Sep 30th, 9:00 AM

Proceedings of the 2016 Information Security Research and Education (INSuRE) Conference (INSuRECon-16)

Information Security Research and Education (INSuRE) Conference

Proceedings of the 2016 Information Security Research and Education (INSuRE) Conference (INSuRECon-16)

The inaugural INSuRECon Conference was held on September 30, 2016. The conference was held virtually using Cisco Webex online meeting and video conferencing software. Five papers were accepted out of 8 submissions. During the conference, each paper was presented by an author at the conference and the audience was provided the opportunity to ask questions of the presenter.

Information Security Research and Education (INSuRE) is a partnership among Centers of Academic Excellence in Information Assurance Research (CAE-R) the National Security Agency (NSA), the Department of Homeland Security and other federal agencies in order to design, develop and test the research network. INSuRE is a self-organizing, cooperative, multi-disciplinary, multi-institutional, and multi-level collaborative research project that can include both unclassified and classified research problems in cybersecurity.

The INSuRECon and the INSuRECon proceedings highlight the most significant results from INSuRE research projects. INSuRE provides an opportunity for students to work on contemporary research problems of national importance. Research problems are proposed and mentored by cybersecurity practitioner's federal and state government.

The five accepted papers are as follows.

1. G. Auger and R. Hilgers. Black Box FISMA-based Security Control Assessment of Public Cloud Providers

   Abstract - Public cloud computing solutions are desirable for business and government agencies to outsource infrastructure technology requirements. This decision transfers the responsibility of certain security controls to the cloud provider, and impacts the ability for system owner oversight of security. Government agencies are required by law to conform to the Federal Information Security Management Act of 2002 (FISMA) that outlines a collection of security controls that must be implemented. Cloud service providers therefore have to implement these controls, at a minimum, to be valid for government usage. Given the known library of controls that must be implemented by the Cloud service provider, this paper identifies 9% of FISMA-based NIST 800-53 security controls can be validated externally by an end-user of a cloud service provider with confidence.

   Keywords: FISMA; cloud-computing; FedRAMP; security assessment; black-box; NIST

2. L. Tomlin, M. Farnam, S. Pan. A Clustering Approach to Industrial Network Intrusion Detection.

   Abstract- Industrial control system (ICS) networks and supervisory control and data acquisition (SCADA) system networks are less likely to be within a strict closed network environment, which increases the likelihood of cyber-attacks. Over the last decade, intrusion detection has become an additional security measure for ICS and SCADA system networks to help prevent and minimize loss that may be sustained from cyber-attacks. ICS and SCADA network communication is typically repetitive and deterministic, which allows normal activity to be more easily modeled on the behavior of system specific events. Given this deterministic behavior, an unsupervised anomaly-based intrusion detection system may provide increased performance over the more typical misuse detection method. We propose an unsupervised machine learning approach for the implementation of a network IDS in power system applications. The approach would supplement a more complex IDS by quantifying the degree by which an event is an attack, given network data states, to improve intrusion detection and minimize false alarm rates. The clustering approach contains four key processes: data preprocessing, unsupervised learning (cluster analysis), generating features from clusters, and classifying states using the Mamdani fuzzy inference system. Data sets from a simulated power distribution system are used to illustrate the impact of the proposed approach.

Keywords: cluster analysis, cluster tendency, feature selection, FIS, IDS, ICS, machine learning, SCADA, smart grid

3. G. Rehm, M. Thompson, B. Busenius, and J. Fowler. Mobile Encryption Gateway (MEG) for Email Encryption

   Abstract - Email cryptography applications often suffer from major problems that prevent their widespread implementation. MEG, or the Mobile Encryption Gateway aims to fix the issues associated with email encryption by ensuring that encryption is easy to perform while still maintaining data security. MEG performs automatic decryption and encryption of all emails using PGP. Users do not need to understand the internal workings of the encryption process to use the application. MEG is meant to be email-client-agnostic, enabling users to employ virtually any email service to send messages. Encryption actions are performed on the user's mobile device, which means their keys and data remain personal. MEG can also tackle network effect problems by inviting non-users to join. Most importantly, MEG uses end-to-end encryption, which ensures that all aspects of the encrypted information remains private. As a result, we are hopeful that MEG will finally solve the problem of practical email encryption.

4. K. Rahman, M. Bishop, and A. Holt. Internet of Things Mobility Forensics.

   Abstract- The Internet of Things (IoT) comes with great possibilities as well as major security and privacy issues. Although digital forensics has long been studied in both academia and industry, mobility forensics is relatively new and unexplored. Mobility forensics deals with tools and techniques that work towards forensically sound recovery of data and evidence from mobile devices [1]. In this paper, we explore mobility forensics in the context of IoT. This paper discusses the data collection and classification process from IoT smart home devices in details. It also contains attack scenario based analysis of

collected data and a proposed mobility forensics model that fits into such scenarios. The paper concludes with a detail discussion of related research problems and future work.

Keywords: Mobility Forensics; Internet of Things; Digital Forensics; Privacy; Cyber Security

5. P. Mane, S. Shanbhag, T. Kamath, P. Mackey, J. Springer. Analysis of Community Detection Algorithms for Large Scale Cyber Networks

Abstract- The aim of this project is to use existing community detection algorithms on an IP network dataset to create supernodes within the network. This study compares the performance of different algorithms on the network in terms of running time. The paper begins with an introduction to the concept of clustering and community detection followed by the research question that the team aimed to address. Further the paper describes the graph metrics that were considered in order to shortlist algorithms followed by a brief explanation of each algorithm with respect to the graph metric on which it is based. The next section in the paper describes the methodology used by the team in order to run the algorithms and determine which algorithm is most efficient with respect to running time. Finally, the last section of the paper includes the results obtained by the team and a conclusion based on those results as well as future work.

Keywords: Network traffic analysis, community detection, graph clustering, modularity, algorithms