Emerging Technologies: Impact on Information Security Risk Evaluation
2016 Boston Federal Reserve Bank of Boston Cybersecurity Conference

James Burrell, Ph.D., CISSP, GISP

SELECTED RESEARCH REFERENCES

CLOUD INFRASTRUCTURES

Expressing and Enforcing Location Requirements in the Cloud using Information Flow Control

Pasquier, T. F. M., & Powles, J. E. (2015, March). Expressing and enforcing location requirements in the cloud using information flow control. In *Cloud Engineering (IC2E), 2015 IEEE International Conference on* (pp. 410-415). IEEE.

URL: http://www.cl.cam.ac.uk/research/srg/opera/publications/papers/2015claw.pdf

Abstract

The adoption of cloud computing is increasing and its use is becoming widespread in many sectors. As cloud service provision increases, legal and regulatory issues become more significant. In particular, the international nature of cloud provision raises concerns over the location of data and the laws to which they are subject. In this paper we investigate Information Flow Control (IFC) as a possible technical solution to expressing, enforcing and demonstrating compliance of cloud computing systems with policy requirements inspired by data protection and other laws. We focus on geographic location of data, since this is the paradigmatic concern of legal/regulatory requirements on cloud computing and, to date, has not been met with robust technical solutions and verifiable data flow audit trails.

Nice A New Framework For Improving Attack Detection In Cloud

Upendra, V., & Mathew, D. J. (2016). Nice A New Framework For Improving Attack Detection In Cloud. *IJMCA*, *4*(1), 136-139.

URL: http://www.ijmca.org/index.php/ojs/article/download/248/pdf

Abstract

Cloud security is one of most important issues that have attracted a lot of research and development effort in past few years. Particularly, attackers can explore vulnerabilities of a cloud system and compromise virtual machines to deploy further large-scale Distributed Denial- of-Service (DDoS). DDoS attacks usually involve early stage actions such as multi-step exploitation, low frequency vulnerability scanning, and compromising identified vulnerable virtual machines as zombies, and finally DDoS attacks through the compromised zombies. Within the cloud system, especially the Infrastructure-as-a-Service (IaaS) clouds, the detection of zombie exploration attacks is extremely difficult. This is because cloud users may install vulnerable

The views expressed in this document are those of the author and do not necessarily represent the views, opinions, or endorsement of the U.S. Government or any agency of the U.S. Government.

applications on their virtual machines. To prevent vulnerable virtual machines from being compromised in the cloud, we propose a multi-phase distributed vulnerability detection, measurement, and countermeasure selection mechanism called NICE, which is built on attack graph based analytical models and reconfigurable virtual network-based countermeasures. The proposed framework leverages Open Flow network programming APIs to build a monitor and control plane over distributed programmable virtual switches in order to significantly improve attack detection and mitigate attack consequences. The system and security evaluations demonstrate the efficiency and effectiveness of the proposed solution.

NETWORK VIRTUALIZATION

Software-Defined Networking Security: Pros and Cons

Dabbagh, M., Hamdaoui, B., Guizani, M., & Rayes, A. (2015). Software-defined networking security: pros and cons. *Communications Magazine, IEEE*, *53*(6), 73-79.

URL: http://ir.library.oregonstate.edu/xmlui/bitstream/handle/1957/57524/DabbaghMehiarElectricalEngineeringComputerScienceSoftware-DefinedNetworkingSecurity.pdf?sequence=1

Abstract

Software-Defined Networking (SDN) is a new networking paradigm that decouples the forwarding and control planes—traditionally being coupled with one another—while adopting a logically centralized architecture aiming to increase network agility and programability. While many efforts are currently being made to standardize this emerging paradigm, careful attentions need to be paid to security at this early design stage too, rather than waiting until the technology becomes mature, thereby potentially avoiding previous pitfalls made when designing the Internet in the 80's. This article focuses on the security aspects of SDN networks. We begin by discussing the new security pros that SDN brings and by showing how some of the long-lasting issues in network security can be addressed by exploiting SDN capabilities. Then, we describe the new security threats that SDN is faced with and discuss possible techniques that can be used to prevent and mitigate such threats.

Security improvement in IoT based on Software Defined Networking (SDN)

Vandana, C. P. Security improvement in IoT based on Software Defined Networking (SDN).

URL: http://ijsetr.org/wp-content/uploads/2016/01/IJSETR-VOL-5-ISSUE-1-291-295.pdf

Abstract

With the evolving Internet of Things (IoT) technology, there is exponential growth in connectivity of heterogeneous devices to the internet. Securing such complex heterogeneous networks and their diverse access protocols is a real challenge leading to security risk. Integration of Software Defined Networking (SDN) with IoT can open up way for better security and access control mechanisms. SDN is an intelligent networking paradigm which opens up vast opportunities to manage and secure IoT. In this paper, we have

discussed the SDN based IoT architecture and have proposed a security framework for IoT based on SDN–IoT architecture.

INTERNET OF THINGS

Internet of Things (IoT): An Over view of Applications and Security Issues Regarding Implementation

Hafsa Tahir, A. K., & Junaid, M. Internet of Things (IoT): An Overview of Applications and Security Issues Regarding Implementation.

URL: http://www.ijmse.org/Volume7/Issue1/paper3.pdf

Abstract

The Internet of Things (IoT) is a powerful paradigm that has made progress in the almost every field of human life. This paper gives an overview of IoT, its enabling technologies, applications and security issues in the wireless technologies. IoT is enabled by a number of different technologies such as Radio Frequency Identifiers (RFID), and Wireless Sensor Networks (WSN). There are huge number of applications of IoT in almost every aspect of life i.e. healthcare, logistics and supply chain management, smart environment and social application etc. only a few of these applications are discussed in this paper. Security is an important concern of wireless networks and so it is one of the main issues in IoT. This paper gives an overview of the few of many security concerns in an IoT system and methods to prevent those issues.

A Secure and Quality-Aware Prototypical Architecture for the Internet of Things

Sicari, S., Rizzardi, A., Miorandi, D., Cappiello, C., & Coen-Porisini, A. (2016). A secure and quality-aware prototypical architecture for the Internet of Things. *Information Systems*, *58*, 43-55.

URL: http://www.dista.uninsubria.it/~alessandra.rizzardi/public/documents/2016_NOSalgo.pdf

Abstract

The increasing diffusion of services enabled by Internet of Things (IoT) technologies raises several risks associated to security and data quality. Together with the high number of heterogeneous interconnected devices, this creates scalability issues, thereby calling for a flexible middleware platform able to deal with both security threats and data quality issues in a dynamic IoT environment. In this paper a lightweight and cross-domain prototype of a distributed architecture for IoT is presented, providing minimum data caching functionality and in-memory data processing. A number of supporting algorithms for the assessment of data quality and security are presented and discussed. In the presented system, users can request services on the basis of a publish/subscribe mechanism, data from IoT devices being filtered according to users requirements in terms of security and quality. The prototype is validated in an experimental setting characterized by the usage

The views expressed in this document are those of the author and do not necessarily represent the views, opinions, or endorsement of the U.S. Government or any agency of the U.S. Government.

of real-time open data feeds presenting different levels of reliability, quality and security.

MALWARE ANALYSIS

A Survey of App Store Analysis for Software Engineering

Martin, W., Sarro, F., Jia, Y., Zhang, Y., & Harman, M. (2016). A Survey of App Store Analysis for Software Engineering. *RN*, *16*, 02.

URL: http://www.cs.ucl.ac.uk/fileadmin/UCL-CS/research/Research_Notes/RN_16_02.pdf

Abstract

App Store Analysis studies information about applications mined from app stores. App stores provide a wealth of information derived from users that would not exist had the applications been distributed via previous software deployment methods. App Store Analysis incorporates this non-technical information with technical information to learn trends and behaviours within these forms of software repositories. Findings from App Store Analysis have a direct and actionable impact on the software teams that develop for app stores, and have led to techniques for requirements engineering, release planning, software design, security and testing. This survey describes and compares the areas of research that have been explored thus far, drawing out new directions future research should take to address open problems and challenges.

Evaluation of Machine Learning Classifiers for Mobile Malware Detection

Narudin, F. A., Feizollah, A., Anuar, N. B., & Gani, A. (2016). Evaluation of machine learning classifiers for mobile malware detection. *Soft Computing*, *20*(1), 343-357.

URL: http://umexpert.um.edu.my/file/publication/00001293_118859.pdf

Abstract

Mobile devices have become a significant part of people’s lives, leading to an increasing number of users involved with such technology. The rising number of users invites hackers to generate malicious applications. Besides, the security of sensitive data available on mobile devices is taken lightly. Relying on currently developed approaches is not sufficient, given that intelligent malware keeps modifying rapidly and as a result becomes more difficult to detect. In this paper, we propose an alternative solution to evaluating malware detection using the anomaly-based approach with machine learning classifiers. Among the various network traffic features, the four categories selected are basic information, content based, time based and connection based. The evaluation utilizes two datasets: public (i.e. MalGenome) and private (i.e. self-collected). Based on the evaluation results, both the Bayes network and random forest classifiers produced more accurate readings, with a 99.97% true-positive rate (TPR) as opposed to the multi-layer perceptron with only 93.03% on the MalGenome dataset. However, this experiment revealed that the k-nearest neighbor classifier efficiently detected the latest Android malware with an 84.57% true-positive rate higher than other classifiers.

The views expressed in this document are those of the author and do not necessarily represent the views, opinions, or endorsement of the U.S. Government or any agency of the U.S. Government.