Final Report: A Hybrid Computing Testbed for Mobile Threat Detection and Enhanced Research and Education in Information

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

Approved for public release; distribution is unlimited.

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA, 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.
RPPR Final Report
as of 31-Jan-2018

Proposal Number: 61520CSRIP

Agreement Number: W911NF-12-1-0440

INVESTIGATOR(S):

Name: Peng Ning
Email: pning@ncsu.edu
Phone Number: 9195130234
Principal: N

Name: Xuxian Jiang
Email: xjiang4@ncsu.edu
Phone Number: 9195137835
Principal: Y

Organization: North Carolina State University
Address: 2701 Sullivan Drive, Raleigh, NC 276957514
Country: USA
DUNS Number: 042092122
EIN: 566000756
Report Date: 20-Nov-2014
Date Received: 30-Jan-2018
Final Report for Period Beginning 21-Aug-2012 and Ending 20-Aug-2014
Title: A Hybrid Computing Testbed for Mobile Threat Detection and Enhanced Research and Education in Information
Begin Performance Period: 21-Aug-2012
End Performance Period: 20-Aug-2014
Report Term: 0-Other
Submitted By: Xuxian Jiang
Email: xjiang4@ncsu.edu
Phone: (919) 513-7835

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

STEM Degrees: 0
STEM Participants: 0

Major Goals: This project aims to build a hybrid computing testbed for detecting emerging mobile threats and improving research and education in information security at North Carolina State University (NCSU). The proposed computing testbed catalyzes the scalable, efficient deployment of the current Virtual Computing Lab (VCL) environment to provide a prototyping environment, which will be used for rapid development and evaluation of a variety of ongoing research projects funded by DoD and other government agencies. Also, the testbed supports research-related education components in system oriented information security courses at NCSU.

Furthermore, we leverage the hybrid testbed (with the additions of various mobile devices) to detect and experiment with emerging mobile threats (e.g., Android malware). One key use of this hybrid testbed is to detect emerging or new threats against current mobile gadgets (e.g., smart phones and tablets), which is not available or possible yet, based on current computing resources. The results and experience gained from operating and managing a real computing testbed will also provide practical insights into emerging threats on mobile Internet for students and researchers. The experience in managing and operating such a hybrid computing testbed will also be valuable to identify new security and performance problems and develop their practical solutions.

Accomplishments: See attached for details of:
Android Malware Genome Project.
Mobile Malware Profiling.
Stealthy Malware Defense.
Information Security Education and Student Training

Training Opportunities: Nothing to Report

Results Dissemination: Nothing to Report

Honors and Awards: Nothing to Report
Protocol Activity Status:

Technology Transfer: Nothing to Report
Final Technical Report
06/2012 - 06/2014

Xuxian Jiang (jiang@cs.ncsu.edu)
Associate Professor, Department of Computer Science
North Carolina State University, Raleigh, NC 27695-8206
http://www.cs.ncsu.edu/faculty/jiang

• Overall Goal
This project aims to build a hybrid computing testbed for detecting emerging mobile threats and improving research and education in information security at North Carolina State University (NCSU). The proposed computing testbed catalyzes the scalable, efficient deployment of the current Virtual Computing Lab (VCL) environment to provide a prototyping environment, which will be used for rapid development and evaluation of a variety of ongoing research projects funded by DoD and other government agencies. Also, the testbed supports research-related education components in system oriented information security courses at NCSU.
Furthermore, we leverage the hybrid testbed (with the additions of various mobile devices) to detect and experiment with emerging mobile threats (e.g., Android malware). One key use of this hybrid testbed is to detect emerging or new threats against current mobile gadgets (e.g., smart phones and tablets), which is not available or possible yet based on current computing resources. The results and experience gained from operating and managing a real computing testbed will also provide practical insights into emerging threats on mobile Internet for students and researchers. The experience in managing and operating such a hybrid computing testbed will also be valuable to identify new security and performance problems and develop their practical solutions.

• Accomplishments

Android Malware Genome Project  With the tremendous help of the proposed hybrid testbed, we have consistently maintained and disseminated a relatively large set of (Android) mobile malware samples within security research community. So far, our dataset has been shared with researchers from more than 400 universities and industry labs worldwide. Our corresponding IEEE Security & Privacy 2012 conference (a.k.a., Oakland’2012) paper has been the most cited Systematization of Knowledge (SoK) paper since its introduction in the Oakland conference history (with 520+ citations as of March 2015 according to Google Scholar Citations). For the upcoming year, as part of our community service, we will continue to share the collected malware samples via Android Malware Genome Project (http://www.malgenomeproject.org/) within research community.

Mobile Malware Profiling  In the continued efforts to systematize the knowledge base about existing Android malware and extract their fundamental properties, we have distilled current
Android mobile malware, including synthesized challenge apps, in a rigorous way – so that the extracted properties can be applied in the developed automated program analysis tool to enhance its capability of determining the presence or absence of malicious behavior of examined apps. Moreover, for current mobile apps that might leak user-sensitive information, we accordingly propose an owner-centric solution to protect valuable user data on smartphones. Our approach allows the data owners to specify security policies when providing their data to third-party apps. It tracks the flow of information to enforce the owners policies at strategic exit points. We evaluate our system against a set of real-world malicious apps and a series of synthetic attacks to show that it can successfully prevent the leakage of unstructured data while incurring reasonable performance overhead. This work has been published in TRUST’2014 conference.

Stealthy Malware Defense With the help of this testbed, we have continued our efforts in pursuing effective techniques to defend against stealthy malware, i.e., rootkits. For example, we have been developing new virtualization-based security service called AirBag for mobile devices. AirBag is a virtualization-based system that enables dynamic switching of (guest) Android images in one VM, with one image acting as a secure one for safe inspection and malware scanning. This way the attack surface of the running (mobile) OS system remains minimized, regardless of the regular Android image that is currently running. This work has been published in NDSS’2014 conference.

Information Security Education and Student Training This project also provides participating graduate students with hands-on experience with virtualization system software development and stealthy (mobile) malware defense. To develop and deploy virtualization-based malware defense solutions, the students first need to gain in-depth understanding of the hypervisor (VMM) and guest operating system internals. Then, they will modify and enhance the hypervisor software for malware profiling and defense functions. Such learning/training experience is not usually provided in traditional operating systems curriculum but is highly sought after by the cloud computing and cybersecurity industry. By participating in this project, the students gain strong competitiveness in the job market and unique advantage in their career development. For example, one female Ph.D. student, i.e., Deepa Srinivasan, joined the Microsoft HyperV core team in May 2013 and another Ph.D. student, Michael Grace, has been helping Samsung Mobile on the KNOX team to better ensure OS kernel integrity since January 2014.