DIMITRIOS DAMOPOULOS

Hoboken, New Jersey
07030, USA
E-mail: ddamop@aegean.gr
E-mail: ddamopou@stevens.gr
Website: www.icsd.aegean.gr/ddamop

PERSONAL INFORMATION

Date of birth:	8 January 1985
Place of birth:	Frankfurt, Germany

EDUCATION

September '13- today

Postdoctoral researcher in the Laboratory for Secure Systems (LSS)

Supervisors: Dr. Georgios Portokalidis,

At Stevens Institute of Technology,
Schaefer School of Engineering & Science, Dept. of Computer Science,
New Jersey, USA

March '10- June '13

Ph.D. Information and Communication Systems Engineering

Title: Anomaly-Based Intrusion Detection and Prevention Systems (IDPS) for Mobile Devices: Design and Development

Supervisors: Dr. Georgios Kambourakis, Prof. Stefanos Gritzalis, Dr. Elisavet Konstantinou

At the University of the Aegean,
Department of Information & Communication Systems Engineering
Karlovassi Greece

October '08- February '10

MSc Technologies and Management of Information and Communication Systems
Studies Program: Information & Communication Systems Security

At the University of the Aegean,
Department of Information & Communication Systems Engineering
Karlovassi Greece (1,5 years degree)
with general degree: 8,2 (max 10)

September '09 - February '10

Erasmus for carrying out the Master Thesis

Title: Anomaly-Based Intrusion Detection Systems for Mobile Devices

Supervisors: Dr. Maria Papadaki, Dr. Nathan Clarke, Prof. Stefanos Gritzalis

At the University of Plymouth United Kingdom
Faculty of Science and Technology
School of Computing & Mathematics

October '03 - May '08 **BSc Industrial Informatics**

Technological Educational Institute of Kavala, Greece (4,5 years) with general degree: 6,63 (max 10)

September '07- April '08 **Erasmus for carrying out the Diploma Thesis:**

Title: Analysis and Guidelines Implementation for the Network Security of the University of Applied Science Oldenburg/Ostfriesland/Wilhelmshaven

Supervisors: Prof. Matthias O. Berger, Wolfgang Eggerichs, Prof. Georgios Kuranistasis

At the University of Applied Science Oldenburg/Ostfriesland/Wilhelmshaven (FH-OOW) department: Wilhelmshaven with degree: 9,5 (max 10)

June '03 **3^{o} Lyceum Kastoria**

Kastoria , Greece with general degree: 15,8 (max 20)

CERTIFICATION

July '12 **OWASP AppSec Research 2012 – University Challenge**

Participated with the Aegean University team

July '12 **ESA (European Space Agency) App Challenge**

20 developers selected across the Europe, to participate in the ESA contest

July '09 **Intensive Program on Information and Communication Security (IPICS)**

IPICS Summer School in Vienna 2009

March '07- April '08 **Cisco Certified Network Associate CCNA**

CCNA Semester 1 with grade: 83.3 *(max 100)*
CCNA Semester 2 with grade: 82.0 *(max 100)*
CCNA Semester 3 with grade: 89.3 *(max 100)*
CCNA Semester 4 with grade: 94.7 *(max 100)*

WORK EXPERIENCE

March '13 - June '13 **Teaching Experience – Laboratory Assistant**

Laboratory Lectures:

- ***Distributed Systems (Java Socket & RMI Programming)***

At the University of the Aegean,
Department of Information & Communication Systems Engineering
Karlovassi Greece

October '12 - February '13

Teaching Experience – Laboratory Assistant

Laboratory Lectures:

- ***Programming Methodologies and Languages II (Java Programming)***

At the University of the Aegean,
Department of Information & Communication Systems Engineering
Karlovassi Greece

March '12 - June '12

Teaching Experience – Laboratory Assistant

Laboratory Lectures:

- ***Programming Methodologies and Languages I (C++ Programming)***
- ***Distributed Systems (Java Socket & RMI Programming)***

At the University of the Aegean,
Department of Information & Communication Systems Engineering
Karlovassi Greece

October '11 - February '12

Teaching Experience – Laboratory Assistant

Laboratory Lectures:

- ***Introduction to Programming (C Programming)***
- ***Programming Methodologies and Languages II (Java Programming)***

At the University of the Aegean,
Department of Information & Communication Systems Engineering
Karlovassi Greece

March '11 - June '11

Teaching Experience – Laboratory Assistant

Laboratory Lectures:

- ***Programming Methodologies and Languages I (C++ Programming)***
- ***Distributed Systems (Java Socket & RMI Programming)***

At the University of the Aegean,
Department of Information & Communication Systems Engineering
Karlovassi Greece

October '10 - February '11

Teaching Experience – Laboratory Assistant

Laboratory Lectures:

- ***Introduction to Programming (C Programming)***
- ***Programming Methodologies and Languages II (Java Programming)***

At the University of the Aegean,
Department of Information & Communication Systems Engineering
Karlovassi Greece

March '07 - August '07

Erasmus Practice at the Network Administration Center of Wilhelmshaven

With daily tasks:

- ***Security Network Program FH-OOW***
- ***Software Development for Host-DB Program***
- ***Daily network operations at the Network Administration Center of Wilhelmshaven***

At the Network Administration Center of Oldenburg/Ostfriesland/Wilhelmshaven (FH-OOW) Department: Wilhelmshaven German

---

SCHOLARSHIPS-REWARDS

September '10 **2nd Award in 1st Greek HTC Android Applications Competition**
Project: E.A.R.T.H (Electrical Appliance Recycle poinTs in Hellas)
HTC Hellas

February '10 **Erasmus Scholarship**
Institute of the National Scholarship (IKY)
for the Erasmus Winter Semester 2009-2010

January '07 **Best Project Award for the 1st generation of ROXANE**
Project: *ROXANE – Robotic Vehicle for Searching Survivors after an Earthquake (1st Generation)*
Technological Educational Institute of Kavala

February '07 **Erasmus Scholarship**
Institute of the National Scholarship (IKY)
for the Erasmus Summer Semester 2007

November ' 05 **Scholarship from IKY**
Institute of the National Scholarship (IKY)
for the year 2003-2004

FOREIGN LANGUAGES

September '07 - February '07 **German Lessons – Advanced**
University
Oldenburg/Ostfriesland/Wilhelmshaven (FH-OOW)
Department Wilhelmshaven, German

August '02 **Zertifikat Deutsch**
Goethe Institute
with general degree 139(max 225) and verbally 46(max 75)

May '01 **Certificate of Competency In English**
University of Michigan English Language Institute

PUBLICATIONS

Journal Papers per review

2013 **From Keyloggers to Touchloggers: Take the Rough with the Smooth.**
D. Damopoulos, G. Kambourakis, S. Gritzalis,
Computer & Security, 2013, Elsevier

2012 **Exposing mobile malware from the inside (or that is your mobile app really doing?**
D. Damopoulos, G. Kambourakis, S. Gritzalis, S. O. Park
Peer-to Peer Networking and Applications, 2012, Springer

2012 **User privacy and modern mobile services: Are they on the same path?**
D. Damopoulos, G. Kambourakis, M. Anagnostopoulos, S. Gritzalis, J. H. Park
Personal and Ubiquitous Computing, 2012, Springer

2012 **MILC: A Secure and Privacy-Preserving Mobile Instant Locator with Chatting.**
A. Loukas, D. Damopoulos, S.A. Menesidou, M.E. Skarkala, G. Kambourakis, S. Gritzalis
Information System Frontiers, 2012, Springer

2011 **Evaluation of Anomaly-Based IDS for Mobile Devices Using Machine Learning Classifiers.**
D. Damopoulos, S. A. Menesidou, G. Kambourakis, M. Papadaki, N. Clarke, S. Gritzalis,
Security and Communication Networks, 2011, Wiley

Conference Papers per review

2013 **A competent post-authentication and non-repudiation biometric-based scheme for m-Learning.**
G. Kambourakis, D. Damopoulos
The 10th IASTED International Conference on Web-based Education (WBE 2013). Innsburg, Austria, 2013, ACTA Press

2012 **Lifting the veil on mobile malware: A complete dynamic solution for iOS.**
D. Damopoulos, G. Kambourakis, S. Gritzalis, S. O. Park
The 2012 Summer FTRA International Symposium on Advances in Cryptography, Security and Applications for Future Computing (ACSA-Summer), Vancouver, Canada, 2012, FTRA

2012 **User-privacy and modern smartphones: A Siri(ous) dilemma**
D. Damopoulos, G. Kambourakis, M. Anagnostopoulos, S. Gritzalis, J. H. Park,
FTRA AIM 2012 International Conference on Advanced IT, Engineering and Management, Seoul, 2012, FTRA

2011 ***iSAM: An iPhone Stealth Airborne Malware***
D. Damopoulos, G. Kambourakis, S. Gritzalis
26th IFIP SEC 2011,Lucerne, Switzerland, 2011, Springer

Hardware and Software implementation

September '12 - Today
i.M.I.L.C. (iPhone Mobile Instant Locator and Chatting)
iOS programming
Under Developing
Website: http://milc.samos.aegean.gr/

January '12 Today
iDMA (iOS Dynamic Malware Analyzer)
iOS programming
Under Developing

November '11
iSPE (iOS Siri Privacy Exposer)
iOS programming

October '11
iTL (iOS TouchLogger)
iOS programming
Website: http://ibackup.samos.aegean.gr/iTL/

June '11
i.S.A.M (iPhone Stealth Airborne Malware)
iOS programming

September '10
E.A.R.T.H (Electrical Appliance Recycle poinTs in Hellas)
Android programming
Website: http://milc.samos.aegean.gr/andapp/f3.html

June '10
iBackUp (Collects iOS Data Files)
Java programming
Website: http://ibackup.samos.aegean.gr/

June '09
M.I.L.C (Mobile Instant Locator and Chatting) – *1st Version*
Android programming
Website: http://milc.samos.aegean.gr/

January '07
R.OX.AN.E (Robotic Vehicle for Searching Survivors after an Earthquake)
Hardware and Software implementation
Assembly programming, Sensor designing

Supervisor at students project

February '13 Today
Secure VoIP + File sharing extension for MILC
Let's Meet
Social Media Malware
Voice and Image authentication for smartphones
NFC Security
Augmented reality mobile game (Security-oriented)
Postgraduate Students
Android programming

Reverse Engineering Android Apps I
Reverse Engineering Android Apps II
Undergraduate Students
Android programming

February '12 **Malware for Android Platforms**
June '12 **UMTS Simulator**
Postgraduate Students
Android programming

Trojan Horse for PC
Postgraduate Students
Java programming

October '11 **WiFi Cracker**
June '11 **BlueSec**
SecSMS
CryptoFiles
Postgraduate Students
Android programming

Journals: Reviewer

International Journal On Advances in Internet Technology, IARIA

Security and Communication Networks (SCN), Wiley

Journal of Network and Computer Applications (JNCA), Elsevier

Conferences & Workshops: Reviewer

The 7th International Symposuim on Security and Multimodality in Pervasive Environment (SMPE-2013) in conjunction with The 27th IEEE International Conference on Advanced Information Networking and Applications (AINA-2013), (Barcelona : Spain), March 2013, IEEE Press

The International Conference on Computing, Networking and Communications(ICNC 2013), (San Diego : USA), January 2013, IEEE Press

The 7th International Conference on Frontier of Computer Science and Technology (FCST-12), Trust, Security and Privacy Track, (Suzhou : China), November 2012

The IEEE 8th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), (Barcelona : Spain), October 2012, IEEE Press

The 8th ACM International Symposium on QoS and Security for Wireless and Mobile Networks (ACM Q2SWinet 2012), (Paphos : Cyprus), October 2012

The International Conference on Computer Convergence Technology (ICCCT 2012), (Jeju : Korea), August 2012, Korea Knowledge Information Technology Society (KKITS)

The 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom-2012), (Liverpool : UK), June 2012, IEEE CS Press

The 2012 FTRA International Conference on Advanced IT, engineering and Management (FTRA AIM 2012), (Seoul : Korea), February 2012, FTRA

The 10th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom 2011), (Changsha : China), November 2011, IEEE Computer Society Press

The 2nd International Conference Ubiquitous Computing and Multimedia Applications (UCMA 2011),, (Daejeon : Korea), April 2011, Springer

4th IFIP International Conference on New Technologies, Mobility and Security (NTMS 2011) , (France : Paris), February 2011, IEEE Press

2nd International Conference on u- and e- Service, Science and Technology (UNESST 2010) , (Jeju Island : Korea), December 2010, Springer LNCS

International Workshop on Secure Multimedia Communication and Services (SECMCS2010), (Nanjing : China), November 2010, IEEE CS Press

6th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob 2010), (Ontario : Canada), October 2010, IEEE Press

---

RESEARCH OUTLINE

From Keyloggers to Touchloggers: Take the Rough with the Smooth.

The proliferation of touchscreen devices brings along several interesting research challenges. One of them is whether touchstroke-based analysis (similar to keylogging) can be a reliable means of profiling the user of a mobile device. Of course, in such a setting, the coin has two sides. First, one can employ the output produced by such a system to feed machine learning classifiers and later on intrusion detection engines. Second, aggressors can install touchloggers to harvest user's private data. This malicious option has been also extensively exploited in the past by legacy keyloggers under various settings, but has been scarcely assessed for soft keyboards. Compelled by these separate but interdependent aspects, we implement the first-known native and fully operational touchlogger for ultra modern smartphones and especially for those employing the proprietary iOS platform. The results we obtained for the first objective are very promising showing an accuracy in identifying misuses, and thus post-authenticating the user, in an amount that exceeds 99%. The virulent personality of such software when used maliciously is also demonstrated through real-use cases.

Exposing mobile malware from the inside (or that is your mobile app really doing?

It is without a doubt that malware especially designed for modern mobile platforms is rapidly becoming a serious threat. The problem is further multiplexed by the growing convergence of wired, wireless and cellular networks, since virus writers can now develop sophisticated malicious software that is able to migrate across network domains. This is done in an effort to exploit vulnerabilities and services specific to each network. So far, research in dealing with this risk has concentrated on the Android platform and mainly considered static solutions rather than dynamic ones. Compelled by this fact, in this paper, we contribute a fully-fledged tool able to dynamically analyze any iOS software in terms of method invocation (i.e., which API methods the application invokes and under what order), and produce exploitable results that can be used to manually or automatically trace software's behavior to decide if it contains malicious code or not. By employing real life malware we assessed our tool both manually, as well as, via heuristic techniques and the results we obtained seem highly accurate in detecting malicious code.

User privacy and modern mobile services: Are they on the same path?

Perhaps, the most important parameter for any mobile application or service is the way it is delivered and experienced by the end-users, who usually, in due course, decide to keep it on their software portfolio or not. Most would agree that security and privacy have both a crucial role to play toward this goal. In this context, the current paper revolves around a key question: Do modern mobile applications respect the privacy of the end-user? The focus is on the iPhone platform security and especially on user's data privacy. By the implementation of a DNS poisoning malware and two real attack scenarios on the popular Siri and Tethering services, we demonstrate that the privacy of the end-user is at stake.

Evaluation of Anomaly-Based IDS for Mobile Devices Using Machine Learning Classifiers.

Mobile devices have evolved and experienced an immense popularity over the last few years. This growth however has exposed mobile devices to an increasing number of security threats. Despite the variety of peripheral protection mechanisms described in the literature, authentication and access control cannot provide integral protection against intrusions. Thus, a need for more intelligent and sophisticated security controls such as intrusion detection systems (IDSs) is necessary. Whilst much work has been devoted to mobile device IDSs, research on anomaly-based or behaviour-based IDS for such devices has been limited leaving several problems unsolved. Motivated by this fact, in this paper, we focus on anomaly-based IDS for modern mobile devices. A dataset consisting of iPhone users data logs has been created, and various classification and validation methods have been evaluated to assess their effectiveness in detecting misuses. Specifically, the experimental procedure includes and cross-evaluates four machine learning algorithms (i.e. Bayesian networks, radial basis function, K-nearest neighbours and random Forest), which classify the behaviour of the end-user in terms of telephone calls, SMS and Web browsing history. In order to detect illegitimate use of service by a potential malware or a thief, the experimental procedure examines the aforementioned services independently as well as in combination in a multimodal fashion. The results are very promising showing the ability of at least one classifier to detect intrusions with a high true positive rate of 99.8%.

MILC: A Secure and Privacy-Preserving Mobile Instant Locator with Chatting.

The key issue for any mobile application or service is the way it is delivered and experienced by users, who eventually may decide to keep it on their software portfolio or not. Without doubt, security and privacy have both a crucial role to play towards this goal. Very recently, Gartner has identified the top ten of consumer mobile applications that are expected to dominate the market in the near future. Among them one can earmark location-based services in number 2 and mobile instant messaging in number 9. This paper presents a novel application namely MILC that blends both features. That is, MILC offers users the ability to chat, interchange geographic co-ordinates and make Splashes in real-time. At present, several implementations provide these services separately or jointly, but none of them offers real security and preserves the privacy of the end-users at the same time. On the contrary, MILC provides an acceptable level of security by utilizing both asymmetric and symmetric cryptography, and most importantly, put the user in control of her own personal information and her private sphere. The analysis and our contribution are threefold starting from the theoretical background, continuing to the technical part, and providing an evaluation of the MILC system. We present and discuss several issues, including the different services that MILC supports, system architecture, protocols, security, privacy etc. Using a prototype implemented in Google's Android OS, we demonstrate that the proposed system is fast performing, secure, privacy-preserving and potentially extensible.

A competent post-authentication and non-repudiation biometric-based scheme for m-Learning.

As mobile learning (mLearning) gains momentum, so does the worry of the parties involved to mLearning activities regarding the security and privacy level of the underlying systems and practices. Indeed, the basically spontaneous nature of mLearning and the variety of out-of-control devices that are used for supporting its activities, makes it prone to a plethora of attacks such as masquerading and man-in-the-middle. Thus, the provision of some sort of post- authentication and non-repudiation service in an effort to deter and repel ill-motivated activities may be of particular value in such realms. Compelled by this fact, in this paper, we introduce a dynamic signature-based biometric scheme to enable the offering of both of the aforementioned services in mLearning domains. We argue that our solution is both practical and lightweight. Its feasibility is also demonstrated through the use of machine learning techniques.

Lifting the veil on mobile malware: A complete dynamic solution for iOS.

It is without a doubt that malware especially designed for modern mobile platforms is rapidly becoming a serious threat. So far, research for dealing with this risk has concentrated on the Android platform and mainly considered static solutions rather than dynamic ones. Compelled by this fact, in this paper, we contribute a fully-fledged tool able to dynamically analyze any iOS software in terms of method invocation (i.e., which API methods the application invokes and under what order), and produce exploitable results that can be used to manually or automatically trace its behavior to decide if it contains malicious code or not. By employing real life malware we assessed our tool both manually as well as via heuristic techniques and the results we obtained are highly accurate in detecting malicious code.

User-privacy and modern smartphones: A Siri(ous) dilemma

The focus of this paper is on iPhone platform security and especially on user's data privacy. We are designing and implementing a new malware that takes over the iOS mDNS protocol and exposes user's privacy information by capitalizing on the new Siri facility. The attack architecture also includes a proxy server which acts as man-in-the-middle between the device and the Apple's original Siri server.

iSAM: An iPhone Stealth Airborne Malware

Modern and powerful mobile devices comprise an attractive target for any potential intruder or malicious code. The usual goal of an attack is to acquire users' sensitive data or compromise the device so as to use it as a stepping stone (or bot) to unleash a number of attacks to other targets. In this paper, we focus on the popular iPhone device. We create a new stealth and airborne malware namely iSAM able to wirelessly infect and self-propagate to iPhone devices. iSAM incorporates six different malware mechanisms, and is able to connect back to the iSAM bot master server to update its programming logic or to obey commands and unleash a synchronized attack. Our analysis unveils the internal mechanics of iSAM and discusses the way all iSAM components contribute towards achieving its goals. Although iSAM has been specifically designed for iPhone it can be easily modified to attack any iOS-based device.