REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
20-02-2016	Final Report	1-Sep-2013 - 31-May-2014

4. TITLE AND SUBTITLE
Final Report: Development and Detection of Mobile Malware

5a. CONTRACT NUMBER
W911NF-13-1-0382

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
611102

6. AUTHORS
Hongmei Chi

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
Florida A&M University
1700 Lee Hall Drive
400 FHAC
Tallahassee, FL 32307 -3200

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)
64622-CS-II.4

12. DISTRIBUTION AVAILIBILITY STATEMENT
Approved for Public Release; Distribution 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
This project provides us with a thorough understanding of the potential development of mobile malware, and it helps develop effective countermeasures to detect mobile malware. It greatly improves the security situation on mobile phone networks (and the Internet) and benefit the broad community of the smartphone users, including U.S. government agencies and military personals.
The proposed research compares the feasibility of three well known machine learning algorithms on the detection of malware on the Android platform. Once accuracy is at an acceptable level, these algorithms performance are

15. SUBJECT TERMS
Android, MalWare, detection, vulnerability detection, data mining

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Hongmei Chi
UU	UU	UU	UU		19b. TELEPHONE NUMBER 850-412-7355

Standard Form 298 (Rev 8/98)
Prescribed by ANSI Std. Z39.18

Report Title

Final Report: Development and Detection of Mobile Malware

ABSTRACT

This project provides us with a thorough understanding of the potential development of mobile malware, and it helps develop effective countermeasures to detect mobile malware. It greatly improves the security situation on mobile phone networks (and the Internet) and benefit the broad community of the smartphone users, including U.S. government agencies and military personals.
The proposed research compares the feasibility of three well known machine learning algorithms on the detection of malware on the Android platform. Once accuracy is at an acceptable level, these algorithms performance are further enhanced to decrease analysis time, which can lead to faster detection rates. The framework makes use of powerful GPU's (Graphics Processing Unit) in order to reduce the time spent on computation for malware detection. Utilizing MATLAB's parallel computing kit, we can execute analysis at a much higher speed due to the increased cores in the GPU. A reduced computation time allows for quick updates to the user about zero day malware, resulting in a decreased impact. With the increase in mobile devices unending, quick detection becomes necessary to combat mobile malware, and with Android alone reaching its 50 billionth app downloads, is no small task.

Enter List of papers submitted or published that acknowledge ARO support from the start of the project to the date of this printing. List the papers, including journal references, in the following categories:

(a) Papers published in peer-reviewed journals (N/A for none)

Received Paper

TOTAL:

Number of Papers published in peer-reviewed journals:

(b) Papers published in non-peer-reviewed journals (N/A for none)

Received Paper

TOTAL:

Number of Papers published in non peer-reviewed journals:

(c) Presentations

[1]Hongmei Chi, Constance Dellor and Christy Chatmon, Analyzing Community Evolution in Complex Networks via Bio-inspired Computing, ADMI 2015, March 19-22, Atlanta,GA
[2] Hongmei Chi, Dominique Hubbard,Simulation Study to Use Wearable Devices Determining the Vitality of Patients, AlaSim 2015, May 6-7, Huntsville, AL
[3] Shuyuan Ho and Hongmei Chi A Sociotechnical Approach to Lawful Interception and Computational Assessment of Information Behavior to Protect Against Insider Threat. FC2 Annual Conference, Oct 13-14, 2015, Tampa, FL,

Number of Presentations: 3.00

Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Received	Paper	
02/09/2016	5.00	Hongmei Chi, Shuyuan Mary Ho, Dominique Hubbard. An online game simulation environment for detecting potential deceptive insiders, Winter Simulation Conference 2016. 11-DEC-15, . : ,
TOTAL:	**1**	

Number of Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Peer-Reviewed Conference Proceeding publications (other than abstracts):

Received	Paper	
03/15/2015	1.00	LaWanda Warren, Hongmei Chi. Securing EHRs via CPMA attribute-based encryption on cloud systems, the 2014 ACM Southeast Regional Conference. 28-MAR-14, Kennesaw, Georgia. : ,
03/15/2015	2.00	Daniel Andrew, Hongmei Chi. An empirical study of botnets on university networks using low-interaction honeypots, the 51st ACM Southeast Conference. 04-APR-13, Savannah, Georgia. : ,
TOTAL:	**2**	

Number of Peer-Reviewed Conference Proceeding publications (other than abstracts):

(d) Manuscripts

Received	Paper	
03/15/2015	3.00	Hongmei Chi and Xavier Simms. A Fast Approach towards Android Malware Detection , INTERNATION Journal of Network Security (01 2015)
TOTAL:	**1**	

Number of Manuscripts:

Books

Received Book

TOTAL:

Received Book Chapter

TOTAL:

Patents Submitted

Patents Awarded

Awards

Graduate Students

NAME	PERCENT_SUPPORTED	Discipline
Xavier Simms	0.50	
Dominique Hubbard	0.25	
FTE Equivalent:	**0.75**	
Total Number:	**2**	

Names of Post Doctorates

NAME	PERCENT_SUPPORTED
FTE Equivalent:	
Total Number:	

Names of Faculty Supported

NAME	PERCENT_SUPPORTED	National Academy Member
Hongmei Chi	0.20	No
Edward Jones	0.10	
Christy Chatmon	0.10	
FTE Equivalent:	**0.40**	
Total Number:	**3**	

Names of Under Graduate students supported

NAME	PERCENT_SUPPORTED	Discipline
David Blake	0.25	B.S in computer Science
Dominique Hubbard	0.25	B.S in computer Science
FTE Equivalent:	**0.50**	
Total Number:	**2**	

Student Metrics

This section only applies to graduating undergraduates supported by this agreement in this reporting period

The number of undergraduates funded by this agreement who graduated during this period:	1.00
The number of undergraduates funded by this agreement who graduated during this period with a degree in science, mathematics, engineering, or technology fields:.....	1.00
The number of undergraduates funded by your agreement who graduated during this period and will continue to pursue a graduate or Ph.D. degree in science, mathematics, engineering, or technology fields:.....	1.00
Number of graduating undergraduates who achieved a 3.5 GPA to 4.0 (4.0 max scale):.....	1.00
Number of graduating undergraduates funded by a DoD funded Center of Excellence grant for Education, Research and Engineering:.....	0.00
The number of undergraduates funded by your agreement who graduated during this period and intend to work for the Department of Defense	0.00
The number of undergraduates funded by your agreement who graduated during this period and will receive scholarships or fellowships for further studies in science, mathematics, engineering or technology fields:	2.00

Names of Personnel receiving masters degrees

NAME	
Xavier Simms	
Total Number:	**1**

Names of personnel receiving PHDs

NAME
Total Number:

Names of other research staff

NAME	PERCENT_SUPPORTED
FTE Equivalent:	
Total Number:	

Sub Contractors (DD882)

Inventions (DD882)

Scientific Progress

Objective: Mobile malwares are an emerging security threat on mobile phone networks, which will have great impacts on the overall security of smartphone networks. The main objectives of this project are 1) to investigate the potential development of mobile malwares, and 2) to develop effective countermeasures to detect mobile malwares.

Approach: This project combats the unauthorized access and transmission of data by analyzing mobile applications to determine if it posed a threat to user information. In order to accomplish this task, a mobile framework was implemented to analyze Android applications for their ability to access and transmit user data. This system was able to detect applications that posed a threat to user data achieving an 88% detection rate. The framework was also able to reduce the total number of applications that needed deep analysis by identify those that required thorough investigation and decreasing the total data set by 56% and thus reducing the total time frame for malware analysis.
Many mobile malware detection methods utilize the APK (Android Application Package) to retrieve source code data for analysis; permissions, functions and other useful information. In this project the applications are allowed to run on devices so that real usage statistics can be retrieved, which include bandwidth, memory, permission list, package names and other data. The data is stored on a database, and queried to build datasets for analysis. The analysis of the data creates a malware probability value that determines the potential of an application to access and transmit user data. The focus in this research is to detect applications that steal user data, which is a subset of different kinds of malwares. The analysis time is then compared on the basis of GPU and CPU to determine the benefit of GPU analysis.

Accomplishments:
(1) Design/Implement database to store user, device and application variables and an application to retrieve data from devices;
(2) Design analysis algorithm to rate each applications potential to access and transmit user data.
(3) Analyze data on the accuracy of detection utilizing application permissions and usage variables using MATLAB;
(4) Evaluate data on the time necessary for analysis of application data sets; and
(5) Assess data on comparison of performance of the CPU and GPU analysis for different malware detection algorithms.

Conclusion and Future Work
This project provides us with a thorough understanding of the potential development of mobile malwares, and it will help develop effective countermeasures to detect mobile malwares. It will greatly improve the security situation on mobile phone networks (and the Internet) and benefit the broad community of the mobile phone users, including U.S. government agencies and military personals. The results obtained from this project can be integrated into U.S. military programs such as Nett Warrior. The techniques and systems developed in this project can help monitor, evaluate, and improve the security situation of the DoD mobile phone networks for potential infiltration, infection, and attacks. In addition, we are planning to extend our detection methods to detect zero-day mobile malwares

Technology Transfer

Project Title: Development and Detection of Mobile Malware
Proposal Number : W911NF1310382---64622CSII
Name Hongmei Chi, Florida A&M University

Objective: Mobile malwares are an emerging security threat on mobile phone networks, which will have great impacts on the overall security of smartphone networks. The main objectives of this project are 1) to investigate the potential development of mobile malwares, and 2) to develop effective countermeasures to detect mobile malwares.

Approach: This project combats the unauthorized access and transmission of data by analyzing mobile applications to determine if it posed a threat to user information. In order to accomplish this task, a mobile framework was implemented to analyze Android applications for their ability to access and transmit user data. This system was able to detect applications that posed a threat to user data achieving an 88% detection rate. The framework was also able to reduce the total number of applications that needed deep analysis by identify those that required thorough investigation and decreasing the total data set by 56% and thus reducing the total timeframe for malware analysis.

Significance: Many mobile malware detection methods utilize the APK (Android Application Package) to retrieve source code data for analysis; permissions, functions and other useful information. In this project the applications are allowed to run on devices so that real usage statistics can be retrieved, which include bandwidth, memory, permission list, package names and other data. The data is stored on a database, and queried to build datasets for analysis. The analysis of the data creates a malware probability value that determines the potential of an application to access and transmit user data. The focus in this research is to detect applications that steal user data, which is a subset of different kinds of malware. The analysis time is then compared on the basis of GPU and CPU to determine the benefit of GPU analysis.

Accomplishments

(1) Design/Implement database to store user, device and application variables and an application to retrieve data from devices;
(2) Design analysis algorithm to rate each applications potential to access and transmit user data.
(3) Analyze data on the accuracy of detection utilizing application permissions and usage variables using MATLAB;
(4) Evaluate data on the time necessary for analysis of application data sets; and
(5) Assess data on comparison of performance of the CPU and GPU analysis for various malware detection algorithms.

Conclusions: The project was successful in detecting the ability of an application to access and transmit a user's data. The project maintained a detection rate of 80% accuracy and at a time of 14 seconds, on the dataset of 41 applications. The implementation was also successful in detecting the number of applications that would require more analysis; by pointing out that 21 applications did not pose a significant threat to user data, and highlighting that 20 of the applications in the dataset should receive further testing and

analysis. The analysis was completed in 14.907 seconds, with 14.106 seconds spent querying the database and waiting for results. It is worth highlighting that the actual computation time was 0.42 seconds, which was spent calculating the log(x) value of the bandwidth and assigning true or false values to the malware probability field. To further improve the execution time a GPU can be used, however there will be minimal effect, because the majority of the time is consumed retrieving data to build the datasets. Further insight can be gained by also making use of other data collected, such as application memory consumption; although this may not have a large correlation to malware behavior.

Future Plans: (1) This project provides us with a thorough understanding of the potential development of mobile malware, and it will help develop effective countermeasures to detect mobile malwares. It will greatly improve the security situation on mobile phone networks (and the Internet) and benefit the broad community of the mobile phone users, including U.S. government agencies and military personals. The results obtained from this project can be integrated into U.S. military programs such as Nett Warrior. The techniques and systems developed in this project can help monitor, evaluate, and improve the security situation of the DoD mobile phone networks for potential infiltration, infection, and attacks. (2) We are planning to extend our detection methods to detect zero-day mobile malwares

References:

[1] LaWanda Warren, Hongmei Chi: Securing EHRs via CPMA attribute-based encryption on cloud systems. ACM Southeast Regional Conference 2014: 20

[2] Arp, Daniel, et al. "Drebin: Effective and explainable detection of android malware in your pocket." Proc. of NDSS. 2014.