REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
13-09-2016	Final Report	1-Aug-2014 - 31-Jul-2016

4. TITLE AND SUBTITLE
Final Report: A Test-bed of Secure Mobile Cloud Computing for Military Applications

5a. CONTRACT NUMBER
W911NF-14-1-0518

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
611103

6. AUTHORS
Xiaojiang Du

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
Temple University
3340 N. Broad Street
Student Faculty Center Suite 427
Philadelphia, PA 19140 -5102

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)
65248-CS-RIP.10

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
Many military applications have the following characteristics: they start from a mobile device (e.g., a night vision goggle) carried by military personnel; they are computation-intensive, requiring the compute-power of a server, and they use Big Data, requiring searching databases. This kind of applications is a typical example of mobile cloud computing (MCC). MCC has lots of applications in the military battlefields. In addition, MCC is expected to be widely used by military and government personnel in non-battlefield environment, such as DoD research labs and offices, where these people access military and government servers (cloud) using their mobile devices. In this

15. SUBJECT TERMS
Test-bed, Mobile Cloud Computing, Security, Military Applications

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			XIAOJIANG DU
UU	UU	UU	UU		19b. TELEPHONE NUMBER 215-204-8888

Report Title

Final Report: A Test-bed of Secure Mobile Cloud Computing for Military Applications

ABSTRACT

Many military applications have the following characteristics: they start from a mobile device (e.g., a night vision goggle) carried by military personnel; they are computation-intensive, requiring the compute-power of a server, and they use Big Data, requiring searching databases. This kind of applications is a typical example of mobile cloud computing (MCC). MCC has lots of applications in the military battlefields. In addition, MCC is expected to be widely used by military and government personnel in non-battlefield environment, such as DoD research labs and offices, where these people access military and government servers (cloud) using their mobile devices. In this project, we requests support for purchasing equipment and devices to establish a Secure Mobile Cloud Computing test-bed at Temple University. The proposed MCC test-bed will be used to support several integrated research and education projects that are to the core interests of the military.

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

Number of Presentations: 0.00

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

Received Paper

TOTAL:

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

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

Received Paper

TOTAL:

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

(d) Manuscripts

Received Paper

TOTAL:

Number of Manuscripts:

Books

Received Book

TOTAL:

Received	Book Chapter

TOTAL:

Patents Submitted

Patents Awarded

Awards

An undergraduate student Robert Woods won the Future of Computing Gold Award, CIS Dept, Temple, April 2015.

Graduate Students

NAME	PERCENT_SUPPORTED	Discipline
Xueli Huang	0.00	
Longfei Wu	0.00	
Shuang Liang	0.00	
Ge Bai	0.00	
Jing Tan	0.00	
FTE Equivalent:	**0.00**	
Total Number:	**5**	

Names of Post Doctorates

NAME	PERCENT_SUPPORTED
FTE Equivalent:	
Total Number:	

Names of Faculty Supported

NAME	PERCENT_SUPPORTED	National Academy Member
Xiaojiang Du	0.00	
Jie Wu	0.00	
FTE Equivalent:	**0.00**	
Total Number:	**2**	

Names of Under Graduate students supported

NAME	PERCENT_SUPPORTED	Discipline
Robert Woods	0.00	
Philip Riesch	0.00	
Benjamin Brandt	0.00	
Gus Kenion	0.00	
Montser Jalil	0.00	
Alex Burns	0.00	
FTE Equivalent:	**0.00**	
Total Number:	**6**	

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: 6.00

The number of undergraduates funded by this agreement who graduated during this period with a degree in science, mathematics, engineering, or technology fields:..... 6.00

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):..... 2.00

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 1.00

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: 0.00

Names of Personnel receiving masters degrees

NAME	
Jing Tan	
Ge Bai	
Total Number:	**2**

Names of personnel receiving PHDs

NAME	
Xueli Huang	
Total Number:	**1**

Names of other research staff

NAME	PERCENT_SUPPORTED
FTE Equivalent:	
Total Number:	

Sub Contractors (DD882)

Inventions (DD882)

Scientific Progress

(1) Foreword
This report summarizes the scientific progress and accomplishments of the following DURIP project:
CONTRACT NUMBER: WF911NF-14-1-0518
TITLE: A Test-bed of Secure Mobile Cloud Computing for Military Applications

(2) Statement of the problem studied
Many military applications have the following characteristics: they start from a mobile device (e.g., a night vision goggle) carried by military personnel; they are computation-intensive, requiring the compute-power of a server, and they use Big Data, requiring searching databases. This kind of applications is a typical example of mobile cloud computing (MCC). MCC has lots of applications in the military battlefields. In addition, MCC is expected to be widely used by military and government personnel in non-battlefield environment, such as DoD research labs and offices, where these people access military and government servers (cloud) using their mobile devices. In this project, we purchased equipment and devices to establish a Secure Mobile Cloud Computing test-bed at Temple University. The proposed MCC test-bed has been used to support several integrated research and education projects that are to the core interests of the military.

The objectives of the supported research projects are to design efficient and effective security schemes for defending camera-based attacks and phishing attacks on MCC, as well as malware detection for MCC, which can significantly enhance information security and hence war-fighting capability. The objective of the supported education programs is to educate and train highly skilled undergraduate and graduate students in these areas, which are critical disciplines to the DoD. The MCC test-bed consists of 32 mobile devices (such as mobile phones and USRP radios), 4 computing servers, 2 storage servers, 1 Gigabit switch, and 2 gateway nodes.

The MCC test-bed has been used to support high-quality research and education in the area of information security and mobile computing, which are key enabling technologies for the military. The test-bed developed new research capabilities at Temple University, and facilitate cutting-edge research relevant to DoD missions, and broaden the Temple research base in support of national defense. The instrumentation significantly enhances the PIs' current research capabilities for performing research and research-related education in areas of great interest to the DoD.

The supported research activities include the following three active projects on MCC: (a) the security and privacy of data stored on cloud; (b) defending phishing attacks on mobile devices and MCC, which could steal private/secret information such as passwords, which allow an attacker to access all the data protected by the passwords; and (c) detecting mobile malwares, which can cause information leaking and many other damages.

(3) Summary of the most important results
(a) The important results of data privacy on cloud are presented in the following.
The security and privacy of data stored on cloud is an important issue. In this work, we propose a novel scheme that can achieve data privacy by hybrid cloud, which consists of public and private cloud, and reduce storage and computation in private cloud, as well as communication overhead between private and public cloud. In particular, we propose a novel algorithm to process private image data. In our algorithm, an image containing privacy information is divided into blocks, and the blocks are shuffled with random start position and random stride. Our scheme operates at the block level instead of the pixel level, which greatly speeds up the computation. We converted the image privacy problem into the jigsaw puzzle problem. To make the jigsaw puzzle problem NP-complete, we modified the image data based on blocks by subtracting a random value for each pixel within the same block and same color dimension. These operations make the pairwise affinity unreliable and make the shuffled image unrecognizable as well as the statistic information. We formulated an optimization problem to minimize the overhead. By carefully selecting the number of blocks and the cluster size, the communication overhead of our scheme on private cloud can be greatly reduced. We implemented our scheme in real network environments (including the Amazon EC2) and tested the security, efficiency, and communication overhead. Both our analysis and experimental results showed that our scheme is secure, efficient, and introduces little overhead. Our experimental results show that (i) our algorithm achieves data privacy but only takes about 1/1000, time of the Advanced Encryption Standard algorithm and (ii) the delay of our hybrid cloud approach (including the private and public cloud communications) is only 3%–5% more compared with the traditional public cloud-only approach. The research results have been published in a peer-reviewed journal paper [1] – Wiley Security and Communication Networks in Dec. 2015.

(b) The important results of phishing attacks on mobile devices and MCC are presented in the following. Recent years have witnessed the increasing threat of phishing attacks on mobile computing platforms. In fact, mobile phishing is particularly dangerous due to the hardware limitations of mobile devices and mobile user habits. In this work, we did a comprehensive study on the security vulnerabilities caused by mobile phishing attacks, including the web page phishing attacks, the application phishing attacks, and the account registry phishing attacks. Existing schemes designed for web phishing attacks on PCs cannot effectively address the various phishing attacks on mobile devices. Hence, we propose MobiFish, a novel automated lightweight anti-phishing scheme for mobile platforms. MobiFish verifies the validity of web pages, applications, and persistent accounts by comparing the actual identity to the claimed identity. MobiFish has been implemented on a Nexus 4 smartphone running the Android 4.2 operating system. We experimentally evaluate the performance of MobiFish with 100 phishing URLs and corresponding legitimate URLs, as well as phishing apps. The results show that MobiFish is very effective in detecting phishing

attacks on mobile phones. The research results have been published in a top journal paper [2] – IEEE Transactions on Vehicular Technology in June 2016.

(c) The important results of detecting mobile malwares are presented in the following.
Mobile devices (e.g., smartphones) continue the popularization worldwide and have become an important part of people's daily lives. Android is the most popular and the best-selling smartphone operating system (OS), holding over 80% of global smartphone market share [3]. However, security and privacy issues are a widely recognized problem of Android, mainly because it is open source and attackers can find security vulnerabilities from the source code. The security of user interface (UI) is particularly important, since mobile users interact directly with the UIs of the system as well as 3rd-party apps. Specifically, users receive most information visually from the UI, and give their inputs in terms of touch, click, and key entry to the UI as well. The manipulation of UIs can pose huge threats to the interaction between user and the mobile device.

In this work, we focus on mobile clickjacking attacks. Clickjacking attack is also known as "UI redress attack". It happens when a malicious app inserts an opaque layer (or in very low transparency) on top of the screen, to trick a user to click on a specific position. The click event seemingly going to the top front window actually goes to the target window underneath. If carefully designed, the user may trigger a concealed button or link in the underlying window. Clickjacking attack could cause severe damage to the user's security and privacy.

In this work, we give a detailed analysis of the potential risks posed by clickjacking. Finally, we propose an automatic, lightweight and effective defense scheme to defeat clickjacking attempts, which is able to overcome the limitations of all existing solutions. All different types of clickjacking attacks and the defense mechanism are implemented on a Nexus 4 smartphone running Android 5.0 system. The effectiveness and overheads of the proposed scheme are evaluated with extensive experiments. The results show that our scheme can effectively prevent clickjacking attacks with only a minor impact to the system.

The research results have been published in a top security conference – the IEEE Conference on Communications and Network Security (IEEE CNS) 2016 [4].

(4) Bibliography
[1] X. Huang, and X. Du, "Achieving Data Privacy on Hybrid Cloud," Security and Communication Networks, Wiley, Volume 8, Issue 18, pages 3771–3781, Dec. 2015.
[2] L. Wu, X. Du, and J. Wu, "Effective Defense Schemes for Phishing Attacks on Mobile Computing Platforms," IEEE Transactions on Vehicular Technology, Issue 8, Vol. 65, pp. 6678 - 6691, June 2016. DOI: 10.1109/TVT.2015.2472993
[3] Gartner, "Worldwide smartphone sales to end users by operating system in 4q15," http://www.gartner.com/newsroom/id/3215217, Feb 2016.
[4] L. Wu, B. Brandt, X. Du, and B. Ji, "Analysis of Clickjacking Attacks and An Effective Defense Scheme for Android Devices", to appear in Proc. of IEEE Conference on Communications and Network Security (IEEE CNS) 2016, acceptance rate 29% =38/131, Philadelphia, PA, Oct. 2016.

Technology Transfer

N/A

Scientific Progress and Accomplishments

Prof. Xiaojiang Du
Dept. of Computer and Information Sciences
Temple University
1925 N. 12th Street
304 SERC, 035-10
Philadelphia PA 19122
Phone: 215-204-8888
Email: dux@temple.edu

(1) Foreword

This report summarizes the scientific progress and accomplishments of the following DURIP project:

CONTRACT NUMBER: WF911NF-14-1-0518

TITLE: A Test-bed of Secure Mobile Cloud Computing for Military Applications

(2) Statement of the problem studied

Many military applications have the following characteristics: they start from a mobile device (e.g., a night vision goggle) carried by military personnel; they are computation-intensive, requiring the compute-power of a server, and they use Big Data, requiring searching databases. This kind of applications is a typical example of mobile cloud computing (MCC). MCC has lots of applications in the military battlefields. In addition, MCC is expected to be widely used by military and government personnel in non-battlefield environment, such as DoD research labs and offices, where these people access military and government servers (cloud) using their mobile devices. In this project, we purchased equipment and devices to establish a Secure Mobile Cloud Computing test-bed at Temple University. The proposed MCC test-bed has been used to support several integrated research and education projects that are to the core interests of the military.

The objectives of the supported research projects are to design efficient and effective security schemes for defending camera-based attacks and phishing attacks on MCC, as well as malware detection for MCC, which can significantly enhance information security and hence war-fighting capability. The objective of the supported education programs is to educate and train highly skilled undergraduate and graduate students in these areas, which are critical disciplines to the DoD. The MCC test-bed consists of 32 mobile devices (such as mobile phones and USRP radios), 4 computing servers, 2 storage servers, 1 Gigabit switch, and 2 gateway nodes.

The MCC test-bed has been used to support high-quality research and education in the area of information security and mobile computing, which are key enabling technologies for the military. The test-bed developed new research capabilities at Temple University, and facilitate cutting-edge research relevant to DoD missions, and broaden the Temple research base in support of national defense. The instrumentation

significantly enhances the PIs' current research capabilities for performing research and research-related education in areas of great interest to the DoD.

The supported research activities include the following three active projects on MCC: (a) the security and privacy of data stored on cloud; (b) defending phishing attacks on mobile devices and MCC, which could steal private/secret information such as passwords, which allow an attacker to access all the data protected by the passwords; and (c) detecting mobile malwares, which can cause information leaking and many other damages.

(3) Summary of the most important results

(a) The important results of data privacy on cloud are presented in the following.
The security and privacy of data stored on cloud is an important issue. In this work, we propose a novel scheme that can achieve data privacy by hybrid cloud, which consists of public and private cloud, and reduce storage and computation in private cloud, as well as communication overhead between private and public cloud. In particular, we propose a novel algorithm to process private image data. In our algorithm, an image containing privacy information is divided into blocks, and the blocks are shuffled with random start position and random stride. Our scheme operates at the block level instead of the pixel level, which greatly speeds up the computation. We converted the image privacy problem into the jigsaw puzzle problem. To make the jigsaw puzzle problem NP-complete, we modified the image data based on blocks by subtracting a random value for each pixel within the same block and same color dimension. These operations make the pairwise affinity unreliable and make the shuffled image unrecognizable as well as the statistic information. We formulated an optimization problem to minimize the overhead. By carefully selecting the number of blocks and the cluster size, the communication overhead of our scheme on private cloud can be greatly reduced. We implemented our scheme in real network environments (including the Amazon EC2) and tested the security, efficiency, and communication overhead. Both our analysis and experimental results showed that our scheme is secure, efficient, and introduces little overhead. Our experimental results show that (i) our algorithm achieves data privacy but only takes about 1/1000, time of the Advanced Encryption Standard algorithm and (ii) the delay of our hybrid cloud approach (including the private and public cloud communications) is only 3%–5% more compared with the traditional public cloud-only approach. The research results have been published in a peer-reviewed journal paper [1] – Wiley Security and Communication Networks in Dec. 2015.

(b) The important results of phishing attacks on mobile devices and MCC are presented in the following.
Recent years have witnessed the increasing threat of phishing attacks on mobile computing platforms. In fact, mobile phishing is particularly dangerous due to the hardware limitations of mobile devices and mobile user habits. In this work, we did a comprehensive study on the security vulnerabilities caused by mobile phishing attacks, including the web page phishing attacks, the application phishing attacks, and the account registry phishing attacks. Existing schemes designed for web phishing attacks on PCs cannot effectively address the various phishing attacks on mobile devices. Hence, we propose MobiFish, a novel automated lightweight anti-phishing scheme for mobile platforms. MobiFish verifies the validity of web pages, applications, and persistent accounts by comparing the actual identity to the claimed identity. MobiFish has been implemented on a Nexus 4 smartphone running the Android 4.2 operating system. We experimentally evaluate the performance of MobiFish with 100 phishing URLs and corresponding legitimate URLs, as well as phishing apps. The results show that MobiFish is very effective in detecting phishing attacks on mobile phones. The research results have been published in a top journal paper [2] – IEEE Transactions on Vehicular Technology in June 2016.

(c) The important results of detecting mobile malwares are presented in the following.
Mobile devices (e.g., smartphones) continue the popularization worldwide and have become an important part of people's daily lives. Android is the most popular and the best-selling smartphone operating system (OS), holding over 80% of global smartphone market share [3]. However, security and privacy issues are a widely recognized problem of Android, mainly because it is open source and attackers can find security vulnerabilities from the source code. The security of user interface (UI) is particularly important, since mobile users interact directly with the UIs of the system as well as 3rd-party apps. Specifically, users receive most information visually from the UI, and give their inputs in terms of touch, click, and key entry to the UI as well. The manipulation of UIs can pose huge threats to the interaction between user and the mobile device.

In this work, we focus on mobile clickjacking attacks. Clickjacking attack is also known as "UI redress attack". It happens when a malicious app inserts an opaque layer (or in very low transparency) on top of the screen, to trick a user to click on a specific position. The click event seemingly going to the top front window actually goes to the target window underneath. If carefully designed, the user may trigger a concealed button or link in the underlying window. Clickjacking attack could cause severe damage to the user's security and privacy.

In this work, we give a detailed analysis of the potential risks posed by clickjacking. Finally, we propose an automatic, lightweight and effective defense scheme to defeat clickjacking attempts, which is able to overcome the limitations of all existing solutions. All different types of clickjacking attacks and the defense mechanism are implemented on a Nexus 4 smartphone running Android 5.0 system. The effectiveness and overheads of the proposed scheme are evaluated with extensive experiments. The results show that our scheme can effectively prevent clickjacking attacks with only a minor impact to the system.

The research results have been published in a top security conference – the IEEE Conference on Communications and Network Security (IEEE CNS) 2016 [4].

(4) Bibliography

[1] X. Huang, and X. Du, "Achieving Data Privacy on Hybrid Cloud," Security and Communication Networks, Wiley, Volume 8, Issue 18, pages 3771–3781, Dec. 2015.

[2] L. Wu, X. Du, and J. Wu, "Effective Defense Schemes for Phishing Attacks on Mobile Computing Platforms," IEEE Transactions on Vehicular Technology, Issue 8, Vol. 65, pp. 6678 - 6691, June 2016. DOI: 10.1109/TVT.2015.2472993

[3] Gartner, "Worldwide smartphone sales to end users by operating system in 4q15," http://www.gartner.com/newsroom/id/3215217, Feb 2016.

[4] L. Wu, B. Brandt, X. Du, and B. Ji, "Analysis of Clickjacking Attacks and An Effective Defense Scheme for Android Devices", to appear in Proc. of IEEE Conference on Communications and Network Security (IEEE CNS) 2016, acceptance rate 29% =38/131, Philadelphia, PA, Oct. 2016