The 9th International Conference on Network and System Security
NSS 2015

November 3rd – 5th, 2015
New York, USA

Conference Program and Information Booklet

Organized By

IEEE CSCloud 2015 Committees, NSS 2015 Committees

Sponsored By

Springer

Pace University,

New York Institute of Technology

Longxiang High Tech,

North America Chinese Talents Association

NSS 2015 Program at a Glance

Tuesday, November 3rd, 2015

Time	Room A	Room C-D
8:30 AM - 9:00 AM	Welcome Opening	
9:00 AM - 10:40 AM		NSS WSP
10:40 AM - 11:00 AM	Coffee Break	
11:00 AM -12:40 PM		NSS SSS
12:40 PM - 1:40 PM	Lunch Break (On your own)	
1:40 PM - 3:20 PM		NSS SSCS
3:20 PM - 3:40 PM	Coffee Break	
3:40 PM - 5:20 PM		NSS APS
5:20 PM - 6:35 PM		NSS SMT

Wednesday, November 4th, 2015

Time	Room A	Room C-D
8:30 AM - 9:30 AM	Keynote: Michael Reiter	
9:30 AM - 9:50 AM	Coffee Break	
9:50 AM - 11:30 AM		NSS ACG
11:30 AM - 12:50 PM		NSS SMCS
12:50 AM - 1:50 PM	Lunch Break (On your own)	
1:50 PM - 2:50 PM	Keynote: Gene Tsudik	
3:00 PM - 4:40 PM		NSS CPSM
6:00 PM - 8:30 PM	Banquet (out of venue)	

Thursday, November 5th, 2015

Time	Room A	Room C-C
8:00 AM - 9:40 AM		NSS SGM
9:40 AM - 10:00 AM	Coffee Break	
10:00 AM - 11:00 AM	Keynote: Steven M. Bellovin	
11:10 AM - 12:30 PM		NSS SSM
12:30 PM - 1:30 PM	Lunch Break (On your own)	
1:40 PM - 6:00 PM		

NSS Keynote

Nov. 4th, 2015, Wednesday, 8:30 AM – 9:30 AM, Room A.

Michael Reiter

University of North Carolina at Chapel Hill, USA

Bio: Michael Reiter is the Lawrence M. Slifkin Distinguished Professor in the Department of Computer Science at the University of North Carolina at Chapel Hill. His research interests include all areas of computer and communications security and distributed computing. His professional responsibilities during his career so far have included Director of Secure Systems Research at Bell Labs; founding Technical Director of CyLab at Carnegie Mellon University; program chair for the the flagship computer security conferences of the IEEE, the ACM, and the Internet Society; and Editor-in-Chief of ACM Transactions on Information and System Security, among others. Dr. Reiter was named an ACM Fellow in 2008 and an IEEE Fellow in 2014.

TITLE: Side-Channels in Multi-Tenant Environments

Abstract: Due to the massive adoption of computing platforms that consolidate potentially distrustful tenants' applications on common hardware --- both large (public clouds) and small (smartphones) --- the security provided by these platforms to their tenants is increasingly being scrutinized. In this talk we review highlights from the last several years of research on a long-suspected but, until recently, largely hypothetical attack vector on such platforms, namely "side-channel attacks". In these attacks, one tenant learns sensitive information about another tenant simply by running on the same hardware with it, but without violating the logical access control enforced by the platform's isolation software (virtual machine monitor or operating system). We will then summarize various strategies we have explored to defend against side-channel attacks in their various forms, both inexpensive defenses against specific attacks and more holistic but expensive protections.

NSS Keynote

Nov. 4th, 2015, Wednesday, 1:50 PM—2:50 PM, Room A

Gene Tsudik

Chancellor's Professor of Computer Science

University of California, Irvine, USA

Bio: Gene Tsudik is a Chancellor's Professor of Computer Science at the University of California, Irvine (UCI). He obtained his PhD in Computer Science from USC in 1991. Before coming to UCI in 2000, he was at IBM Zurich Research Laboratory (1991-1996) and USC/ISI (1996-2000). Over the years, his research interests included many topics in security and applied cryptography. He is the Director of Secure Computing and Networking Center (SCONCE) at UCI. Gene Tsudik is a former Fulbright Scholar and a fellow of the ACM and the IEEE. From 2009 to 2015 he served as the Editor-in-Chief of ACM Transactions on Information and Systems Security (TISSEC).

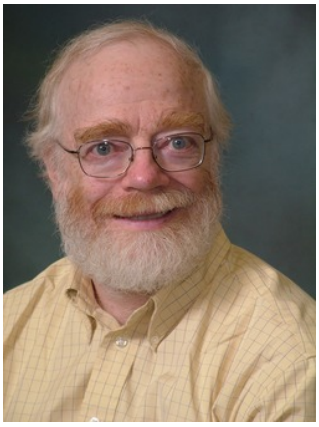
TITLE: Secure and Private Proximity-Based Discovery of Common Factors in Social Networks

Abstract: The recent decade has witnessed a rapid increase in popularity of mobile personal devices (notably, smartphones) that function as all-purpose personal communication portals. Concurrently, On-line Social Networks (OSNs) have continued their impressive proliferation. Meanwhile, the notion of "OSN privacy" remains elusive and even self-contradictory. Centralized nature of prominent OSNs is unlikely to change, which does not bode well for OSN users' privacy. However, some user privacy can be gained from making certain OSN functionality available off-line, such as discovering common contacts and other features, as well as establishing affinity-based connections. OSNs stand to gain from this, since users could avail themselves of OSN functionality in scenarios where none currently exists, e.g., whenever Internet connectivity is unavailable, expensive or insufficient. At the same time, OSN users benefit from increased privacy because off-line interactions are invisible to OSN providers.

This talk will explore off-line private proximity-based use of OSNs and will present a working system (called UnLinked) that is grafted atop a popular OSN -- LinkedIn. One key challenge is how to ensure integrity, authenticity and privacy of users' profile information when they engage in off-line interactions. This can be addressed via specialized privacy-agile cryptographic protocols. This talk will overview the design, architecture and functionality of UnLinked and will highlight important outstanding issues.

NSS Keynote

Nov. 5th, 2015, Thursday, 10:00 AM—11:00 AM, Room A



Steven M. Bellovin

Columbia University, New York, USA

Bio: Steven M. Bellovin is the Percy K. and Vidal L. W. Hudson Professor of computer science at Columbia University, where he does research on networks, security, and especially why the two don't get along, as well as related public policy issues. In his spare professional time, he does some work on the history of cryptography. He joined the faculty in 2005 after many years at Bell Labs and AT&T Labs Research, where he was an AT&T Fellow. He received a BA degree from Columbia University, and an MS and PhD in Computer Science from the University of North Carolina at Chapel Hill. While a graduate student, he helped create Netnews; for this, he and the other perpetrators were given the 1995 Usenix Lifetime Achievement Award (The Flame). Bellovin has served as Chief Technologist of the Federal Trade Commission. He is a member of the National Academy of Engineering and is serving on the Computer Science and Telecommunications Board of the National Academies, the Department of Homeland Security's Science and Technology Advisory Committee, and the Technical Guidelines Development Committee of the Election Assistance Commission; he has also received the 2007 NIST/NSA National Computer Systems Security Award and has been elected to the Cybersecurity Hall of Fame.

TITLE: Thinking Security

Abstract: Many computer applications are bound to a particular point in time; more precisely, to a given set of technologies and costs. The same is true of computer security. Unfortunately, once something becomes possible people become wedded to it, and never look back at the environment and assumptions that made it possible or even necessary. This is especially serious for security, since it causes us to endure the costs and annoyances of marginally useful (or even harmful) mechanisms while blinding us to newer threats. What can be done? How can we recognize the implicit assumptions in what we're doing? Can we do better in the future? How do differing threat models affect the question?

Technical Program

The 9th International Conference on Network and System Security (NSS 2015)

Day 1 (11/3)

Welcome

8:30 AM--9:00 AM

NSS WSP: Wireless Security and Privacy

Tuesday 9:00 AM—10:40 AM, Room C-D *Session Chair: Brian Ricks*

Dandelion - Revealing Malicious Groups of Interest in Large Mobile Networks
Wei Wang, Mikhail Istomin and Jeffrey Bickford.

Distance-based Trustworthiness Assessment for Sensors in Wireless Sensor Networks
Jongho Won and Elisa Bertino.

Isolation of Multiple Anonymous Attackers in Mobile Networks
Brian Ricks and Patrick Tague.

No Place to Hide that Bytes won't Reveal: Sniffing Location-Based Encrypted Traffic to Track a User's Position
Giuseppe Ateniese, Briland Hitaj, Luigi Vincenzo Mancini, Nino Vincenzo Verde and Antonio Villani.

Coffee Break: 10:40 AM –11:00 AM

NSS SSS: Smartphone and Systems Security

Tuesday 11:00 AM—12:40 PM, Room C-D *Session Chair: Meikang Qiu*

Compartmentation Policies for Android Apps: A Combinatorial Optimization Approach
Guillermo Suarez-Tangil, Juan Tapiador and Pedro Peris-Lopez.

Unraveling the Security Puzzle: A Distributed Framework to Build Trust in FPGAs
Devu Manikantan Shila, Vivek Venugopalan and Cameron Patterson.

Android Botnets: What URLs are telling us
Andi Fitriah Abdul Kadir, Natalia Stakhanova and Ali Akbar Ghorbani.

DisARM: Mitigating Buffer Overflow Attacks on Embedded Devices
Javid Habibi, Ajay Panicker, Aditi Gupta and Elisa Bertino.

Lunch Break (On Your Own)
12:40 PM – 1:40 PM

NSS SSCS: Short Papers Security Cloud Systems

Thursday 1:40 PM—3:20 PM, Room C-D *Session Chair: P. Krishnan*

A Game Theoretic Framework for Cloud Security Transparency
Abdulaziz Aldribi and Issa Traore

Detecting malicious activity on smartphones using sensor measurements

Roger Piqueras Jover, Ilona Murynets and Jeffrey Bickford

VICI: Visual Caller Identification for Contact Center Applications
P. Krishnan and Navjot Singh

Let's Get Mobile: Secure FOTA for Automotive Systems
Hafizah Mansor, Konstantinos Markantonakis, Raja Naeem Akram and Keith Mayes

Performance Analysis of Real-Time Covert Timing Channel Detection using a Parallel System
Ross Gegan, Dipak Ghosal, Rennie Archibald and Matthew Farrens

Coffee Break: 3:20 PM – 3:40 PM

NSS APS: Application Security

Tuesday 3:40 PM—5:20 PM, Room C-D *Session Chair: Qingji Zheng*

RouteMap: A Route and Map Based Graphical Password Scheme for Better Multiple Password Memory
Weizhi Meng.

Indicators of Malicious SSL Connections
Riccardo Bortolameotti, Andreas Peter, Maarten H. Everts and Damiano Bolzoni.

Multi-constrained Orientation Field Modeling and Its Application for Fingerprint Indexing
Jinwei Xu and Jiankun Hu.

Service in denial - clouds going with the winds
Vit Bukac, Vlasta Stavova, Lukas Nemec, Zdenek Riha and Vashek Matyas.

NSS SMT: Security Management

Tuesday 5:20 PM—6:35 PM, Room C-D *Session Chair: Ravi Sandhu*

A framework for policy similarity evaluation and migration based on change detection
Jaideep Vaidya, Basit Shafiq, Vijay Atluri and David Lorenzi.

MT-ABAC: A Multi-Tenant Attribute-Based Access Control Model with Tenant Trust
Navid Pustchi and Ravi Sandhu.

Managing Multi-dimensional Multi-granular Security Policies using Data Warehousing
Mahendra Pratap Singh, Shamik Sural, Vijay Atluri, Jaideep Vaidya and Ussama Yaqub.

Day 2 (11/4)

NSS Keynote: Michael Reiter

Nov. 4th, 2015, Wednesday, 8:30 AM – 9:30 AM, Room A. *Session Chair: Shouhuai Xu*

Coffee Break: 9:30 AM – 9: 50 AM

NSS ACG: Applied Cryptography

Wednesday 9:50 AM—11:30 AM, Room C-D *Session Chair: Chunhua Su*

CLKS: Certificateless Keyword Search on Encrypted Data
Qingji Zheng, Xiangxue Li and Aytac Azgin.

Secure Cloud Storage for Dynamic Group: How to Achieve Identity Privacy-Preserving and Privilege Control
Hui Ma and Rui Zhang.

GP-ORAM: A Generalized Partition ORAM
Jinsheng Zhang, Wensheng Zhang and Daji Qiao.

Anonymous Evaluation System
Lucjan Hanzlik, Kamil Kluczniak, Miroslaw Kutylowski and Przemysław Kubiak.

NSS SMCS: Short Papers Mobile and Cloud Security

Thursday 11:30 AM – 12:50 PM, Room C-D *Session Chair: Jiankun Hu*

De-anonymizable Location Cloaking for Privacy-controlled Mobile Systems
Chao Li and Balaji Palanisamy.

First-Priority Relation Graph-based Malicious Users Detection in Mobile Social Networks
Li Xu, Limei Lin and Sheng Wen.

A Study of Network Domains Used in Android Applications
Mark Fioravanti, Ayush Shah and Shengzhi Zhang.

Detecting Malicious Temporal Alterations of ECG signals in Body Sensor Networks
A Hang Cai and Krishna Venkatasubramanian

Lunch Break (On Your Own)
12:50 PM – 1:50 PM

NSS Keynote: Gene Tsudik

Nov. 4th, 2015, Wednesday, 1:50 PM—2:50 PM, Room A *Session Chair: Meikang Qiu*

NSS CPSM: Cryptosystems

Thursday 3:00 PM–4:40 PM, Room C-D *Session Chair: Xiaoshuang Ma*

An Efficient Leveled Identity-Based FHE

Fuqun Wang, Kunpeng Wang and Bao Li.

Evolving Highly Nonlinear Balanced Boolean Functions with Optimal Resistance to DPA Attacks

Ashish Jain and Narendra S. Chaudhari.

Related-Key Rectangle Attack on Round-reduced \textit{Khudra} Block Cipher

Xiaoshuang Ma and Kexin Qiao.

A New Statistical Approach For Integral Attack

Jiageng Chen, Atsuko Miyaji, Chunhua Su and Liang Zhao.

Banquet (Out of Venue)
6:00PM -- 8:30 PM

Day 3 (11/5)

NSS SGM: Short Papers Cryptographic Mechanisms

Thursday 8:00 AM – 9:40 AM, Room C-C *Session Chair: Atsuko Miyaji*

Foundations of Optical Encryption: A Candidate Short-key Scheme
Giovanni Di Crescenzo, Shahab Etemad and Ron Menendez.

From Pretty Good To Great: Enhancing PGP using Bitcoin and the Blockchain
Duane Wilson and Giuseppe Ateniese.

A Scalable Multiparty Private Set Intersection
Atsuko Miyaji and Shohei Nishida.

Electronic Contract Signing without Using Trusted Third Party
Zhiguo Wan, Robert Deng and David Lee.

New Message Authentication Code Based on APN Functions and Stream Ciphers
Teng Wu and Guang Gong.

Coffee Break
9:40 AM – 10:00 AM

NSS Keynote: Steve M. Bellovin

Nov. 5th, 2015, Thursday, 10:00 AM—11:00 AM, Room A *Session Chair: Shouhuai Xu*

NSS SSM: Short Papers Security Mechanisms

Wednesday 11:10 AM – 12:30 PM, Room C-C *Session Chair: Longbin Chen*

Assessing Attack Surface with Component-based Package Dependency
Su Zhang, Xinwen Zhang, Xinming Ou, Nigel Edwards, Jing Jin and Liqun Chen.

An Abstraction for the Interoperability Analysis of Security Policies
Javier Baliosian and Ana Cavalli.

Cryptographically Secure On-Chip Firewalling
Jean-Michel Cioranesco, Craig Hampel, Rodrigo Portella Do Canto and Guilherme Ozari De Almeida.

Enforcing Privacy in Distributed Multi-Domain Network Anomaly Detection
Christian Callegari, Stefano Giordano and Michele Pagano.

General Information

Registration Desk

The Registration Desk will be open to assist you at the following times:

- Tuesday, November 3rd, 2015, 08:00 – 18:00
- Wednesday, November 4th, 2015, 08:00 – 18:00
- Thursday, November 5th, 2015, 08:00 – 12:00

Location: Main Lobby.

Conference materials, name badges, and other proceedings will be distributed at the Registration Desk.

Name Badges

All delegates, sponsors, speakers, and attendees of CSCloud/NSS 2015, associated workshops, and summit will be provided with a name badge, to be collected upon registration. This badge must be worn at all times as it is your official pass to all sessions of the conferences, lunches, morning and afternoon teas, and banquets.

Social Events

Welcome Reception

Banquet Dinner: 6:00 PM – 8:30 PM, Wednesday, November 4th, 2015.

Presentation Instruction

You are required to arrive at the room (in which you will deliver your talk) at least 15 minutes before the commencement of the session. Upon arrival please confirm your attendance with the Session Chair and familiarize yourself with the venue. Please bring with you a single paragraph summary, including your name (as you would like to be introduced), affiliation and research interests (maximum 100 words). Please present this to the Session Chair upon arrival, for use for introductory purposes, prior to your talk. Upon arrival, please copy your slides file to the presentation computer. If you plan to use your own equipment, please ensure it is ready to go prior to the session commencing, since there is very little time between presentations. If you have requested optional equipment, ensure that is in the room. For all assistance, please speak to the Session Chair.

Message Board

Any program changes or urgent announcements from the secretariat and private messages will be posted on the message board in the registration area. Please check the message board occasionally.

Venue

Auditorium on Broadway (AoB):

The AoB is located at 1871 Broadway, New York, a few blocks from the 59th street - Colombus Circle subway station (trains: A, B, C, D, 1).

Route: From Grand Central Station to Auditorium on Broadway