SEPYCE - Security and Privacy in Computing Environment

Special Track along with FUTURE COMPUTING 2017, February 19 - 23, 2017 - Athens, Greece
https://www.iaria.org/conferences2017/FUTURECOMPUTING17.html

Woomin Hwang
National Security Research Institute
Daejeon, South Korea

Abstract—**Recent advances in computing environment provide users with not only great convenience but also increased risk that valuables are information will be lost, stolen, changed, or misused. Also, this risk extends to emerging systems of all kinds, including large-scale distributed systems, control systems, and embedded systems and it encompasses systems with hardware, software, and human components. Although attacks and defenses have been made for improving traditional security and privacy, the fast changing computing systems are always new and require research to solve many challenges. In this special track, two contributions address some research challenges and describe tools and systems to respond to them.**

Keywords–Security; Privacy; Threats.

I. Introduction

Recent advances in computing environment provide users with great convenience. Following rapid changes of user demands, computing environment changes fast and is more diversifying. Along with ordinary personal computing environments, for example, cloud computing, IoT (Internet of Things), the Bigdata market continues to mature. Cloud computing environment is getting popular for the active use of services like SaaS (Software as a Service) and Microservices. IoT platform permeates through our daily life with fast-growing services like smart home and connected cars. Bigdata is expected to contribute to ignite new business about all . Machine Learning is recently combined with previous computing platforms. Such a change represents a new era that technologies become embedded in our society in different ways. It is also shown as a major agenda, the fourth industrial revolution, of annual meetings by World Economic Forum since last year.

However, such advances in computing environment increase the risk that valuable information will be lost, stolen, changed, or misused. And these risks extend to emerging systems of all kinds, including large-scale distributed systems, control systems, and embedded systems and it encompasses systems with hardware, software, and human components. Gartner chose adaptive security architecture as one of the top 10 strategic technology trends in 2017 because of the rapid change of computing environment [1]. They also emphasized that computing systems and environments have to incorporate security considerations in their early design stages based on the understanding that security concerns need to be addressed in the system life cycle. In cyber security framework for such purposes, identifying security threats along with the response and recovery for incident handling is inevitable and requires more attention.

Various security threats are in action. Examples are like follows, but actual threats are not limited to them: attacks to the cloud computing environment, Internet of Things with least security considerations, APT (Adaptive Persistent Threat), Ransomwares [2], Possible security risks coming from open sources, etc.

Here, we briefly check recent security threats and methodologies to defend them.

II. Security Threats

Security threats are real and vulnerabilities attack valuable information on various computing environments.

A. In Cloud

Cloud computing environment is built on virtualization technology, which enables multiple tenants share a single instance of a computing resource. Because the extensibility of cloud is achieved by sharing resources, cloud service providers try to consolidate more tenants with less number of nodes. Though multi-tenancy gives benefits to deploying IT services, it may also add vulnerabilities to them. A vulnerability of a hypervisor makes all consolidated tenants susceptible to attack. There are number of CVEs (Common Vulnerabilities and Exposures) about major hypervisors as cloud computing become more popular.

Weak isolation of partitioned sharing resources by the service infrastructure may cause malicious attacker steal valuable information from other tenants. Several researches published that some architectural attacks are available, such as covert-/ side channels through microarchitectural timing attack utilizing CPU architecture and rowhammer attack originated from DRAM characteristics. They used various shared resources including branch predictor, caches, a memory bus, memory, and network. It may generate more serious problems with containers, which are a good way to deploy microservices. In addition, problems from resource-sharing technologies also affect data protection located in permanent storage. Along with the conventional Information leakage by the malicious insiders, data loss by various causes and tradeoffs between performance and isolability of each tenant can raise data breach problem. More threats can be found in [3][4][5].

B. In IoT (Internet of Things)

The number of IoT devices is estimated to reach 16 billion by 2021 [6]. If connected IoT devices are abused as routes of attacks for cyber criminals, malfunctioning devices for connected cars, home appliances, or healthcare would inflict damage to users properties. There was a DDoS attack on 20 September 2016, which shows that security threats come into a reality in our daily life. More than 500,000 IoT devices infected by a malware program, Mirai, performed the DDoS attack in DNS service, resulting in the inaccessibility of major websites including Twitter, Reddit, Netflix, and so on. As we can see from the example, it is necessary to embed security throughout the design process of IoT devices.

C. APTs (Advanced Persist Threats)

Advanced Persist Threat is a set of stealthy and continuous hacking processes often orchestrated by human targeting a specific entity. By adapting sociotechnical methodology, hackers try to find ways to reconnaissance, infiltrate, search, harvest, and exfiltrate. Because APT is a type of targeted attack, it is highly customized, uses a wide variety of techniques, and is performed over long periods of time. No standard characteristics of the threat indicate that ordinary users and security researches need to attend more about their defense against them.

D. Ransomware

In addition, we can think one more example, Ransomware. Ransomware is a type of malware that encrypts data on the compromised computer and compels the user to buy passwords to get data back. It causes financial damage to individuals, and the number of victim is increasing rapidly. Even a base infrastructure, San Francisco light rail system, was attacked by the HDDCryptor ransomware. CryptoLocker grossed more than $30 million in ransom in a hundred days. Because clones appear with different encryption methods and ransomware blackmarket explodes, more researches and incident response is required.

E. Additional Issues

In addition to the topics above, security breaches from the abuse of open sources, no preparation against game-changing hardwares, and privacy-preserving data usage problem become serious key issues for security.

III. Countermeasures

Researches and products have been proposed to deal with those threats. As traditional solutions, secure coding is a basic solution. If the reason of information leakage is from a resource-sharing environment, partition them or move tenants to another resource.

In general, the best way to defend the APTs is to ensure that users are prepared against targeted attacks. But there should be more effort to find solutions to mitigate potential risk from attacks. Automating vulnerability analysis tools and methodology could be one solution. Like what we have seen from successes in playing Go, it could be better if it combines with Artificial Intelligence trained for cyber security, though it requires more study.

For IoT devices, some researches try to discover software vulnerabilities, analyze codes, verify the correctness of implementation, and perform patches to the open sources frequently cloned and used. There are some researches and surveys for the networked IoT devices; a vulnerability discovery method based on cloned code verification [7], Software Defined Networking architectures [8][9], vulnerability scanning [10][11], white-box [12]/black-box testing [13], etc.

Digital forensics technologies continue to enhance its applicability. NIST published a guide for cybersecurity event recovery (800-184), which is an extended version of cyber security framework (800-53) by adding recovery features. Digital forensics technologies play an important role in responding and recovering phase of their seven phases of the cyber security framework. In cloud computing environment, the analysis result of the guest filesystem for VMs and records from the host filesystem for VM images help cloud monitoring systems better, thus making digital forensics technology widely applicable. Combined with host monitoring and analysis capabilities, recovery from data loss, auditing and compliances could be easier and give customers more detailed information.

Recent important change is the paradigm shift originated from the advance of artificial intelligence. Bigdata, AI with cloud will be used more to predict and respond to security threats. Bigdata based security solutions will make prediction and user behavioral analytics against cyber threats more practical. Artificial Intelligence will be applied to respond security threats automatically in realtime. There is policy supports to utilize potential impact of Bigdata. The US White House proposed the Consumer Privacy Bill of Rights Act of 2015 (CPBRA), which defines a basic concept of pseudonymization and contains principles and requirements for considering pseudonymized data as personal information. EU also defined anonymous/pseudonymous information and in the General Data Protection Regulation of 2016 (GDPR).

SECaaS market is going to grow rapidly. SECaaS (Security as a Service) [14] is a cost effective outsourced security management service when the total cost of ownership is considered. Companies can equip up-to-date security infrastructure with less maintenance cost by applying It. Its purpose is to provide up-to-date security services for incorporating infrastructure with less maintenance cost. It generally includes authentication, antivirus, malware detection, intrusion detection, and security management. According to a forecast, the SECaaS market size is estimated to grow from USD 3.12 Billion in 2015 to USD 8.52 Billion by 2020 [15].

Along with the fast technical advancement, sharing of threat intelligence and cooperative movement by security companies leads faster response to security threats. Cyber Threat Alliance (CTA) was co-founded by several security companies to share threat intelligence on attacks. Other global corporations run threat intelligence sharing platforms such as IBMs X-force Exchange, Microsofts Cybersecurity Engagement Center (CSEC), FireEyes iSight Threat Intelligence, and Threat Intelligence Exchange of McAfee.

IV. In This Track

In a special track on Security and Privacy in Computing Environment [16], held as part of the FUTURE COMPUTING 2017 conference in Athens, Greece, two contributions are presented that explains their recent researches about current security issues.

Hwang [17] describes an APT detection method by profiling user activities based on Indicator of Compromise (IOC) and chasing malware activities. He proposed an integrated detection architecture by using a customized open source host-based intrusion detection system and Virustotal's capabilities. In the system, one or more small agents are installed to a system to be monitored. Collected information is transferred to the manager for analysis and correlation. After getting details about suspicious files or processes from Virustotal, the manager checks whether it exists in Normal profile database and IOC database. It completes detection with the report. They tried to integrate with intelligent systems to cover frequently changing malwares the Virustotal cannot cover.

Choi [18] describes an intermediate result of malware analysis system with a deep introspection methodology. They focused on the fact that a malware analysis framework needs to control execution conditions to make malwares executable in sandbox. Conditions include location of specific files, registry file import before malware execution, and serial execution of multiple malwares. They also found that memory dump process should be accelerated to provide more information for analysis. As a solution, they proposed a malware analysis framework. For the framework, they customized existing Cuckoo sandbox to analyze malwares with various intended execution conditions. They also implemented API Trigger-based memory dump to extract hidden information from malware in memory. APIs for boosting memory dump is also implemented in the host, KVM hypervisor.

V. Conclusion

Fast-changing computing environments give us a lot of opportunities and drawbacks. Rapid propagation of Cloud computing, IoT and AI create more threats for its popularity and demand of quick deployment. There will be more countermeasures that makes inprovement in security techniques and policies as attacks are evolving and diversifying. Like the solutions that we discussed in this special track, we will find ways what we always have.

References

[1] Gartner, “Gartner’s Top 10 Strategic Technology Trends for 2017 - Smarter With Gartner,” Oct. 2016. [Online]. Available: http://www.gartner.com/smarterwithgartner/gartners-top-10-technology-trends-2017/

[2] C. Everett, “Ransomware: to pay or not to pay?” Computer Fraud & Security, vol. 2016, no. 4, Apr. 2016, pp. 8–12. [Online]. Available: http://linkinghub.elsevier.com/retrieve/pii/S1361372316300367

[3] CSA Top Threats Working Group, “The Treacherous 12: Cloud Computing Top Threats in 2016,” Tech. Rep., Feb. 2016.

[4] ITU-T Study Group 17, “Recommendation ITU-T X.1601 Security framework for cloud computing,” Oct. 2015. [Online]. Available: http://handle.itu.int/11.1002/1000/12613

[5] ENISA, “ENISA threat Landscape 2015 (ETL 2015),” ENISA, Jan. 2016. [Online]. Available: https://www.enisa.europa.eu/publications/etl2015

[6] “Ericsson Mobility Report - on the pulse of the networked society,” Tech. Rep., Jun. 2016. [Online]. Available: https://www.ericsson.com/res/docs/2016/ericsson-mobility-report-2016.pdf

[7] H. Li, J. Oh, H. Oh, and H. Lee, “Automated source code instrumentation for verifying potential vulnerabilities,” in IFIP International Information Security and Privacy Conference. Springer International Publishing, 2016, pp. 211–226.

[8] Z. Qin, G. Denker, C. Giannelli, P. Bellavista, and N. Venkatasubramanian, “A Software Defined Networking architecture for the Internet-of-Things,” in NOMS 2014 - 2014 IEEE/IFIP Network Operations and Management Symposium. IEEE, 2014, pp. 1–9. [Online]. Available: http://ieeexplore.ieee.org/document/6838365/

[9] V. R. Tadinada, “Software Defined Networking: Redefining the Future of Internet in IoT and Cloud Era,” in 2014 2nd International Conference on Future Internet of Things and Cloud (FiCloud). IEEE, 2014, pp. 296–301. [Online]. Available: http://ieeexplore.ieee.org/document/6984209/

[10] L. Markowsky and G. Markowsky, “Scanning for vulnerable devices in the Internet of Things.” IDAACS, 2015. [Online]. Available: http://ieeexplore.ieee.org/abstract/document/7340779/

[11] A. Costin, A. Zarras, and A. Francillon, “Automated Dynamic Firmware Analysis at Scale - A Case Study on Embedded Web Interfaces.” AsiaCCS, 2016, pp. 437–448. [Online]. Available: http://dl.acm.org/citation.cfm?doid=2897845.2897900

[12] J. Yang, H. Zhang, and J. Fu, “A Fuzzing Framework Based on Symbolic Execution and Combinatorial Testing.” GreenCom/iThings/CPScom, 2013. [Online]. Available: http://ieeexplore.ieee.org/abstract/document/6682399/

[13] J. Bau, E. Bursztein, D. Gupta, and J. C. Mitchell, “State of the Art - Automated Black-Box Web Application Vulnerability Testing.” IEEE Symposium on Security and Privacy, 2010. [Online]. Available: http://ieeexplore.ieee.org/abstract/document/5504795/

[14] A. Furfaro, A. Garro, and A. Tundis, “Towards Security as a Service (SecaaS): On the modeling of Security Services for Cloud Computing,” in 2014 International Carnahan Conference on Security Technology (ICCST). IEEE, pp. 1–6. [Online]. Available: http://ieeexplore.ieee.org/document/6986995/

[15] Markets and Markets, “Security as a Service Market worth 8.52 Billion USD by 2020 ,” Feb. 2016. [Online]. Available: http://www.marketsandmarkets.com/PressReleases/security-as-a-service.asp

[16] SEPYCE : Security and Privacy in Computing Environments, Athens, Greece. [Online]. Available: http://www.iaria.org/conferences2017/filesFUTURECOMPUTING17/SEPYCE.pdf

[17] S. O. Hwang, “APT Detection with Host Based Intrusion System and Intelligent Systems,” in Security and Privacy in Computing Environments, along with FUTURE COMPUTING 2017.

[18] S.-h. Choi, W. Hwang, and K.-W. Park, “Towards Software-Defined Malware Analysis with a Deep Introspection,” in Security and Privacy in Computing Environments, along with FUTURE COMPUTING 2017.