Introduction to Web and Internet Security

Patrick McDaniel
AT&T Labs - Research
Florham Park, NJ
pdmcdan@research.att.com

Avi Rubin
Johns Hopkins University
Baltimore, MD
rubin@jhu.edu

Abstract

Ever wonder what that key at the bottom of the browser means? Or what a firewall is? Have you ever been authenticated, and if not, does it hurt? What is a VPN and do they come in blue? This tutorial will answer these and many other questions related to the security of our digital lives.

Over the course of this one day tutorial, we present an introduction to the methods and pitfalls of Web and Internet security. We explore the types of security being used to support applications and services on the Web with a focus on practical issues. The terminology and use of contemporary security is described, and best practices explained. Topics covered include, but are not restricted to, the basics of cryptography, certificate management, (web) server security, and wireless security and privacy. The tutorial concludes with a brief survey of emerging areas and applications in Web and Internet security.

1 Tutorial Overview and Objectives

There are many common misconceptions on the purpose, efficacy, and use of security on the Internet in general, and the web in specific. This has directly contributed to the lack of real security in applications and services in the past. Well documented vulnerabilities and attacks have undermined the average user's confidence in the Internet. This trend will continue until better security tools are made available and safer computing is practiced by administrators and end users. One key area that needs attention is education: the average user must be able to make informed choices about the way she conducts herself on the Internet. She will have the ability to make these choices only after she understands the implications of her actions. The primary goal of this tutorial is to give the attendees just this understanding.

This one day tutorial is aimed at informing the general WWW community about the terminology, technologies, and emerging trends in web and Internet security. Targeted at both practitioners or researchers, we will explore the purpose and technologies of Internet and Web security. The structure of the tutorial will be to build from a basic description of security, then move to general areas (Web and network security), and finally to describe emerging trends in security research. We will provide examples taken from the expected attendees domains. Where possible, we will demonstrate particular technologies (e.g., VPNs) and attacks (e.g., snarf, on WEP).

Both presenters are experienced teachers. Rubin and McDaniel have taught several tutorials and courses on topics in general security. Much of the content will be drawn from these sources, as well as from the books on the topic area Rubin has authored. Rubin and McDaniel are also active researchers in the security community. They both have published in the major security conferences and have thier work highlighted in the national and international press. Rubin has been the vice-chair of the security and privacy track of WWW, and served as program chair of many of the major conferences in the area. McDaniel has served on numerous program comittees and is presently acting as depty vice-chair for the the security and privacy track of WWW.

Tutorial Outline

1. Introduction to security
    - (a) What is security?
    - (b) General terminology
    - (c) How security impacts the average user
    - (d) Attacks, threats, and trust
2. Cryptography basics
    - (a) Encryption, decryption
    - (b) Keys, lengths, and harness
    - (c) Asymmetric key cryptography
    - (d) Hash functions
    - (e) Authentication
    - (f) PKI and key management
    - (g) Privacy
3. Web security
    - (a) What is web security?
    - (b) Web authentication (basic and digest)
    - (c) SSL
    - (d) Cookies
    - (e) Web code: Java, Javascript, and Active-X
4. Network security
    - (a) Networking basics: IP, routing, and network management
    - (b) Firewalls
    - (c) IPsec
    - (d) DDOS
5. Security tools
    - (a) Intrusion Detection
    - (b) DDOS counter-measures
    - (c) VPNS
6. Emerging Trends and Open Problems
    - (a) Routing Security
    - (b) Wireless networks
    - (c) Document management (e.g., HIPPA)

General Information

Title : Introduction to Web and Internet Security
Contact: Patrick McDaniel (pdmcdan@research.att.com)
Duration: full day
Prerequisite knowledge: general Computer Science background
Available for Publication: yes

Bio for Dr. Patrick McDaniel

Patrick Drew McDaniel is a principle researcher at AT&T Labs-Research and an Adjunct Professor of the Stern School of Business at New York University (NYU) in Manhattan. Dr. McDaniel received his Ph.D. from the University of Michigan in 2001 and subsequently joined the highly regarded Secure Systems Group at AT&T Research. His research efforts have focused on distributed systems security, scalable public key infrastructures, routing security, and component architectures. As a Principle Investigator of the DARPA funded Antigone project, McDaniel has investigated languages and architectures for security policy determination and enforcement. PMcDaniel's interests lie in experimental computer science focusing on systems evaluation, design, and implementation.

Dr. McDaniel has published works in the top information and network security conferences. His widely cited paper from the 2003 IEEE Conference on Security and Privacy, ”Methods and Limitations of Security Policy Reconciliation”, established the asymptotic limits of policy management. This work has lead to collaboration in areas such Grid computing and component systems with researchers and faculty at top institutions. McDaniel has sat on the program committees for several or the major systems and security conferences including USENIX Annual Technical Conference, the USENIX Security Symposium, and WWW. He has also been a frequent member of NSF proposal evaluation panels and taught tutorials on various topics in information security and Internet privacy. McDaniel has had his research reported on in many news outlets including the New York Times and the International Herald Tribute, and has been interviewed on CNN Financial News.

Bio for Dr. Avi Rubin

Dr. Avi Rubin is Associate Professor of Computer Science and Technical Director of the Information Security Institute at Johns Hopkins University. Prior to joining Johns Hopkins Rubin was a research scientist at AT&T Labs. Rubin is author of several books including Firewalls and Internet Security, second edition (with Bill Cheswick and Steve Bellovin, Addison Wesley, 2003), White-Hat Security Arsenal (Addison Wesley, 2001), and Web Security Sourcebook (with Dan Geer and Marcus Ranum, John Wiley & Sons, 1997). He is Associate Editor of ACM Transactions on Internet Technology, Associate Editor of IEEE Security & Privacy, and an Advisory Board member of Springer's Information Security and Cryptography Book Series. Rubin serves on the board of directors of the USENIX Association.