Journal of Advances in Science and Technology
Vol. 12, Issue No. 25, (Special Issue) December-2016, ISSN 2230-9659

Data Security and Threat Modeling for Smart City Infrastructure

V. J. Patwardhan[1]*, P. K. Patil[2], S. G. Gollagi[3]

[1]CSE Dept., HSIT, Nidasoshi

[2]CSE Dept., HSIT, Nidasoshi

[3]Assistant Professor, CSE Dept., HSIT, Nidasoshi

Abstract – Smart city opens up data with a wealth of information that brings innovation and connects government, industry and citizens. Cyber insecurity, on the other hand has raised concerns among data privacy and threats to smart city systems.

In this paper, we look into security issues in smart city infrastructure from both technical and business operation perspectives and propose an approach to analyze threats and to improve data security of smart city systems. The assessment process takes hundreds of features into account. Data collected during the assessment stage are then imported into an algorithm that calculates the threat factor. Mitigation strategies are provided to help reducing risks of smart city systems from being hacked into and to protect data from being misused, stolen or identifiable. Study shows that the threat factor can be reduced significantly by following this approach.

Experiments show that this comprehensive approach can reduce the risks of cyber intrusions to smart city systems. It can also deal with privacy concerns in this big data arena.

Keywords - Smart City, Cyber Physical, Threat Modeling, Data Security

----------♦----------

I. INTRODUCTION

Smart city improves the livability, workability and sustainability and connects people from urban to suburban areas and gathers data from a large number of Beacons, RFIDs, wearable devices, and all kinds of other sensors connected through Raspberry Pi, Arduino and other microcontrollers.

To address the security and privacy issues in smart city big data setting, corporations and government have developed a lot of innovative technologies. On the other hand, due to the complexity of the problems, those problems cannot be solved with technology alone. Good policies and effective business operations have to be put in place in order to make smart city systems free from data breaches.

National Institute of Standard and Technology (NIST) started a global city teams challenge in 2013. It has brought together more than 100 companies, universities, and other organizations to form teams that developed and applied networked technologies. NIST plans to host “Cybersecurity for Smart City Infrastructure” workshop every year.

Experience API (xAPI), developed by Depart of Defense (DoD) is an application program interface that can be used to congregate data generated from various sensors. It is a simple interface to store and retrieve records generated by learning management systems and smart city sensors. A database named LRS stores data generated in the smart city system. The advantage of using xAPI is that all devices are interconnected not through complicated local networks. Rather they all connected through LRS that all devices feed data to the LRS. Using a dashboard, information on all connected devices are filtered, displayed and visualized.

As LRS data may includes entry access, power usage, current temperature, power grid information, social network data, mobility network data, medical records and other personal identifiable information, protecting those data and conducting threat analysis becomes very important. The current authentication methods on LRS use unencrypted username and password. Thus makes it vulnerable to cyber criminals.

II. DATA BREACHES AND TECHNIQUES

Techniques used by hackers range from low tech ones such as phishing and social engineering to more advanced techniques such as malware, backdoors, third party supply chains attacks, zero-day attacks, etc. From our research, we discovered that most of the known attacks could have been prevented. For easy analysis, we categorize the techniques that hackers used to launch attacks into four areas:

- System architecture, firewalls, software patches
- Malware, security policies and human factors
- Third-party chains and insider threat
- Database schemas and encryption technologies

Next we look into these areas and analyze the techniques that hackers used aiming to find comprehensive solutions to counter those attacks

A. Firewalls, Patches and Architecture

Sony has an external intrusion on PlayStation Network (PSN) in April 2011. An unauthorized person has obtained names, addresses, emails, dates of birth, PSN usernames and passwords, credit card numbers, billing addresses and password security questions of 101.6 million users. Twelve million credit card numbers were unencrypted and were stolen and could easily be read. In July 2014, Sony paid $15 million settlement to the victims.

Not only did Sony fail to use firewalls to protect its networks, it was using outdated versions of the Apache Web server with no patches applied on the PlayStation Network. These problems were flagged on security forums two or three months prior to the April data breach, which were monitored by Sony employees.

One World Labs founder Chris Roberts was able to hack into planes' in-flight entertainment system and make the plane turn sideways.

B. Malware, Policies and Human Factors

On November 24, 2014, the corporate network of Sony Pictures had been hacked. The attackers took terabytes of private data, deleted the original copies from Sony computers, and left messages threatening to release the information if Sony didn't comply with the attackers' demands.

C. Third-Party Chains and Insider Threat

Following Target data breach which exposed 70 million customer data in 2013, The Home Depot appears to be another victim of a data breach of their POS systems, reportedly by the same Russian hacking group that hit Target, Michaels, Neiman Marcus and P.F. Chang's. As much as 56 million customer data were stolen.

All breaches mentioned above are corporations. Banks are more secure, thanks for the independent networking and secure electronic data exchange service. However this is no longer true. In August 2014, 76 million customer data was stolen from JP Morgan Chase due to data were partially encrypted.

Government and corporations especially third party vendors are vulnerable to cyber intruders. Universities, as an open freedom of information platform also suffer hard from the attacks.

D. Partial Data Encryptions and Weak Encryptions

Four million data were stolen from OPM. The compromised data contains government security clearances and federal employee records including SSNs and other Personal Identifiable Information (PII). The story published in June 2015. However the breach was first detected in April but it appears to have begun at least late 2014. The intrusion came before OPM implement new security procedures that restrict remote access.

In January 2005, George Mason University (GMU) was hacked. Names, photos, and social security numbers of 32,000 students and staff were compromised. It took a week for GMU IT staff to identify the attack. Sensitive data were stolen and used. Partial data encryption was to blame. In July 2014, GMU had another security incident involving a malware intrusion into the university's network.

For one incident, there may be many areas to look into. For example, networks and systems at GMU had weak encryption, malware and operations issues. Imagine it took a week to discover the intrusion. A hacker could steal 300MB data in less than a second. Sony had malware, weak encryption, firewall, operations and insider threat problems all combined. The threat factor was so high that systems could easily get hit and once hacked, the consequences would be significant.

So far there have been many ways to harden firewalls, monitor patches installations, detect malwares and apply encryptions. As a matter of fact, many corporations have implemented a lot of such technologies to protect their networks and systems. On the other hand, incidents of intrusions are still on the rise. Not only to information systems, threats to critical infrastructure such as power grids become a concern to many people. A new comprehensive approach combing technologies with policies and business operations is needed to assess threats and mitigate risks.

III. THREAT ASSESSMENT AND RISK MITIGATIONS

We have proposed a new approach to assess threats to smart city systems by gathering hundreds of features from system architecture, networks, operating systems, database schemas, encryption techniques, security policies, business operations, and corporate data. This Hardware, intelligence, Software, Policies and Operation (HiSPO) approach uses an algorithm we developed to calculate threat factors automatically based on those features. The threat factor gives us how robust a smart city system is facing the cyber threats.

A. Threat Intelligence

Threat intelligence is to gather and share global threat information, alerts, actors, malware and provide analysis to the government and industries. More advanced analysis includes trends, news and profiles so that trusted partners can detect and defer adversaries more effectively. The key benefits of good threat intelligence include:

- Detect unknown attacks
- Increase security analyst efficiency
- Accelerate incident response
- Reduce risk
- Improve Return on Investment (ROI) and
- Effective countermeasures

Continuous monitoring and intelligence sharing make it very useful in threat analysis.

Identifying threats can be done by classifying threats into several board categories, such as spoofing, tampering, session hijacking, denial of service and elevation of privilege, or putting together a threats list with categories.

Here are areas being considered in the HiSPO approach:

- Identify network threats
- Identify host threats
- Identify application threats
- Inspect security policies
- Inspect operational security (including insider threats)
- Analyze attack trees and attack patterns

Identifying network threats is to analyze the network topology and the flow of packets, and inspect routers, firewalls and switch configurations.

Identifying host threats can be done by examining the security setting of system servers, application server, patches, open ports, services, access control, authentication, password cracking, viruses, Trojan horses, worms etc.

Identifying application threats is to check authentication, authorization, code vulnerability, input validation, session hijacking, password policy setting, data encryption, sql injection, exception handling, auditing and logging, etc.

Inspecting security policies includes server, router and switch policy, remote access policy, wireless and Bluetooth policy, database credential policy, technology equipment disposal policy, logging policy, lab security policy, softwareinstallation policy, workstation security, privacy protection policy, web application security policy and compliances.

Inspecting operational security is to analyzing systems without updated virus definitions, insider threats, security policy enforcement, account managements, authorized connections on firewall, restricted/banned site access attempts, etc.

In addition, the HiSPO approach also integrates data from public and commercial threat analysis and threat intelligence systems including PASTA (Process for Attack Simulation and Threat Analysis), CVSS (Common Vulnerability Scoring System), NRAT (Network risk Assessment Tool), WASC (Web Application Security consortium), and FireEye as a service to get more up-to- date threat data.

B. Threat Modeling

Threat modeling process starts with gathering information in network and system architecture, operating systems and updates, components and configurations of applications, data and data storage, database schemas, services and roles, encryptions and external dependencies. Then we look at the business objectives, security policies, procedures and compliance with interviews from executives ranging from CISO and IT managers. After this step, we look at the business operations of the company and interview top executives including CIO, COO and CEO.

Next, we conduct a series of vulnerability assessments. Based on the data collected, we start

modeling threats to the company. Figure 1 shows the initial threat modeling diagram.

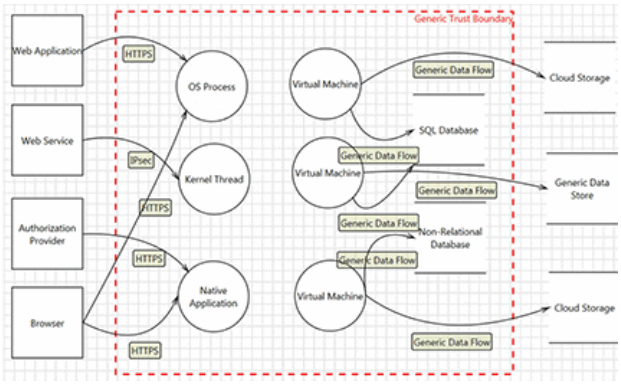

Figure 1: Initial threat modeling diagram

The diagram here only shows partial network configurations. For the assessment work we conducted, the full diagram contains more than 200 nodes and 800 links.

C. Risk Assessment

Based on the threat modeling, the system generates a list of threats and associated risks. Threats are divided into different categories: spoofing, DoS, elevation of privilege, and tempering etc. Human intervention is required at this step to determine whether the threat is at “high risk”, “medium risk” or “low risk”. Actions can be taken either by marking a threat “need investigation”, “mitigated”, “not applicable” or an action has “not started”.

This step requires experienced personnel to make judgments. Using the dynamic threat library that comes with the HiSPO algorithm can give tremendous help.

D. Threat Factors and HiSPO Algorithm

To measure threat, we use threat factor that calculated based on more than 200 features gathered from the previous steps. Threat library contains all threats and updated from time to time. Each threat is assigned a weight. The value of threat factor is calculated using

$$t = 0.5 * \sum_{i=1}^{n} w_i * (t_i + \delta) + 0.01 * (c_{B+} c_{T+} c_{E)} + 0.02 * f_{T1}$$

$$w_i = \frac{1}{\sum_i (t_i)}$$

Where

t_i – Value of threat i

w_i –Weight of threat i

t –Overall threat factor

δ_t-Weight adjustment for threat i

c_B, c_T, c_E-Base, Temporal and environmental scores in CVSS

f_{T1} -Threat intelligence value.

The HiSPO algorithm considers threats and risks of most security areas including hardware, software, policies and business operations. So the threat factor provides an overall view of security of smart city systems. Reducing the threat factor will in return enhance the security and reduce the risks of data breaches to smart city systems.

D. Threat Report

Threat report contains threat modeling executive summary, model name, owner, reviewer, contributors, description, and model diagram. It also lists a detailed description about name and nature of the threat, actions that have been taken and data flow diagram that corresponding to the threat surface.

The report also contains vulnerability assessment results with data discovered during the process.

The final report gives threat factors that were calculated before mitigation and after the assessment and mitigation period. For the system we worked on, the first month of assessment and mitigation leads to the threat factor dropping down from originally 0.71 to 0.38.

After the first round, many areas of the smart city systems were secured. However the blue-hat team was still able to reveal data from the system. The second round of assessment and mitigations took additional three months. When it was done, the threat factor was further reduced to 0.18. At this point, our blue-hat team was no longer able to find any data from the system.

Based on the threat factors that were calculated before and after the assessment, we provide mitigation strategies that would improve overall security of the smart city systems.

IV. CONCLUSION

Threat analysis and risk mitigation are important for corporation and government agencies. In the past, people

focus more on installing firewalls and patches, less focus on configuring and monitoring firewalls, encryptions, access control and business operations.

Even with huge money invested, intrusions still could not be prevented or mitigated.

The new approach takes hundreds of features from various areas into consideration. The approach looks at smart city architecture, firewalls and malware protection programs. It also looks at database schemas, data encryption technologies, security policies, and corporation operations. The vulnerability assessment stage is an iterated process with many threat analysis life cycles. Based on the data collected, the algorithm calculates threat factor and normalizes it. A lower threat factor means the smart city systems would be hacked at lower risk. The approach also uses defense in depth and threat mitigations strategies, and provides recommendations.

We will further study threat modeling and risk mitigation technologies, and improve the threat library to shorten the threat assessment life cycle. The adaptation of this innovate approach can minimum intrusions to government agencies and private sectors and reduce the threats and risks to smart city system in this cyber in-security space.

REFERENCES

NIST 800-122 (2010). Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), National Institute of Standards and Technology.

Rulz, J. et.al. (2012). A Methodology for the Analysis and Modeling of Security Threats and Attacks for Systems of Embedded Components. 20th Euromicro International Conference on Parallel, Distributed & Network-based Processing. p261-268.

Xu, D. et. al. (2012). Automated Security Test Generation with Formal Threat Models. IEEE Transactions on Dependable & Secure Computing. Vol. 9 Issue 4, p526-540.

NIST (2014). National Initiative for Cybersecurity Education (NICE). National Institute of Standards and Technology.

Mousavian, S., Valenzuela, J. & Wang, J. (2015) A Probabilistic Risk Mitigation Model for Cyber-Attacks to PMU Networks. IEEE Transactions on Power Systems. Vol. 30 Issue 1, p156-165.

Privacy Clearinghouse. (2014). University of Maryland, College Park. Retrieved from https://www.privacyrights.org/data-breach-asc?title=maryland

Baltimore Sun (2014). UMCP reports another cybersecurity breach. Retrieved from http://www.baltimoresun.com/news/maryland/education/blog/bs-md- umd-another-cyberattack-20140320,0,798878.story#ixzz3EAtmElmM

Ledley, R. & Wang, S. P. (2013). Computer Architecture and Security, Wiley, ISBN 978-1-1181-6881-3. January 2013.

Corresponding Author

V. J. Patwardhan*

CSE Dept, HSIT, Nidasoshi

E-Mail – vm.pvaidehi@gmail.com