REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
13-08-2018	Final Report	1-Jun-2015 - 31-May-2018

4. TITLE AND SUBTITLE
Final Report: Moving Target Defense Through Dynamic Virtual Machine Placement in Clouds

5a. CONTRACT NUMBER
W911NF-15-1-0262

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
611102

6. AUTHORS

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
George Mason University
4400 University Drive, MSN 4C6

Fairfax, VA 22030 -4422

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS (ES)
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
66276-CS.12

12. DISTRIBUTION AVAILIBILITY STATEMENT
Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Songqing Chen
UU	UU	UU	UU		19b. TELEPHONE NUMBER 703-993-3176

RPPR Final Report
as of 22-Aug-2018

Agency Code:

Proposal Number: 66276CS **Agreement Number: W911NF-15-1-0262**
INVESTIGATOR(S):

Name: Songqing Chen
Email: sqchen@gmu.edu
Phone Number: 7039933176
Principal: Y

Organization: **George Mason University**
Address: 4400 University Drive, MSN 4C6, Fairfax, VA 220304422
Country: USA

DUNS Number: 077817450 EIN: 540836354
Report Date: 31-Aug-2018 Date Received: 13-Aug-2018
Final Report for Period Beginning 01-Jun-2015 and Ending 31-May-2018
Title: Moving Target Defense Through Dynamic Virtual Machine Placement in Clouds
Begin Performance Period: 01-Jun-2015 **End Performance Period:** 31-May-2018
Report Term: 0-Other

Submitted By: Songqing Chen Email: sqchen@gmu.edu
Phone: (703) 993-3176

Distribution Statement: 1-Approved for public release; distribution is unlimited.

STEM Degrees: 1 **STEM Participants:** 4

Major Goals: The major goal of this project is understand in-depth the principle of moving target defense (MTD) and utilize it to safe guard cloud computing and to mitigate the risks of potential compromises. For this purpose, in this project, we have investigated cloud virtualization and security from both theoretical and practical perspectives in order to establish a foundation for moving target defense strategies in clouds, and to create new cost-effective defense strategies to improve cloud security.

Accomplishments: To achieve our proposed objectives, we have conducted our research which can be classified into three parts: (1) the modeling part that addresses when to move, and where to move; (2) the system part that focuses on the cloud side-channel attacks and the new designs of hypervisor scheduling that takes into MTD into account; (3) the new applications and defenses that focuses on EDoS. Please refer to the attached report for more details.

Training Opportunities: All students participating this project have gained extensive research experience, from theoretical and/or system perspectives, on security, particular cloud security and virtualization, and either have completed the degree or are making steady progress towards their degrees.

At GMU, a female Ph.D. student, Huangxin Wang, has dedicated to this project. She works on two aspects (theoretical and applications) trying to pursue in-depth understanding of MTD principles and its applications on EDoS. She has successfully defended her dissertation, titled as "E♂ective and Economical Moving Target Defense for Secure Cloud Computing" and joined Facebook. She was co-directed by Dr. Songqing Chen and Dr. Fei Li, two PIs of the project.

In addition, another Ph.D. student from GMU, Li Liu, has also dedicated to this project and mainly focused on the system perspective by trying to utilize the MTD principle to the scheduling in order to safeguard the cloud infrastructure.

At TAMU, a female undergraduate student, Sara Ballard, and a disability undergraduate student, Harry Staley, have participated in this project. They have been working on the risk evaluation and placement optimization.

RPPR Final Report
as of 22-Aug-2018

Results Dissemination: We have presented our research results in various occasions and conferences and journals, such as the10th USENIX Workshop on Offensive Technologies (WOOT '16), Austin, TX, August 8–9, 2016; IEEE Conference on Communications and Network Security (CNS) 2016, Philadelphia, PA USA; the International Conference on Security and Privacy in Communication Networks (SECURECOMM'2016); the 37th IEEE International Conference on Distributed Computing Systems (ICDCS 2017), Atlanta, GA, June 5-8, 2017; the 31st Annual IFIP WG 11.3 Conference on Data and Applications Security and Privacy (DBSec'17), Philadelphia, PA, July 19-21, 2017; the IEEE
International Conference on Communications (ICC) held on Kansas City, Mo, May 20-24, 2018; the 14th EAI International Conference on Security and Privacy in Communication Networks (SecureComm 2018), held at Singapore, August 8-10, 2018.

Honors and Awards: Nothing to Report

Protocol Activity Status:

Technology Transfer: Nothing to Report

PARTICIPANTS:

Participant Type: PD/PI
Participant: Songqing Chen
Person Months Worked: 9.00 **Funding Support:**
Project Contribution:
International Collaboration:
International Travel:
National Academy Member: N
Other Collaborators:

Participant Type: Co PD/PI
Participant: Fei Li
Person Months Worked: 8.00 **Funding Support:**
Project Contribution:
International Collaboration:
International Travel:
National Academy Member: N
Other Collaborators:

Participant Type: Co PD/PI
Participant: Wanyu Zang
Person Months Worked: 8.00 **Funding Support:**
Project Contribution:
International Collaboration:
International Travel:
National Academy Member: N
Other Collaborators:

Participant Type: Co PD/PI
Participant: Meng Yu
Person Months Worked: 8.00 **Funding Support:**
Project Contribution:
International Collaboration:
International Travel:
National Academy Member: N
Other Collaborators:

RPPR Final Report
as of 22-Aug-2018

Participant Type: Graduate Student (research assistant)
Participant: Huangxin Wang
Person Months Worked: 15.00 **Funding Support:**
Project Contribution:
International Collaboration:
International Travel:
National Academy Member: N
Other Collaborators:

Participant Type: Graduate Student (research assistant)
Participant: Li Liu
Person Months Worked: 15.00 **Funding Support:**
Project Contribution:
International Collaboration:
International Travel:
National Academy Member: N
Other Collaborators:

ARTICLES:

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
Journal: The 10th USENIX Workshop on Offensive Technologies (WOOT)
Publication Identifier Type: Other Publication Identifier:
Volume: Issue: First Page #:
Date Submitted: 8/8/16 12:00AM Date Published: 8/8/16 2:05PM
Publication Location:
Article Title: Abusing Public Third-Party Services for Cloud EDoS Attacks
Authors: Huangxin Wang, Zhonghua Xi, Fei Li, and Songqing Chen
Keywords: Cloud attacks, EDoS
Abstract: Cloud computing has been widely adopted nowadays as it provides economical, elastic and scalable services to customers. The cloud resources are offered in an on demand manner and the consumers are charged based on their resource usage, known as “pay-as-you-go.” Such a cloud utility scheme opens the door to Economic Denial of Sustainability (EDoS) attacks in which the cloud consumers would suffer from financial losses. In this paper, we uncover the severity of EDoS attacks through demonstrating that EDoS attacks can be easily conducted at very low costs. In specific, we show that attackers can launch amplification attacks against the cloud consumers by abusing the free public third-party services provided by the Internet giants such as Google, Microsoft, Facebook and LinkedIn. Through studying the characteristics of 10 main public third-party services, we reveal that all of them can be abused to launch EDoS attacks and the amplification factor can reach up to 135K. To combat against the
Distribution Statement: 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support: **Y**

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
Journal: Journal of Computer Security
Publication Identifier Type: DOI Publication Identifier: 10.3233/JCS-171104
Volume: Pre-press Issue: Pre-press First Page #: 1
Date Submitted: 8/6/18 12:00AM Date Published: 3/1/18 10:00AM
Publication Location:
Article Title: Risk-aware multi-objective optimized virtual machine placement in cloud
Authors: Jin Han, Wangyu Zang, Li Liu, Songqing Chen, Meng Yu
Keywords: Cloud security, multiple objective, virtual machine placement, risk metrics model, VM allocation strategy
Abstract: Cloud computing, while becoming more and more popular as a dominant computing platform, introduces new securitychallenges. When virtual machines are deployed in a cloud environment, virtual machine placement strategies can significantlyaffect the overall security risks of the entire cloud. In recent years, the attacks are specifically designed to co-locate with target virtual machines in the cloud. The virtual machine placement without considering the security risks may put the users, or even the entire cloud, in danger. In this paper, we present a comprehensive approach to quantify the security risk of cloud environments from network, host and VM. Accordingly, we propose a Security-aware Multi-Objective Optimization based virtual machine Placement scheme (SMOOP) to seek a Pareto-optimal solution that reduces the overall security risks of a cloud, while considering workload balance, resource utilization on CPU, memory, disk, and network traffic. New placement strategies are designed
Distribution Statement: 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support: **Y**

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
Journal: ICST Transactions on Security and Safety
Publication Identifier Type: DOI Publication Identifier: 10.4108/eai.4-1-2018.153525
Volume: 4 Issue: 13 First Page #: 153525
Date Submitted: 8/6/18 12:00AM Date Published: 1/1/18 5:00AM
Publication Location:
Article Title: Attribution of Economic Denial of Sustainability Attacks in Public Clouds
Authors: Mohammad Karami, An Wang, Songqing Chen
Keywords: Economic Denial of Sustainability, EDoS Detection, Markov Chain, Hidden semi Markov Model
Abstract: The cloud pricing model leaves cloud consumers vulnerable to Economic Denial of Sustainability (EDoS) attacks. In this type of attacks, an adversary first identifies web resources with high levels of cloud resource consumption, and then uses a botnet of compromised hosts to make fraudulent requests to these costly web resources. The attacker's goal is to disrupt the economical sustainability of the victim by inflicting cost through fraudulent consumption of billable cloud resources. In this paper, we propose two different Markov-based models to profile the behavior of legitimate users in terms of their resource consumption and the resource request patterns to detect malicious sources engaged in fraudulent use of cloud resources. Our experimental evaluation results demonstrate the effectiveness of the proposed attribution methodology for identifying malicious sources participating in EDoS attacks.
Distribution Statement: 1-Approved for public release; distribution is unlimited.
Acknowledged Federal Support: **Y**

CONFERENCE PAPERS:

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: the 10th USENIX Workshop on Offensive Technologies (WOOT '16)
Date Received: 08-Aug-2016 Conference Date: 08-Aug-2016 Date Published: 08-Aug-2016
Conference Location: Austin, TX
Paper Title: Abusing Public Third-Party Services for EDoS Attacks
Authors: Huangxin Wang, Zhonghua Xi, Fei Li, and Songqing Chen
Acknowledged Federal Support: **Y**

RPPR Final Report
as of 22-Aug-2018

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: IEEE Conference on Communications and Network Security (CNS)
Date Received: 08-Aug-2017 Conference Date: 17-Oct-2016 Date Published: 17-Oct-2016
Conference Location: Philadelphia, PA
Paper Title: ExtensionGuard: Towards Runtime Browser Extension Information Leakage Detection
Authors: Wentao Chang; Songqing Chen
Acknowledged Federal Support: **Y**

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: The 12th EAI International Conference on Security and Privacy in Communication Networks (SECURECOMM)
Date Received: 08-Aug-2017 Conference Date: 10-Oct-2016 Date Published: 10-Oct-2016
Conference Location: Guangzhou, China
Paper Title: Attribution of Economic Denial of Sustainability Attacks in Public Clouds
Authors: Mohammad Karami; Songqing Chen
Acknowledged Federal Support: **Y**

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: Proceedings of the third ACM Workshop on Moving Target Defense (MTD 2016)
Date Received: 08-Aug-2017 Conference Date: 25-Oct-2016 Date Published: 25-Oct-2016
Conference Location: Vienna, Austria
Paper Title: Towards Cost-Effective Moving Target Defense Against DDoS and Covert Channel Attacks
Authors: Huangxin Wang; Fei Li; Songqing Chen
Acknowledged Federal Support: **Y**

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: Proceedings of the 37th IEEE International Conference on Distributed Computing Systems (ICDCS 2017)
Date Received: 08-Aug-2017 Conference Date: 05-Jun-2017 Date Published: 07-Jun-2017
Conference Location: Atlanta, GA
Paper Title: An Adversary-Centric Behavior Modeling of DDoS Attacks
Authors: An Wang; Aziz Mohaisen; Songqing Chen
Acknowledged Federal Support: **Y**

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: Proceedings of the 31st Annual IFIP WG 11.3 Conference on Data and Applications Security and Privacy (DBSec'17)
Date Received: 08-Aug-2017 Conference Date: 19-Jul-2017 Date Published: 20-Jul-2017
Conference Location: Philadelphia, PA
Paper Title: Reducing Security Risks of Clouds through Virtual Machine Placement
Authors: Jin Han; Wanyu Zang; Songqing Chen; Meng Yu
Acknowledged Federal Support: **Y**

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: Proceedings of the IEEE International Conference on Communications (ICC'2018)
Date Received: 06-Aug-2018 Conference Date: 20-May-2018 Date Published: 20-May-2018
Conference Location: Kansas City, MO
Paper Title: Empirical Evaluation of the Hypervisor Scheduling on Side Channel Attacks
Authors: Li Liu, An Wang, Wanyu Zang, Meng Yu, Songqing Chen
Acknowledged Federal Support: **Y**

RPPR Final Report
as of 22-Aug-2018

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: Proceedings of the 14th EAI International Conference on Security and Privacy in Communication Networks (SecureComm'2018)
Date Received: 13-Aug-2018 Conference Date: 08-Aug-2018 Date Published: 08-Aug-2018
Conference Location: Singapore, Singapore
Paper Title: Shuffler: Mitigate Cross-VM Side-channel Attacks via Hypervisor Scheduling
Authors: Li Liu, An Wang, Wanyu Zang, Meng Yu, Mengbai Xiao, Songqing Chen
Acknowledged Federal Support: **Y**

Final Report

The major goal of this project is understand in-depth the principle of moving target defense (MTD) and utilize it to safe guard cloud computing and to mitigate the risks of potential compromises. For this purpose, we investigate cloud virtualization and security from both theoretical and practical perspectives. The objectives are to establish a foundation for moving target defense strategies in clouds, and to create new cost-effective defense strategies to improve cloud security. To achieve our proposed goals, our research has mainly been conducted along three thrusts: modeling, systems, and applications.

Through this project, we have published our research results over 10 papers so far, and a female Ph.D. student at GMU has successfully defended her dissertation, titled "Effective and Economical Moving Target Defense for Secure Cloud Computing", and joined Facebook. Another Ph.D. student at GMU is actively formulating his disertation on the MTD. In addition, at TAMU, a female undergraduate student, Sara Ballard, and a disability undergraduate student, Harry Staley, have participated in this project. They have been working on the risk evaluation and placement optimization. The following summarizes our major research activities conducted in the project period with more details provided in the annual interim reports.

1 Modeling MTD

Through modeling, we aim to achieve better and in-depth understanding of MTD principles. Our work has mainly focused on the when to move and where to move.

1.1 Towards Cost-Effective Moving Target Defense Against DDoS and Covert Channel Attacks

Traditionally, network and system configurations are static. Attackers have plenty of time to exploit the system's vulnerabilities and thus they are able to choose when to launch attacks wisely to maximize the damage. An unpredictable system configuration can significantly lift the bar for attackers to conduct successful attacks. Recent years, moving target defense (MTD) has been advocated for this purpose. An MTD mechanism aims to introduce dynamics to the system through changing its configuration continuously over time, which we call adaptations. Though promising, the dynamic system reconfiguration introduces overhead to the applications currently running in the system. It is critical to determine the right time to conduct adaptations and to balance the overhead afforded and the security levels guaranteed. This problem is known as the MTD timing problem. Little prior work has been done to investigate the right time in making adaptations. In this study, we take the first step to both theoretically and experimentally study the timing problem in moving target defenses. For a broad family of attacks including DDoS attacks and cloud covert channel attacks, we model this problem as a renewal reward process and propose an

optimal algorithm in deciding the right time to make adaptations with the objective of minimizing the long-term cost rate. In our experiments, both DDoS attacks and cloud covert channel attacks are studied. Simulations based on real network traffic traces are conducted and we demonstrate that our proposed algorithm outperforms known adaptation schemes. For more details, please refer to the following paper:
1. Huangxin Wang, Fei Li, and Songqing Chen. "Towards Cost-Effective Moving Target Defense Against DDoS and Covert Channel Attacks". Proceedings of the third ACM Workshop on Moving Target Defense (MTD 2016), Vienna, Austria, October 24, 2016.

1.2 Reducing Security Risks of Clouds through Virtual Machine Placement

Cloud computing, while becoming more and more popular as a dominant computing platform, introduces new security challenges. When virtual machines are deployed in a cloud environment, virtual machine placement strategies can significantly affect the overall security risks of the entire cloud. In recent years, the attacks are specifically designed to co-locate with target virtual machines in the cloud. The virtual machine placement without considering the security risks may put the users, or even the entire cloud, in danger. In this study, we present a comprehensive approach to quantify the security risk of cloud environments from network, host and VM. Accordingly, we propose a Security-aware Multi-Objective Optimization based virtual machine Placement scheme (SMOOP) to seek a Pareto-optimal solution that reduces the overall security risks of a cloud, while considering workload balance, resource utilization on CPU, memory, disk, and network traffic. New placement strategies are designed and our evaluation results demonstrate their effectiveness. The security of clouds could be improved with affordable overheads. The latest VM allocation policies are further studied and integrated into our designs to defeat the co-residence attacks. For more details, please refer to the following two papers:
2. Jin Han, Wanyu Zang, Songqing Chen, and Meng Yu. "Reducing Security Risks of Clouds through Virtual Machine Placement". Proceedings of the 31st Annual IFIP WG 11.3 Conference on Data and Applications Security and Privacy (DBSec'17), Philadelphia, PA, July 19-21, 2017.
3. Jin Han, Wanyu Zang, Li Liu, Songqing Chen, and Meng Yu. "Risk-aware Multi-objective Optimized Virtual Machine Placement in Cloud". Journal of Computer Security, pp. 1-24, March 2018. DOI: 10.3233/JCS- 171104

1.3 An Adversary-Centric Behavior Modeling of DDoS Attacks

Distributed Denial of Service (DDoS) attacks are some of the most persistent threats on the Internet today. The evolution of DDoS attacks calls for an in-depth analysis of those attacks. A better understanding of the attackers' behavior can provide insights to unveil patterns and strategies utilized by attackers. The prior art on the attackers' behavior analysis often falls in two aspects: it assumes that adversaries are static, and makes certain simplifying assumptions on their behavior, which often are not supported by real attack data. In this study, we take a data-driven approach to designing and validating three DDoS attack models from temporal (e.g., attack magnitudes), spatial (e.g., attacker origin), and spatiotemporal (e.g., attack inter-launching time) perspectives. We design these models based on the analysis of traces consisting of more than 50,000 verified DDoS attacks from industrial mitigation operations. Each model is also validated by testing its effectiveness in accurately predicting future DDoS attacks. Comparisons against simple intuitive models further show that our models can more accurately capture the essential features of DDoS

attacks. For more details, please refer to the following two papers:
4. An Wang, Aziz Mohaisen, and Songqing Chen. "An Adversary-Centric Behavior Modeling of DDoS Attacks". Proceedings of the 37th IEEE International Conference on Distributed Computing Systems (ICDCS 2017), Atlanta, GA, June 5-8, 2017.
5. An Wang, Wentao Chang, Songqing Chen, and Aziz Mohaisen. "A Data-Driven Study of DDoS Attacks and Their Dynamics". IEEE Transactions on Dependable and Secure Computing, Vol. 14, No. 8, August 2018.

2 MTD to Improve Cloud Security

Besides the theoretical work through modeling, we also consider to adopt MTD principle in clouds to deal with side channel attacks.

2.1 Empirical Evaluation of the Hypervisor Scheduling on Side Channel Attacks

Along with the wide adoption of the cloud platform, various attacks also target clouds. Due to the sharing of the underlying physical resources among different virtual machines (VMs), various side-channel attacks have been demonstrated to be capable of stealing victim's secret information, such as encryption key, by monitoring the victim's access pattern to a shared hardware, such as CPU cache. Among various defense mechanisms proposed, the hypervisor scheduling based schemes shed some light on lightweight solutions that are more likely to be adopted in practice. However, scheduling is affected by several factors that have not been thoroughly investigated so far. In this study, we aim to study in-depth the impact of various factors affecting the hypervisor scheduling, with the objective to understand their impact on mitigating these side-channel attacks. Our results can not only deepen our understanding, but also provide some guidelines to design effective scheduling based defenses in the future. For more details, please refer to the following paper:
6. Li Liu, An Wang, Wanyu Zang, Meng Yu, and Songqing Chen. "Empirical Evaluation of the Hypervisor Scheduling on Side Channel Attacks". Proceedings of the IEEE International Conference on Communications (ICC'2018), Kansas City, MO, May 20-24, 2018.

2.2 Shuffler: Mitigate Cross-VM Side-channel Attacks via Hypervisor Scheduling

Cloud computing relies on resources sharing to achieve high resource utilization and economy of scale. Meanwhile, contention on shared resources opens doors for co-located virtual machines (VMs) to have negative impacts on each other, and even introduces vulnerabilities such as information leakage. For example, via CPU cache-based side-channel attacks, an attacker VM can extract crypto keys from a victim VM.

To cost-effectively secure the cloud against those threats without sacrificing resource sharing, in this paper, we first investigate the factors that can impact the success of such attacks. Our investigation reveals that the root cause of such attacks is the constant sharing patterns of hardware resources between VMs. Based on our findings, we quantify the negative impacts a VM can have on another VM on the same machine using the *vulnerable probability*, and propose lightweight and generic scheduler-based defense mechanisms called *Shuffler schedulers*, which can effectively limit

the vulnerable probability of all VMs. The key is that distributing CPU time to vCPUs with equal probability would reduce the overall vulnerable probability of the system. Our analyses and experimental results show that the Shuffler schedulers can effectively reduce information leakage to mitigate cross-VM side-channel attacks, with little performance penalty while preserving high resource utilization. For more details, please refer to the following paper:
7. Li Liu, An Wang, Wanyu Zang, Meng Yu, Mengbai Xiao, and Songqing Chen. "Shuffler: Mitigate Cross-VM Side-channel Attacks via Hypervisor Scheduling". Proceedings of the 14th EAI International Conference on Security and Privacy in Communication Networks (SecureComm'2018), Singapore, Singapore, August 8-10, 2018.

3 Using MTD in other Applications

Beyond the cloud infrastructure, we have also considered other cloud threats and application contexts, such as EDoS, and aimed to develop MTD based detection and mitigation strategies.

3.1 Abusing Public Third-Party Services for Cloud EDoS Attacks

Cloud computing has been widely adopted nowadays as it provides economical, elastic and scalable services to customers. The cloud resources are offered in an on demand manner and the consumers are charged based on their resource usage, known as pay-as-you-go. Such a cloud utility scheme opens the door to Economic Denial of Sustainability (EDoS) attacks in which the cloud consumers would suffer from financial losses. In this study, we uncover the severity of EDoS attacks through demonstrating that EDoS attacks can be easily conducted at very low costs. In specific, we show that attackers can launch amplification attacks against the cloud consumers by abusing the free public third-party services provided by the Internet giants such as Google, Microsoft, Facebook and LinkedIn. Through studying the characteristics of 10 main public third-party services, we reveal that all of them can be abused to launch EDoS attacks and the amplification factor can reach up to 135K. To combat against the uncovered attacks, we propose several mitigation strategies for the third-party service providers as well as the cloud consumers. For more details, please refer to the following paper:
8. Huangxin Wang, Zhonghua Xi, Fei Li, and Songqing Chen. "Abusing Public Third-Party Services for EDoS Attacks". Proceedings of the 10th USENIX Workshop on Offensive Technologies (WOOT'16), Austin, TX, August 8-9, 2016.

3.2 Attribution of Economic Denial of Sustainability Attacks in Public Clouds

The cloud pricing model leaves cloud consumers vulnerable to Economic Denial of Sustainability (EDoS) attacks. In this type of attacks, an adversary first identifies web resources with high levels of cloud resource consumption, and then uses a botnet of compromised hosts to make fraudulent requests to these costly web resources. The attackers goal is to disrupt the economical sustainability of the victim by inflicting cost through fraudulent consumption of billable cloud resources. In this study, we propose two different Markov-based models to profile the behavior of legitimate users in terms of their resource consumption and the resource request patterns to detect malicious sources engaged in fraudulent use of cloud resources. Our experimental evaluation results demonstrate the effectiveness of the proposed attribution methodology for identifying malicious sources participating

in EDoS attacks. For more details, please refer to the following papers:
9. Mohammad Karami and Songqing Chen. "Attribution of Economic Denial of Sustainability Attacks in Public Clouds". Proceedings of the International Conference on Security and Privacy in Communication Networks (SECURECOMM'2016), Guangzhou, China, Oct. 10-12, 2016.
10. Mohammad Karami, An Wang, and Songqing Chen. "Attribution of Economic Denial of Sustainability Attacks in Public Clouds". ICST Transactions on Security Safety, 4(13): e2, 2018.

3.3 ExtensionGuard: Towards Runtime Browser Extension Information Leakage Detection

Many browser extensions process sensitive information, such as bookmarks and browsing history that are available from the browsers, and social security number and password that are shown on Web pages. Thus, an increasing interest has been growing among attackers to exploit this new attacking platform to compromise browser security. The most common attacks from malicious extensions include accessing users' sensitive information and leaking them to unauthorized third parties. Some recent studies discussed the possible attacks launched from malicious extensions but few proposed practical solutions to address the issue. In this study, we present the ExtensionGuard, an optimized and customizable dynamic taint tracking system that can closely track the sensitive information processed by browser extensions, and detect any information leakage events at runtime. We evaluate ExtensionGuard against a set of malicious and benign extensions. The evaluation results show that ExtensionGuard is able to effectively mitigate various information leakage attacks without incurring high performance overhead. For more details, please refer to the following paper:
11. Wentao Chang and Songqing Chen. "ExtensionGuard: Towards Runtime Browser Extension Information Leakage Detection". Proceedings of the IEEE Conference on Communications and Network Security (CNS'2016), Philadelphia, PA, Oct. 17-19, 2016.