REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
12-01-2023	Final Report	25-Dec-2018 - 24-Sep-2022

4. TITLE AND SUBTITLE
Final Report: Information Retrieval in Clouds

5a. CONTRACT NUMBER
W911NF-19-1-0049

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
University of Delaware
210 Hullihen Hall

Newark, DE 19716 -0099

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)
70963-NC.3

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			Haining Wang
UU	UU	UU	UU		19b. TELEPHONE NUMBER 302-831-6865

RPPR Final Report
as of 25-Jan-2023

Agency Code: 21XD

Proposal Number: 70963NC **Agreement Number: W911NF-19-1-0049**
INVESTIGATOR(S):

Name: Haining Wang
Email: hnw@udel.edu
Phone Number: 3028316865
Principal: Y

Name: Jidong Xiao
Email: jidongxiao@boisestate.edu
Phone Number: 2084264420
Principal: N

Organization: **University of Delaware**
Address: 210 Hullihen Hall, Newark, DE 197160099
Country: USA
DUNS Number: 059007500 EIN: 516000297

Report Date: 24-Dec-2022 Date Received: 12-Jan-2023
Final Report for Period Beginning 25-Dec-2018 and Ending 24-Sep-2022
Title: Information Retrieval in Clouds
Begin Performance Period: 25-Dec-2018 **End Performance Period:** 24-Sep-2022
Report Term: 0-Other

Submitted By: Haining Wang Email: hnw@udel.edu
Phone: (302) 831-6865

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

STEM Degrees: **STEM Participants:**

Major Goals: Cloud computing nowadays is prevalent in our daily life, and it has been commonly used to provide IT [Information Technology] services over the Internet. Virtualization, as the foundation and main enabling technology of cloud computing, has played a crucial role in computing resource management inside a cloud, sharing finite hardware resources among a large number of software systems and programs. However, the security of virtualization has become a major concern for organizations and individuals who are hesitating to deploy their critical applications or data in cloud environments. This is mainly due to the fact that a hypervisor, which is a key component of virtualization and is controlled by cloud vendors, runs directly on the hardware or a host operating system [OS] to create and manage the guest OSes and have a higher privilege level than guest OSes. While significant research efforts have been paid to understand the cyber threats exposed by cloud computing, it is yet unclear how insecure/secure cloud environments are.

This project attempts to seek an answer for this question from a new and different perspective: information retrieval in clouds. In particular, we consider to retrieve information in two directions. One direction is from attackers' point of view, we investigate how much sensitive information attackers can obtain; the other direction is from defenders' perspective, we investigate how much sensitive information defenders can collect. The research will serve as a catalyst to promote the security level in cloud environments. The exploration of VME will help us understand how much security risk and vulnerability attackers can cause if they gain in-depth knowledge of underlying hypervisors via information retrieval, and then we will develop corresponding countermeasures to prevent such information leakage and reduce the damage. The further investigation of VMI will enable us to build a one-for-many VMI and memory enhance forensic tool, which will significantly enhance existing defense techniques such as intrusion detection.

Our final goals include: (1) collect hypervisor information so as to build hypervisor fingerprints, (2) build a cover channel to transfer information secretly, and (3) extend VMI techniques to enable more powerful inspections of a target VM, such as detecting nested VM rootkit and reconstructing memory based file systems.

Accomplishments: VME: From attackers' perspective, we have investigated how attackers can utilize processor model specific registers (MSRs) to collect and transfer information. MSRs are special registers in computer

processors used for collecting information or triggering certain CPU features. They are especially useful for performance monitoring or debugging. There is a large volume of MSRs: CPU vendors such as Intel and AMD have defined hundreds of MSRs for their processors. Actually, Intel has dedicated one entire volume of their software developer's manual (SDM), which consists of more than 400 pages, explaining the behaviors of each MSR. For this reason, over the years, we have constantly seen developers submitting patches in the KVM or Xen community to fix MSR related issues. We have observed that many MSRs in a virtual machine exhibit different behaviors when the underlying hypervisors are different. Based on such a difference, we can, from inside the virtual machine, build a fingerprint of the underlying hypervisor.

We also investigated the security implications of virtual machine live migration and how attackers can tamper with regular VM migrations. What we found has been reported in the paper “Understanding the Security Implication of Aborting Live Migration,” which has been published in the IEEE Transactions on Cloud Computing (TCC) in 2020. In order for attackers to perform the above attacks, they first need to identify a vulnerability in the system so that they can either take over the system, or launch attacks against the vulnerability. Unfortunately, due to complexity of operating systems, such vulnerabilities are commonly existed.

Moreover, we developed a nested virtual machine- based rootkit, which utilizes the virtual machine live migration technique to migrate a target virtual machine into a nested virtualized environment. Such an attack allows attackers to actively or passively collect victim’s sensitive information. We evaluated the time it takes to launch such an attack, and the performance overhead it incurs in the virtualized environment. We also proposed and developed a detection mechanism that can effectively detect such attacks. This task has been completed and our findings and results have been reported in a research paper published in 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) in 2021.

VMI: From defenders’ perspective, we plan to extend VMI technique to support more functionalities. More specifically, we aim to detect whether or not the target virtual machine is actually running as a hypervisor, thus allows another (nested) virtual machine running inside it. Detecting such a situation allows defenders to determine whether or not a virtual machine has been compromised, or a nested VM based rootkit is installed. Our approach is based on a technique called memory deduplication. More specifically, we develop and run a detection program at the host level, when nested virtualization is existing, certain memory pages are expected to be existing in both the inner-most virtual machine and the middle-layer hypervisor. And the duplication of these memory pages will trigger memory page merging. Based on this, we can determine whether or not the middle-layer hypervisor is existing.

When vulnerabilities are discovered, patches will be developed and should be applied as soon as possible. The team therefore also studied how to apply patches efficiently without incurring significant downtime. To this end, the team
developed a novel live patching method which utilizes both the SMM and the SGX. Our findings and results were report in a research paper, which has been published in the 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) in 2020. This paper was nominated for the best paper award at the conference, one of the 3 nominees, out of 291 submissions. Our team also investigated how to collect the target system’s sensitive information and therefore protect and introspect a target system from a lower-level by leveraging the Intel Management Engine (Intel ME). The resulted paper “Nighthawk: Transparent System Introspection from Ring -3” has been published in the 24th European Symposium on Research in Computer Security (ESORICS) in 2019.

We also developed a user-level crypto engine which stores sensitive information (such as crypto keys) in debug registers as well as in CPU cache. Compared to existing works, our engine runs in user level, as opposed to kernel level, which means our engine requires less privilege most of the time, and when privilege is truly needed, we leverage the virtualization technology comes with modern x86 CPUs, which allows us to switch between root mode and non-root mode. Overall, our engine protects sensitive keys against memory base attacks such as the cold boot attack.

Training Opportunities: At the University of Delaware, One Ph.D. student participated in the proposed research tasks. At the Boise State University, one Ph.D. student and one undergraduate student were involved in the development and evaluation of the proposed VME and VMI approaches. These students have received detailed instructions and mentoring in cloud security and computer system research. In particular, they learned virtualization technology, investigated hypervisor implementations, and explored from security perspectives, what problems are existing in current mainstream hypervisors, and what we can do to address these problems. The knowledge and skills that the students have learned can be applicable to broad areas of security and system research.

RPPR Final Report
as of 25-Jan-2023

Results Dissemination: - Xing Gao, Jidong Xiao, Haining Wang, Angelos Stavrou, "Understanding the Security Implication of Aborting Virtual Machine Live Migration", IEEE Transactions on Cloud Computing (TCC), 10(2): 1275-1286 (2022)

- Patrick Cronin, Xing Gao, Haining Wang, Chase Cotton, "Time-Print: Authenticating USB Flash Drives with Novel Timing Fingerprint", IEEE Symposium on Security and Privacy 2022: 1002-1017.

- Jidong Xiao, Lei Lu, Hai Huang, Haining Wang, "Virtual Machine Extrospection: A Reverse Information Retrieval in Clouds", IEEE Transactions on Cloud Computing 9(1): 401-413 (2021).

- Joseph Connelly, Taylor Roberts, Xing Gao, Jidong Xiao, Haining Wang, Angelos Stavrou, “CloudSkulk: A Nested Virtual Machine Based Rootkit and Its Detection", The 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), June, 2021.

- Patrick Cronin, Xing Gao, Haining Wang, Chase Cotton, "An Exploration of ARM System-Level Cache and GPU Side Channels", ACSAC 2021: 784-795.

- Patrick Cronin, Xing Gao, Chengmo Yang, and Haining Wang,
"Charger-Surfing: Exploiting a Power Line Side-Channel for Smartphone Information Leakage", In USENIX Security Symposium 2021, Vancouver, BC, Canada, August 2021.

- Xing Gao, Jidong Xiao, Haining Wang, and Angelos Stavrou, "Understanding the Security Implication of Aborting Live Migration" IEEE Transactions on Cloud Computing (TCC), 2020.

- Lei Zhou, Fengwei Zhang, Jinghui Liao, Zhenyu Ning, Jidong Xiao, Kevin Leach, Westley Weimer, and Guojun Wang, "KShot: Live Kernel Patching with SMM and SGX", The 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Valencia, Spain, June, 2020. Best Paper Award Nomination (3 out of 291 submissions).

- Lei Zhou, Jidong Xiao, Kevin Leach, Westley Weimer, Fengwei Zhang, and Guojun Wang, "Nighthawk: Transparent System Introspection from Ring-3", The 24th European Symposium on Research in Computer Security (ESORICS), Luxembourg, September, 2019.

Honors and Awards: - IEEE Fellow for the contribution of network and cloud security (Haining Wang)

- Best Paper Nominee at the 50th IEEE/IFIP DSN 2020 (Jidong Xiao)

- Ph.D, Awarded in July, 2021 (Patrick Cronin)

Protocol Activity Status:

Technology Transfer: Nothing to Report

PARTICIPANTS:

Participant Type: PD/PI
Participant: Haining Wang
Person Months Worked: 1.00 **Funding Support:**
Project Contribution:
National Academy Member: N

Participant Type: Co PD/PI
Participant: Jidong Xiao
Person Months Worked: 1.00 **Funding Support:**
Project Contribution:

National Academy Member: N

Participant Type: Graduate Student (research assistant)
Participant: Patrick Cronin
Person Months Worked: 12.00 **Funding Support:**
Project Contribution:
National Academy Member: N

Participant Type: Graduate Student (research assistant)
Participant: Shariful Alam
Person Months Worked: 12.00 **Funding Support:**
Project Contribution:
National Academy Member: N

Participant Type: Undergraduate Student
Participant: Taylor Roberts
Person Months Worked: 4.00 **Funding Support:**
Project Contribution:
National Academy Member: N

ARTICLES:

Publication Type: Journal Article Peer Reviewed: Y **Publication Status:** 1-Published
Journal: IEEE Transactions on Cloud Computing
Publication Identifier Type: DOI Publication Identifier:
Volume: Issue: First Page #:
Date Submitted: 9/1/19 12:00AM Date Published:
Publication Location:
Article Title: Understanding the Security Implication of Aborting Live Migration
Authors: Gao, Xing Gao and Xiao, Jidong Xiao and Wang, Haining Wang and Stavrou, Angelos Stavrou
Keywords: Virtual Machine, Live Migration, TCP Reset Attack, Cloud
Abstract: Live migration of Virtual machines (VMs) has become a regular tool for edge and cloud operators to facilitate system maintenance, fault tolerance, and load balancing, with little impact on running instances. However, the potential security risks of live migration of VMs are still obscure. In this paper, we expose a new vulnerability in the existing VM live migration approaches, especially the post-copy approach. The entire live migration mechanism relies upon reliable TCP connectivity for the transfer of the VM state. We demonstrate that, if the host server is vulnerable to off-path TCP attacks, the loss of TCP reliability leads to VM live migration failure. We demonstrate that, by intentionally aborting the TCP connection, attackers can cause unrecoverable memory inconsistency for post-copy, leading to a significant increase in downtime and performance degradation of the running VM.
Distribution Statement: 2-Distribution Limited to U.S. Government agencies only; report contains proprietary info
Acknowledged Federal Support: **Y**

RPPR Final Report
as of 25-Jan-2023

CONFERENCE PAPERS:

Publication Type: Conference Paper or Presentation **Publication Status:** 1-Published
Conference Name: The 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)
Date Received: Conference Date: 24-Jun-2021 Date Published: 24-Jun-2021
Conference Location: Taipei, Taiwan
Paper Title: CloudSkulk: A Nested Virtual Machine Based Rootkit and Its Detection
Authors: Connelly, Joseph and Roberts, Taylor and Gao, Xing and Xiao, Jidong and Wang, Haining Wang and St
Acknowledged Federal Support: **Y**

Partners

,

I certify that the information in the report is complete and accurate:
Signature: Haining Wang
Signature Date: 1/12/23 11:00PM

W911NF1910049 : Information Retrieval in Clouds

Reporting Period: DEC 25, 2018 to SEP 24, 2022

Date Received:

Submitter: Haining Wang

Major Goals

Cloud computing nowadays is prevalent in our daily life, and it has been commonly used to provide IT [Information Technology] services over the Internet. Virtualization, as the foundation and main enabling technology of cloud computing, has played a crucial role in computing resource management inside a cloud, sharing finite hardware resources among a large number of software systems and programs. However, the security of virtualization has become a major concern for organizations and individuals who are hesitating to deploy their critical applications or data in cloud environments. This is mainly due to the fact that a hypervisor, which is a key component of virtualization and is controlled by cloud vendors, runs directly on the hardware or a host operating system [OS] to create and manage the guest OSes and have a higher privilege level than guest OSes. While significant research efforts have been paid to understand the cyber threats exposed by cloud computing, it is yet unclear how insecure/secure cloud environments are.

This project attempts to seek an answer for this question from a new and different perspective: information retrieval in clouds. In particular, we consider to retrieve information in two directions. One direction is from attackers' point of view, we investigate how much sensitive information attackers can obtain; the other direction is from defenders' perspective, we investigate how much sensitive information defenders can collect. The research will serve as a catalyst to promote the security level in cloud environments. The exploration of VME will help us understand how much security risk and vulnerability attackers can cause if they gain in-depth knowledge of underlying hypervisors via information retrieval, and then we will develop corresponding countermeasures to prevent such information leakage and reduce the damage. The further investigation of VMI will enable us to build a one-for-many VMI and memory enhance forensic tool, which will significantly enhance existing defense techniques such as intrusion detection.

Our final goals include: (1) collect hypervisor information so as to build hypervisor fingerprints, (2) build a cover channel to transfer information secretly, and (3) extend VMI techniques to enable more powerful inspections of a target VM, such as detecting nested VM rootkit and reconstructing memory based file systems.

Accomplishments Under Goals

VME: From attackers' perspective, we have investigated how attackers can utilize processor model specific registers (MSRs) to collect and transfer information. MSRs are special registers in computer processors used for collecting information or triggering certain CPU features. They are especially useful for performance monitoring or debugging. There is a large volume of MSRs: CPU vendors such as Intel and AMD have defined hundreds of MSRs for their processors. Actually, Intel has dedicated one entire volume of their software developer's manual (SDM), which consists of more than 400 pages, explaining the behaviors of each MSR. For this reason, over the years, we have

constantly seen developers submitting patches in the KVM or Xen community to fix MSR related issues. We have observed that many MSRs in a virtual machine exhibit different behaviors when the underlying hypervisors are different. Based on such a difference, we can, from inside the virtual machine, build a fingerprint of the underlying hypervisor.

We also investigated the security implications of virtual machine live migration and how attackers can tamper with regular VM migrations. What we found has been reported in the paper "Understanding the Security Implication of Aborting Live Migration," which has been published in the IEEE Transactions on Cloud Computing (TCC) in 2020. In order for attackers to perform the above attacks, they first need to identify a vulnerability in the system so that they can either take over the system, or launch attacks against the vulnerability. Unfortunately, due to complexity of operating systems, such vulnerabilities are commonly existed.

Moreover, we developed a nested virtual machine- based rootkit, which utilizes the virtual machine live migration technique to migrate a target virtual machine into a nested virtualized environment. Such an attack allows attackers to actively or passively collect victim's sensitive information. We evaluated the time it takes to launch such an attack, and the performance overhead it incurs in the virtualized environment. We also proposed and developed a detection mechanism that can effectively detect such attacks. This task has been completed and our findings and results have been reported in a research paper published in 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) in 2021.

VMI: From defenders' perspective, we plan to extend VMI technique to support more functionalities. More specifically, we aim to detect whether or not the target virtual machine is actually running as a hypervisor, thus allows another (nested) virtual machine running inside it. Detecting such a situation allows defenders to determine whether or not a virtual machine has been compromised, or a nested VM based rootkit is installed. Our approach is based on a technique called memory deduplication. More specifically, we develop and run a detection program at the host level, when nested virtualization is existing, certain memory pages are expected to be existing in both the inner-most virtual machine and the middle-layer hypervisor. And the duplication of these memory pages will trigger memory page merging. Based on this, we can determine whether or not the middle-layer hypervisor is existing.

When vulnerabilities are discovered, patches will be developed and should be applied as soon as possible. The team therefore also studied how to apply patches efficiently without incurring significant downtime. To this end, the team developed a novel live patching method which utilizes both the SMM and the SGX. Our findings and results were report in a research paper, which has been published in the 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) in 2020. This paper was nominated for the best paper award at the conference, one of the 3 nominees, out of 291 submissions. Our team also investigated how to collect the target system's sensitive information and therefore protect and introspect a target system from a lower-level by leveraging the Intel Management Engine (Intel ME). The resulted paper "Nighthawk: Transparent System Introspection from Ring -3" has been published in the 24th European Symposium on Research in Computer Security (ESORICS) in 2019.

We also developed a user-level crypto engine which stores sensitive information (such as crypto keys) in debug registers as well as in CPU cache. Compared to existing works, our engine runs in user level, as opposed to kernel level, which means our engine requires less privilege most of the time, and when privilege is truly needed, we leverage the virtualization technology comes with modern x86 CPUs, which allows us to switch between root mode and non-root mode. Overall, our engine protects sensitive keys against memory base attacks such as the cold boot attack.

Plans Next Period

Results Dissemination

- Xing Gao, Jidong Xiao, Haining Wang, Angelos Stavrou, "Understanding the Security Implication of Aborting Virtual Machine Live Migration", IEEE Transactions on Cloud Computing (TCC), 10(2): 1275-1286 (2022)

- Patrick Cronin, Xing Gao, Haining Wang, Chase Cotton, "Time-Print: Authenticating USB Flash Drives with Novel Timing Fingerprint", IEEE Symposium on Security and Privacy 2022: 1002-1017.

- Jidong Xiao, Lei Lu, Hai Huang, Haining Wang, "Virtual Machine Extrospection: A Reverse Information Retrieval in Clouds", IEEE Transactions on Cloud Computing 9(1): 401-413 (2021).

- Joseph Connelly, Taylor Roberts, Xing Gao, Jidong Xiao, Haining Wang, Angelos Stavrou, “CloudSkulk: A Nested Virtual Machine Based Rootkit and Its Detection", The 51st Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), June, 2021.

- Patrick Cronin, Xing Gao, Haining Wang, Chase Cotton, "An Exploration of ARM System-Level Cache and GPU Side Channels", ACSAC 2021: 784-795.

- Patrick Cronin, Xing Gao, Chengmo Yang, and Haining Wang, "Charger-Surfing: Exploiting a Power Line Side-Channel for Smartphone Information Leakage", In USENIX Security Symposium 2021, Vancouver, BC, Canada, August 2021.

- Xing Gao, Jidong Xiao, Haining Wang, and Angelos Stavrou, "Understanding the Security Implication of Aborting Live Migration" IEEE Transactions on Cloud Computing (TCC), 2020.

- Lei Zhou, Fengwei Zhang, Jinghui Liao, Zhenyu Ning, Jidong Xiao, Kevin Leach, Westley Weimer, and Guojun Wang, "KShot: Live Kernel Patching with SMM and SGX", The 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Valencia, Spain, June, 2020. Best Paper Award Nomination (3 out of 291 submissions).

- Lei Zhou, Jidong Xiao, Kevin Leach, Westley Weimer, Fengwei Zhang, and Guojun Wang, "Nighthawk: Transparent System Introspection from Ring-3", The 24th European Symposium on Research in Computer Security (ESORICS), Luxembourg, September, 2019.

Honors and Awards

- IEEE Fellow for the contribution of network and cloud security (Haining Wang)

- Best Paper Nominee at the 50th IEEE/IFIP DSN 2020 (Jidong Xiao)

- Ph.D, Awarded in July, 2021 (Patrick Cronin)

Training Opportunities

At the University of Delaware, One Ph.D. student participated in the proposed research tasks. At the Boise State University, one Ph.D. student and one undergraduate student were involved in the development and evaluation of the proposed VME and VMI approaches. These students have received detailed instructions and mentoring in cloud security and computer system research. In

particular, they learned virtualization technology, investigated hypervisor implementations, and explored from security perspectives, what problems are existing in current mainstream hypervisors, and what we can do to address these problems. The knowledge and skills that the students have learned can be applicable to broad areas of security and system research.

Technology Transfer

Nothing to Report

Participants

Name	Role	Person Months
Xiao, Jidong	Co PD/PI	1
Alam, Shariful	Graduate Student (research assistant)	12
Cronin, Patrick	Graduate Student (research assistant)	12
Wang, Haining	PD/PI	1
Roberts, Taylor	Undergraduate Student	4