Internet: Security and Privacy challenges
(October 24-28, 2015)
MHRD Scheme on Global Initiative on Academic Network (GIAN)

Overview

The Internet has made almost instantaneous access and dissemination of information possible. Increase in number of users as well as ever-growing number of applications have resulted in emergence of Internet as a necessity of modern life; be it banking, setting up business, academic portal etc. Downside is that anonymity and ease of remote access have made it possible for malicious users to exploit vulnerabilities.

With increase in popularity of Internet, devices such as smartphones, TVs etc. have become Internet enabled. This Internet connectivity have exposed these devices to Internet threats. Any information access through such devices can be eavesdropped and can also be used for remote control of devices. One way to secure devices is through scanning and analyzing inward network traffic for threats. Analysis of voluminous traffic data on-device is not possible in real-time. Clouds, on the other hand, can be used for such analyses as these have vast computational as well information stores.

Security threats against Internet are however a major concern for security architects and analysts. Awareness of these threats can prevent users from falling prey to social networking techniques used by malware authors. This awareness is much needed for research on security solutions. This course aims at discussing security aspects of Internet architecture, mobile cloud computing, online social networkings and state of the art research solutions in mitigating the security threats.

Objectives:

1. Overview of limitations of current Internet architecture and Content-Centric Networking as an alternative paradigm
2. Internet threats to mobile devices
3. Security aspects of mobile cloud computing
4. Security and privacy issues in Online Social Network

Course organization (10 Hours, 4 Modules each of 2.5 hours): Four modules are

1. Future Internet Architecture Security and Privacy challenges
2. Mobile Cloud Computing: Novel Privacy Issues and Possible Solutions
3. OnLine Social Network Security and Privacy
4. How to do a presentation; Exam

Course Details

Module 1: Future Internet Architecture Security and Privacy challenges

The Internet is an amazing success story, connecting hundreds of millions of users. However, in the last decade, there has been a growing realization that the current Internet Protocol is reaching the limits of its senescence. In fact, the way people access and utilize it has changed radically since the 1970-s when its architecture was conceived. This has prompted several research efforts that aim to design potential next-generation Internet architectures. In particular, Content-Centric Networking (CCN) is an emerging networking paradigm being considered as a possible replacement for the current IP-based host-centric Internet infrastructure. CCN focuses on content distribution, which is arguably not well served by IP. Named-Data Networking (NDN) is an example of CCN.

NDN is also an active research project under the NSF Future Internet Architectures (FIA) program. FIA emphasizes security and privacy from the outset and by design. To be a viable

Internet architecture, NDN must be resilient against current and emerging threats. In this talk, we highlight the main security and privacy issues we identified in NDN.

This lecture is based on the following research contributions:

[1] Alberto Compagno, Mauro Conti, Paolo Gasti, Gene Tsudik. Poseidon: "Mitigating Interest Flooding DDoS Attacks in Named Data Networking". *In Proceedings of the 38th IEEE Conference on Local Computer Networks* (IEEE LCN 2013), pp. 630-638, Sydney, Australia, October 21-24, 2013.

[2] Mauro Conti, Paolo Gasti, Marco Teoli. "A Lightweight Mechanism for Detection of Cache Pollution Attacks in Named Data Networking". In (Elsevier) *Computer Networks*, 57(16): 3178-3191, 2013.

[3] Alberto Compagno, Mauro Conti, Paolo Gasti, Luigi V. Mancini, Gene Tsudik. "Violating Consumer Anonymity: Geo-locating Nodes in Named Data Networking". *In Proceedings of the 13th International Conference on Applied Cryptography and Network Security* (ACNS 2015), in press, New York, NY, USA, June 2-5, 2015. (Best Student Paper Award)

[4] Alberto Compagno, Mauro Conti, Cesar Ghali, Gene Tsudik. "To NACK or not to NACK? Negative Acknowledgments in Information-Centric Networking". *In Proceedings of the 24th IEEE International Conference on Computer Communications and Networks* (IEEE ICCCN 2015), in press, Las Vegas, Nevada, USA, August 3 - 6, 2015.

[5] Moreno Ambrosin, Christoph Busold, Mauro Conti, Ahmad-Reza Sadeghi, Matthias Schunter. "Updaticator: Updating Billions of Devices by an Efficient, Scalable and Secure Software Update Distribution Over Untrusted Cache-enabled Networks". *In Proceedings of the European Symposium on Research in Computer Security* (ESORICS 2014), pp. 76-93, Wroclaw, Poland, September 7-11, 2014.

[6] Moreno Ambrosin, Mauro Conti, Paolo Gasti, Gene Tsudik. " Covert Ephemeral Communication in Named Data Networking". *In Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security* (ACM SIGSAC ASIACCS 2014), pages 15-26, Kyoto, Japan, June 4-6, 2014. DOI: 10.1145/2590296.2590306, ISBN: 978-1-4503-2800-5.

Module 2: Mobile Cloud Computing: Novel Privacy Issues and Possible Solutions

Mobile devices can be maliciously exploited to violate the privacy of people. In most attack scenarios, the adversary takes local or remote control of the device, by leveraging a vulnerability of the system, hence sending back the collected information to some web service. Apart from this type of more ``traditional" local exploits, we argue that several other threats are possible: an adversary might not interact actively with the mobile device, but he could be able to eavesdrop the network traffic of the device from the network side (e.g., controlling a Wi-Fi access point). The fact that the network traffic is often encrypted makes the attack even more challenging, but not impossible. In this lecture we discuss security aspects on mobile cloud computing, departing from traditiona local-device threats, and focusing on threats coming from eavesdropping (possibly encrypted) network traffic.

This lecture is based on the following research contributions:

[1] Mauro Conti, Nicola Dragoni, Sebastiano Gottardo. "MITHYS: Mind The Hand You Shake, Protecting mobile devices from SSL usage vulnerabilities". *In Proceedings of the 9th International Workshop on Security & Trust management* (ESORICS 2013 workshop: STM 2013), pp. 65-81, Egham, UK, September 12-13, 2013.

[2] Mauro Conti, Luigi V. Mancini, Riccardo Spolaor, Nino Vincenzo Verde. " Can't you hear me knocking: Identification of user actions on Android apps via traffic analysis". *In Proceedings of the 5th ACM Conference on Data and Application Security and Privacy* (ACM SIGSAC CODASPY 2015), to appear, San Antonio, TX, USA, March 2-4, 2015.

[3] Claudio Ardagna, Mauro Conti, Mario Leone, Julinda Stefa. " An Anonymous End-to-End Communication Protocol for Mobile Cloud Environments". *IEEE Transactions on Services Computing*, 7(3): pp. 373-386, 2014

[4] Mauro Conti, Luigi V. Mancini, Riccardo Spolaor, Nino Vincenzo Verde. " Analyzing Android Encrypted Network Traffic to Identify User Actions". *IEEE Transactions on Information Forensics & Security*, in press, 2016.

[5] Vincent F. Taylor, Riccardo Spolaor, Mauro Conti, Ivan Martinovic. "AppScanner: "Automatic Fingerprinting of Smartphone Apps From Encrypted Network Traffic". *In Proceedings of the 1st IEEE European Symposium on Security and Privacy* (IEEE EuroSP 2016), in press, Saarbrücken, Germany, March 21-24, 2016.

Module 3: OnLine Social Network Security and Privacy

In this lecture, we will discuss security and privacy issues raised by the usage of OnLine Social Networks (OSN). In particular, we will focus on aspects such as fake profile detection, techniques to violate and protect privacy in the ONS, as well as anonymization and de-anonymizatin approaches.

This lecture is based on the following research contributions:

[1] Mauro Conti, Radha Poovendran, Marco Secchiero. "FakeBook: Detecting Fake Profiles in On Line Social Networks". *In Proceedings of the 1st IEEE/ACM International Workshop on Cybersecurity of Online Social Network* (IEEE/ACM CSOSN 2012), pp. 1071-1078, Istanbul, Turkey, August 26, 2012.

[2] Mauro Conti, Arbnor Hasani, Bruno Crispo. " Virtual Private Social Networks and a Facebook Implementation". *ACM Transactions on the Web*, 7(3), 14:1--14:31, 2013.

[3] Filipe Beato, Mauro Conti, Bart Preneel . " Friend in the Middle (FiM): Tackling Social Networks De-Anonymization. *In Proceedings of the 5th IEEE International Workshop on SECurity and SOCial Networking* 2013 (IEEE SESOC 2013, workshop of PerCom 2013), pages. 279-284, San Diego, CA, USA, March 18-22, 2013.

[4] Filipe Beato, Mauro Conti, Bart Preneel, Dario Vettore. " VirtualFriendship: Hiding interactions on Online Social Networks". *In Proceedings of the IEEE Conference on Communications and Network Security* (IEEE CNS 2014), in press, San Francisco, CA, USA, October 29-31, 2014.

[5] Giuseppe Cascavilla, Andrea Burattin, Mauro Conti. " SocialSpy: Browsing (Supposedly) Hidden Information in Online Social Networks". *In Proceedings of the 9th International Conference on Risks and Security of Internet and Systems* (CRiSIS 2014), in press, Trento, Italy, August 27-29, 2014

Module 4: How to do a presentation

In this lecture we will host presentation of research topics chosen by students. For each presentation, it will follow a discussion in class with all the group of students, and will be given feedback to the presenter on the presentation, as well as possible research ideas and directions.

The Faculty

Dr. Mauro Conti is Associate Professor, University of Padua, where he is founder and leader of the SPRITZ Security and Privacy Research Group and EU Marie Curie Fellow at Department of Mathematics, University of Padua. He is a leading researcher in security and privacy. In this area, he has published more than 140 papers in international peer-reviewed journals (IEEE TDSC, IEEE TPDS, IEEE TIFS, ACM TWEB, IEEE TSC, IEEE COMST, etc.) and conferences (USENIX Security, ACM CCS, ACM AsiaCCS, ACM WiSec, ACM SACMAT, ACM MobiHoc, ACNS, IEEE ICDCS, and ESORICS, etc.). He is Associate Editor for several journals, including IEEE Communications Surveys & Tutorials and and IEEE Transactions for Information Forensics and Security. He has served as Program Committee member of several conferences, including ACM WiSec, ACM CODASPY, ACM SACMAT, IEEE INFOCOM, IEEE CNS, IEEE PASSAT, IEEE MASS, and ACNS. He was panelist at ACM CODASPY 2011. He was General Chair for SecureComm 2012 and ACM SACMAT 2013, and Program Chair for several conferences including TRUST 2015 and ICISS 2016, and for the Security Track of IEEE CCNC '16. As a visiting researcher, he has been to the Center for Secure Information Systems (CSIS) at George Mason University, Vrije Universiteit Amsterdam, UCLA, Los Angeles and UCI, Irvine.

Home Page: http://www.math.unipd.it/~conti/index.html