentation(s) and logistics of attendance:

Date: Thursday 26 Jan 2017

Time: 1:10-1:50 pm ET

Location: https://capitol.adobeconnect.com/cae_tech_talk/

Just log in as “Guest” and enter your name. No password required.

Title/Topic: Consumer Privacy vs Data Mining: Issues with Smart Meter Data

Audience Skill Level: Intermediate, Advanced

Presenter(s): Vitaly Ford (Tennessee Tech University)
Description:

Smart Grid technologies have been revolutionizing the legacy power grid through advanced sensor networks, two-way communication capabilities, and immediate detection of outages. As a critical part of the Smart Grid, the Advanced Metering Infrastructure (AMI) can provide granular energy consumption data and report them to a utility company, utilizing electrical smart meters. This talk will address an intricate challenge in AMI concerning a protocol supporting consumer privacy protection within the energy consumption data analysis. We will discuss security issues in the existing AMI infrastructure and demonstrate how data can be secured in a privacy-preserving way without losing data mining opportunities. The proposed AMI protocol is based on a certificateless public key encryption that is used as a baseline for establishing a session key. Utility companies will be able to perform an energy consumption data analysis and maintain consumer privacy. At the same time, consumers will be able to retrieve their own data and keep their true identity anonymous. This talk will conclude with a discussion about various attacks on the protocol and address a novel energy consumption differential attack against consumers.

Date: Thursday 26 Jan 2017

Time: 2:00-2:40 pm ET

Location: https://capitol.adobeconnect.com/cae_tech_talk/

Just log in as “Guest” and enter your name. No password required.

Title/Topic: Defeating Malware Packing and Code Obfuscation Techniques

Audience Skill Level: Intermediate

Presenter: Josh Stroschein (Dakota State University)

Description:

Modern malware goes to great lengths to thwart detection and analysis during distribution, infection and operation. In this talk we’ll discuss common techniques used by modern malware to hide its intentioned functionality through packing, obfuscation and anti-analysis techniques. We’ll cover effective approaches that a malware analyst can use to peel back these layers and reveal the malwares true purpose. Topics include, but not limited to, reverse engineering, static and dynamic analysis, use of debuggers, and IDA Python.
CAE Tech Talks are also recorded

Recordings of live presentations are posted to the website below:

https://capitol.instructure.com/courses/510/external_tools/66

Pdf versions of the presentations are posted to the website below:

https://capitol.instructure.com/courses/510/files

Contact

CAE Tech Talk events are advertised thru email and posted to the news and calendar section of the CAE community website: www.caecommunity.org

For questions on CAE Tech Talk, please send email to CAETechTalk@nsa.gov