DON'T MISS THE CO-LOCATED WORKSHOPS

Washington, DC • August 9–10, 2010

Workshops will be held before the 19th USENIX Security Symposium. See each workshop's Web site for information about how to participate as well as the latest program information.

EVT/WOTE '10: 2010 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections

Monday–Tuesday, August 9–10, 2010
www.usenix.org/evtwote10

EVT/WOTE '10 brings together researchers from a variety of disciplines, ranging from computer science and human-computer interaction experts through political scientists, legal experts, election administrators, and voting equipment vendors.

CSET '10: 3rd Workshop on Cyber Security Experimentation and Test

Monday, August 9, 2010
www.usenix.org/cset10

CSET '10 will focus on the science, design, architecture, construction, operation, and use of cyber security experiments in network testbeds and infrastructures. While specifically centered on works that relate to emulation testbeds, the workshop's scope includes all work relevant to cyber security experimentation and evaluation (e.g., simulation, deployment, traffic models).

WOOT '10: 4th USENIX Workshop on Offensive Technologies

Monday, August 9, 2010
www.usenix.org/woot10

The 4th USENIX Workshop on Offensive Technologies aims to bring together researchers and practitioners in system security to present research advancing the understanding of attacks on operating systems, networks, and applications.

HealthSec '10: 1st USENIX Workshop on Health Security and Privacy

Tuesday, August 10, 2010
www.usenix.org/healthsec10

HealthSec '10 is intended as a forum for discussion of aggressively innovative and potentially disruptive ideas on all aspects of medical and health security and privacy. A main goal is to promote cross-disciplinary interactions among fields, including technology, medicine, and policy.

HotSec '10: 5th USENIX Workshop on Hot Topics in Security

Tuesday, August 10, 2010
www.usenix.org/hotsec10

HotSec '10 takes a broad view of security and privacy and encompasses research on topics including, but not limited to, large-scale threats, network security, hardware security, software security, programming languages, applied cryptography, anonymity, human-computer interaction, sociology, and economics.

MetriCon 5.0: Fifth Workshop on Security Metrics

Tuesday, August 10, 2010
http://www.securitymetrics.org/content/Wiki.jsp?page=Metricon5.0

MetriCon 5.0 is the fifth annual conference dedicated to security metrics. It is a forum for presenting new approaches for measuring information security effectiveness, with a bias towards practical, specific approaches. Attendance at Metricon 5.0 is by invitation only. Find out how to participate on the workshop's Web site.

CollSec '10: 2010 Workshop on Collaborative Methods for Security and Privacy

Tuesday, August 10, 2010
www.usenix.org/collsec10

CollSec '10 aims to bring to the forefront innovative approaches that involve the use of collaborative methods for privacy and security. While the workshop will touch on themes that lie at the heart of the USENIX Security Symposium, discussion will focus on the boundary between collaborative algorithms and swarm intelligence and the implementation domains of networking, privacy, and security.

Register for workshops and USENIX Security '10 at www.usenix.org/sec10/register

19th USENIX SECURITY SYMPOSIUM

Washington, DC • August 11–13, 2010

The USENIX Security Symposium brings together researchers, practitioners, system administrators, system programmers, and others interested in the latest advances in the security of computer systems and networks.

The 3-day program includes:

Keynote Address by:

- Roger G. Johnston, *Vulnerability Assessment Team, Argonne National Laboratory*

Refereed Papers:

- Refereed paper presentations showcasing new research in a variety of subject areas including cryptography, using humans, dissecting bugs, and more

Invited Talks by Industry Experts such as:

- "Understanding Scam Victims: Seven Principles for Systems Security," by Frank Stajano, *Senior Lecturer at the University of Cambridge, UK*
- "End-to-End Arguments: The Internet and Beyond," by David P. Reed, *MIT Media Laboratory*
- Plus a Poster Session, BoFs, and more

Stay Connected...

http://www.usenix.org/facebook/sec10

http://twitter.com/USENIXSecurity

Co-Located Workshops:

EVT/WOTE '10: 2010 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections
August 9–10, 2010

CSET '10: 3rd Workshop on Cyber Security Experimentation and Test
August 9, 2010

WOOT '10: 4th USENIX Workshop on Offensive Technologies
August 9, 2010

CollSec '10: 2010 Workshop on Collaborative Methods for Security and Privacy
August 10, 2010

HealthSec '10: 1st USENIX Workshop on Health Security and Privacy
August 10, 2010

HotSec '10: 5th USENIX Workshop on Hot Topics in Security
August 10, 2010

MetriCon 5.0: Fifth Workshop on Security Metrics
August 10, 2010

Register by July 19, 2010, and save! **www.usenix.org/sec10**

19th USENIX Security Symposium

Washington, DC

August 11–13, 2010

For program updates and to register, see www.usenix.org/sec10.

Wednesday, August 11, 2010

9:00 a.m.–10:30 a.m.

Keynote Address: Proving Voltaire Right: Security Blunders Dumber Than Dog Snot

Roger G. Johnston, *Vulnerability Assessment Team, Argonne National Laboratory*

Voltaire famously said (sort of) that the main problem with common sense is that it is not all that common. Security is a case in point. We repeatedly encounter security devices and systems with little or no security built in. This talk gives examples of common design blunders, easy-to-exploit vulnerabilities, and sloppy thinking associated with electronic devices involving physical security, including locks, tags, GPS, RFIDs, biometrics, and voting machines. I will also discuss common blunders in how organizations think about security. I'll conclude by proposing reasons why common sense and security are often alien to each other and suggest possible countermeasures—some of which involve examining what cyber security and physical security could learn from each other.

11:00 a.m.–12:30 p.m.

Refereed Papers: Protection Mechanisms

Adapting Software Fault Isolation to Contemporary CPU Architectures
David Sehr, Robert Muth, Cliff Biffle, Victor Khimenko, Egor Pasko, Karl Schimpf, Bennet Yee, and Brad Chen, *Google, Inc.*

Making Linux Protection Mechanisms Egalitarian with UserFS
Taesoo Kim and Nickolai Zeldovich, *MIT CSAIL*

Capsicum: Practical Capabilities for UNIX
Robert N.M. Watson and Jonathan Anderson, *University of Cambridge;* Ben Laurie and Kris Kennaway, *Google, Inc.*

Invited Talk: Toward an Open and Secure Platform for Using the Web

Will Drewry, *Software Security Engineer, Google*

As users spend more of their computing time in the interconnected world of the Internet, their software and data are exposed to attackers at an increasing rate. Web browser developers are pursuing features to mitigate this, but these mechanisms are primarily restricted to the browser itself. Google Chrome OS is an open source, lightweight OS built for simplicity, speed, and security for Web-focused users. Its security functionality extends beyond the benefits of the browser, Google Chrome, to the core OS environment. I will explore the design and implementation of that functionality and the challenges that lie ahead.

2:00 p.m.–3:30 p.m.

Refereed Papers: Privacy

Structuring Protocol Implementations to Protect Sensitive Data
Petr Marchenko and Brad Karp, *University College London*

PrETP: Privacy-Preserving Electronic Toll Pricing
Josep Balasch, Alfredo Rial, Carmela Troncoso, Bart Preneel, Ingrid Verbauwhede, and Christophe Geuens, *K.U. Leuven*

An Analysis of Private Browsing Modes in Modern Browsers
Gaurav Aggarwal and Elie Burzstein, *Stanford University;* Collin Jackson, *CMU;* Dan Boneh, *Stanford University*

Invited Talk: Windows 7 Security from a UNIX Perspective

Crispin Cowan, *Senior Program Manager, Windows Core Security, Microsoft, Inc.*

UNIX advocates, including me, have long mocked Windows for having a fundamentally insecure computing model. Issues leveled at Windows have included the lack of separation of privilege between the user and the TCB, a willingness to execute code from untrusted sources, and myriad buffer overflow vulnerabilities. However, most of these criticisms pertain to Windows XP or the 9X series. Much has changed between those and Windows 7. I will compare and contrast the security of Windows and UNIX, at both technological and cultural levels, with results that may surprise members of both communities.

4:00 p.m.–5:30 p.m.

Refereed Papers: Detection of Network Attacks

BotGrep: Finding P2P Bots with Structured Graph Analysis
Shishir Nagaraja, Prateek Mittal, Chi-Yao Hong, Matthew Caesar, and Nikita Borisov, *University of Illinois at Urbana-Champaign*

Fast Regular Expression Matching Using Small TCAMs for Network Intrusion Detection and Prevention Systems
Chad R. Meiners, Jignesh Patel, Eric Torng, Alex X. Liu, and Eric Norige, *Michigan State University*

Searching the Searchers with SearchAudit
John P. John, *University of Washington;* Fang Yu, Yinglian Xie, and Martín Abadi, *Microsoft Research Silicon Valley;* Arvind Krishnamurthy, *University of Washington*

Invited Talk: TBA

James Lewis, *Senior Fellow and Program Director at the Center for Strategic and International Studies*

Please see www.usenix.org/sec10/tech for updates.

6:00 p.m.–7:30 p.m. **Symposium Reception**

Thursday, August 12, 2010

9:00 a.m.–10:30 a.m.

Refereed Papers: Dissecting Bugs

Toward Automated Detection of Logic Vulnerabilities in Web Applications
Viktoria Felmetsger, Ludovico Cavedon, Christopher Kruegel, and Giovanni Vigna, *University of California, Santa Barbara*

Baaz: A System for Detecting Access Control Misconfigurations
Tathagata Das, Ranjita Bhagwan, and Prasad Naldurg, *Microsoft Research India*

Cling: A Memory Allocator to Mitigate Dangling Pointers
Periklis Akritidis, *University of Cambridge, UK*

Invited Talk: Staying Safe on the Web Yesterday, Today, and Tomorrow

Sid Stamm, *Security & Privacy Nut at Mozilla*

The World Wide Web is rapidly evolving, and its corresponding security and privacy problems are changing, too. More than ever before, user agents such as Firefox are being relied upon to provide a safe browsing experience, and so we must adapt to the ever-changing state of the Web. Sid will recount some stories of security problems in Mozilla's past and will examine the current state of security and privacy in Firefox. Finally, he will describe the future of the Web browser, covering Mozilla's plans for upcoming releases and examining some questions in Web security and privacy that don't yet have answers.

11:00 a.m.–12:30 p.m.

Refereed Papers: Cryptography

ZKPDL: A Language-Based System for Efficient Zero-Knowledge Proofs and Electronic Cash
Sarah Meiklejohn, *University of California, San Diego;* C. Chris Erway and Alptekin Küpçü, *Brown University;* Theodora Hinkle, *University of Wisconsin—Madison;* Anna Lysyanskaya, *Brown University*

Practical Large-Scale Privacy-Preserving Distributed Computation Robust against Malicious Users
Yitao Duan, *NetEase Youdao, Beijing, China;* John Canny, *University of California, Berkeley*

SEPIA: Privacy-Preserving Aggregation of Multi-Domain Network Events and Statistics
Martin Burkhart, Mario Strasser, Dilip Many, and Xenofontas Dimitropoulos, *ETH Zurich, Switzerland*

Invited Talk: The Evolution of the Flash Security Model

Peleus Uhley, *Senior Security Researcher, Adobe*

The Adobe Flash Player security model must address several complex challenges: meeting the needs of enterprise admins, end users, Web site owners, and content creators; adapting and scaling as improvements are made to Web standards; functioning in multiple browsers on multiple operating systems installed on desktop PCs, mobile devices, and more; and providing a security model that is consistent for everyone regardless of their combination of browser, OS, and device. I will discuss how Adobe is addressing some of these challenges through real-world case studies, from past events that resulted in significant changes to the security model to what factors are now influencing us. I will close with some thoughts on future challenges as the Web expands from the desktop onto mobile devices, tablets, and TVs.

2:00 p.m.–3:30 p.m.

Refereed Papers: Internet Security

Dude where's that IP? Circumventing Measurement-based IP Geolocation
Phillipa Gill and Yashar Ganjali, *University of Toronto;* Bernard Wong, *Cornell University;* David Lie, *University of Toronto*

Idle Port Scanning and Non-interference Analysis of Network Protocol Stacks Using Model Checking
Roya Ensafi, Jong Chun Park, Deepak Kapur, and Jedidiah R. Crandall, *University of New Mexico*

Building a Dynamic Reputation System for DNS
Manos Antonakakis, Roberto Perdisci, David Dagon, Wenke Lee, and Nick Feamster, *Georgia Institute of Technology*

Invited Talk: Understanding Scam Victims: Seven Principles for Systems Security

Frank Stajano, *Senior Lecturer at the University of Cambridge, UK*

The success of many attacks on computer systems can be traced back to the security engineers not understanding the psychology of the users they meant to protect. Paul Wilson and I examined a variety of scams that were investigated, documented, and recreated for the BBC TV programme *The Real Hustle* and we extracted from them some principles about the recurring behavioral patterns of victims that hustlers have learnt to exploit. We argue that an understanding of these vulnerabilities, and the need to take them into account during design rather than shifting blame onto the users, is a paradigm shift for the security engineer which, if adopted, will lead to stronger systems security.

Thursday, August 12, 2010 (continued)

4:00 p.m.–5:30 p.m.

Refereed Papers: Real-World Security

Scantegrity II Municipal Election at Takoma Park: The First E2E Binding Governmental Election with Ballot Privacy
Richard Carback, *UMBC CDL;* David Chaum; Jeremy Clark, *University of Waterloo;* John Conway, *UMBC CDL;* Aleksander Essex, *University of Ottawa;* Paul S. Herrnson, *CAPC, UMCP;* Travis Mayberry, *UMBC CDL;* Stefan Popoveniuc, *GW;* Ronald L. Rivest and Emily Shen, *MIT CSAIL;* Alan T. Sherman, *UMBC CDL;* Poorvi L. Vora, *GW*

Acoustic Side-Channel Attacks on Printers
Michael Backes, *Saarland University and Max Planck Institute for Software Systems (MPI-SWS);* Markus Dürmuth, Sebastian Gerling, Manfred Pinkal, and Caroline Sporleder, *Saarland University*

Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study
Ishtiaq Rouf, *University of South Carolina, Columbia;* Rob Miller, *Rutgers University;* Hossen Mustafa and Travis Taylor, *University of South Carolina, Columbia;* Sangho Oh, *Rutgers University;* Wenyuan Xu, *University of South Carolina, Columbia;* Marco Gruteser, Wade Trappe, and Ivan Seskar, *Rutgers University*

Invited Talk: TBA

Please see www.usenix.org/sec10/tech for updates.

6:00 p.m.–7:30 p.m. **Poster Session & Happy Hour** See www.usenix.org/sec10/poster for how to submit a poster.

Friday, August 13, 2010

9:00 a.m.–10:30 a.m.

Refereed Papers: Web Security

VEX: Vetting Browser Extensions for Security Vulnerabilities
Sruthi Bandhakavi, P. Madhusudan, Samuel T. King, and Marianne Winslett, *University of Illinois at Urbana-Champaign*

Securing Script-Based Extensibility in Web Browsers
Vladan Djeric and Ashvin Goel, *University of Toronto*

AdJail: Practical Enforcement of Confidentiality and Integrity Policies on Web Advertisements
Mike Ter Louw, Karthik Thotta Ganesh, and V.N. Venkatakrishnan, *University of Illinois at Chicago*

Invited Talk: TBA

Scott Borg, *Chief Economist, US Cyber Consequences Unit*

Please see www.usenix.org/sec10/tech for updates.

11:00 a.m.–12:30 p.m.

Refereed Papers: Securing Systems

Realization of RF Distance Bounding
Kasper Bonne Rasmussen and Srdjan Capkun, *ETH Zurich*

The Case for Ubiquitous Transport-Level Encryption
Andrea Bittau and Michael Hamburg, *Stanford;* Mark Handley, *UCL;* David Mazières and Dan Boneh, *Stanford*

Automatic Generation of Remediation Procedures for Malware Infections
Roberto Paleari, Lorenzo Martignoni, and Emanuele Passerini, *Università degli Studi di Milano;* Drew Davidson, Matt Fredrikson, and Somesh Jha, *University of Wisconsin;* Jon Giffin, *Georgia Institute of Technology*

Invited Talk: TBA

Please see www.usenix.org/sec10/tech for updates.

2:00 p.m.–3:30 p.m.

Refereed Papers: Using Humans

Re: CAPTCHAs—Understanding CAPTCHA Solving from an Economic Context
Marti Motoyama, Kirill Levchenko, Chris Kanich, Damon McCoy, Geoffrey M. Voelker, and Stefan Savage, *University of California, San Diego*

Chipping Away at Censorship Firewalls with User-Generated Content
Sam Burnett, Nick Feamster, and Santosh Vempala, *Georgia Tech*

Fighting Coercion Attacks in Key Generation Using Skin Conductance
Payas Gupta and Debin Gao, *Singapore Management University*

Invited Talk: End-to-End Arguments: The Internet and Beyond

David P. Reed, *MIT Media Laboratory*

A key factor supporting the Internet's growth is the use of "end-to-end arguments" to decide where to place functionality in the overall architecture. Many assert that the Internet in its maturity must begin to lock in specialized functions for mobile phones, video conferencing, cyberwarfare enablement, and more. Reed, one of the authors who co-articulated the end-to-end argument as a design principle, argues that it is not dead—it is more important than ever.