



DEPAUL UNIVERSITY

COLLEGE OF COMPUTING AND DIGITAL MEDIA

Institute for Professional Development

WIRELESS LAN SECURITY PROGRAM

An eight-week in-depth program covering the latest solutions to wireless LAN security issues

DePaul University's Wireless LAN Security Program presents a comprehensive study of current wireless LAN (WLAN) security technologies. The program focuses on teaching networking and security professionals the technologies and tools to build a secure WLAN. The program will begin with an overview of common security attacks against WLANs and the vulnerability of the 802.11 standard. The program then delves into a variety of security protection methods, including Wired Equivalent Privacy (WEP), tunnel-based Virtual Private Network (VPN), Port-based Access Control (802.1X), RADIUS service for authentication, Temporal Key Integrity Protocol (TKIP), and the Advanced Encryption Standard (AES), along with a discussion of the strengths and weaknesses of these methods.

Classroom lectures will be complemented by in-class lab demonstrations, reading, assignments, and hands-on lab exercises. Various tools used at the wireless security labs at DePaul University will be presented. Students in the program will use these tools to evaluate the performance of various WLAN security technologies.

YOU WILL LEARN ABOUT:

- Common security attacks against wireless LANs
- Wireless LAN services and the IEEE 802.11 standard
- Problems with the Wired Equivalency Privacy (WEP) algorithm
- Pros and cons of a tunnel-based Virtual Private Network (VPN) solution
- Hotspots and authentication services
- 802.1X and the Extensible Authentication Protocol (EAP)
- Authentication with RADIUS (Remote Authentication Dial In User Service)
- Key management
- 802.11i data encryption: Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES)
- Wi-fi Protected Access® (WPA) 1.0 and WPA® 2.0
- Wireless LAN performance and security management
- Security policy and compliance considerations

DePaul University
College of Computing and Digital Media
Institute for Professional Development
243 S. Wabash Avenue, Room 301
Chicago, IL 60604-2300
(312)362-6282
ipd.cdm.depaul.edu

WIRELESS LAN SECURITY PROGRAM

The proliferation of wireless LAN installations, from enterprise environments to homes and hotspots, has made WLANs ubiquitous. For the enterprise, the many benefits of wireless connectivity are an important factor in decisions about technology investments and the cost of doing business. However, their widespread use and ease of installation has also introduced many security challenges. The risks of an unsecure WLAN are many: exposure of an organization's network traffic; unauthorized access to network resources, including the potential for malicious exploitation of those resources; the difficulty of monitoring rogue Access Points (AP) on company premises, etc. Because solutions to WLAN security issues are varied and WLAN standards are always evolving, the Wireless LAN Security Program is designed to provide an in-depth understanding of current technologies and an overview of the pros and cons of various solutions.

The Wireless LAN Security Program begins with a discussion of common security threats against WLANs, and their impact on the enterprise. To build a solid foundation for WLAN security, an overview of the IEEE 802.11 standard with a focus on the Medium Access Control (MAC) protocol will be presented. The program will then cover the original approach to wireless security, Wired Equivalent Privacy (WEP); the problems with WEP; and the pros and cons of using tunnel-based Virtual Private Networks (VPNs), a common solution that addresses many problems of WEP.

The comprehensive solution to WLAN security is 802.11i. It adopts the 802.1X standard to address the issue of authentication. For issues of data integrity and encryption, 802.11i offers two solutions. An evolutionary approach is Temporal Key Integrity Protocol (TKIP), which is backward compatible with WEP. A better and more secure approach is Counter Mode with CBC-MAC Protocol (CCMP), which is a replacement for WEP. The program will discuss both of these encryption protocols in detail. Of course, technology alone cannot address all security issues; therefore, the program will also touch on security policy and quality assurance to develop a comprehensive solution to securing WLANs.

The Wireless LAN Security Program is designed for network/security professionals who will benefit from these technologies and tools to build a secured WLAN. Students in the program will gain the knowledge to identify the most cost-effective solution from different vendors and will also learn to develop business cases for WLANs. The pros and cons of all solutions will be discussed, along with ongoing challenges and continuing research in WLAN security.

CURRICULUM

The following topics are covered in the program. Each unit involves reading and assignments, and in addition, most units also include in-class lab exercises.

PROGRAM INTRODUCTION AND WIRELESS LAN SECURITY THREATS

Program overview. Fundamentals of wireless services (802.11, 802.15, and 802.16). Common threats against wireless LANs.

OVERVIEW OF WIRELESS LANS

802.11 standards. Physical layer. Medium Access Control (MAC) layer (DCF, PCF, and HCF). Wireless LAN design (frequency reuse).

SECURITY FUNDAMENTALS AND WIRED EQUIVALENCY PRIVACY (WEP)

Fundamentals of network security: authentication and encryption. Authentication in 802.11. Wired Equivalent Privacy (WEP). Cracking WEP encryption.

HOTSPOTS, AUTHENTICATION SERVICES AND VPN

Hotspots and authentication services. NoCat for hotspots. Virtual Private Networks (VPNs). Tunnel-based VPNs (PPTP, L2TP, and OpenVPN).

802.1X AND RADIUS SERVER

The 802.1X Port-based Authentication Protocol. RADIUS (Remote Authentication Dial In User Service) server.

**EXTENSIBLE AUTHENTICATION
PROTOCOL (EAP) METHODS AND
KEY MANAGEMENT**

EAP for Wireless services. 802.11i key management. EAP-TLS. EAP-TTLS. Protected Extensible Authentication Protocol (PEAP).

802.11 DATA ENCRYPTION

802.11i overview. Message Integrity Code (MIC). Temporal Key Integrity Protocol (TKIP) and Wi-Fi Protected Access (WPA) 1.0. AES (Advanced Encryption Standard)/CCMP and WPA 2.0

**WIRELESS LAN SECURITY
MANAGEMENT**

WLAN security policy and compliance. SNMP (Simple Network Management Protocol) for WLAN security management. Security monitoring. Performance management. Course review.

GENERAL INFORMATION

ADMISSION

Professional experience in the networking industry is highly desired. Applicants should have basic knowledge of PC architecture and the Windows and Linux operating systems as well as general concepts of computer networks, including Ethernet and TCP/IP.

A substantial commitment of time is required for this intensive course of study. Final admission will be determined by the admissions committee on the basis of an applicant's overall qualifications, including work history and educational background.

FACILITIES

To promote the learning process, the Institute maintains special-purpose laboratories as well as dedicated classrooms equipped with state-of-the-art audio/visual equipment.

In addition, the School's unique Course OnLine (COL) technology allows students to replay lectures over the Internet. COL captures and replays five components of the classroom experience—audio, video, PC screen, whiteboard, and document camera input—and incorporates them into one interface to provide an innovative rebroadcast system. Lab-based components conducted outside of the classroom are not recorded. Students are encouraged to attend all lectures.

SCHEDULE

The Institute offers one section of the program each quarter. Classes meet one evening per week.

FACULTY

The program will be taught by a faculty member from the College of Computing and Digital Media. Faculty will be available throughout the program both in person and through electronic mail.

COLLEGE OF COMPUTING AND DIGITAL MEDIA

The college, through its School of Computing and its School of Cinema and Interactive Media, offers a variety of programs at the undergraduate and graduate levels. Over 1,000 students are enrolled in the college's bachelor's programs and over 2,000 students are enrolled in the master's and Ph.D. programs making the college's graduate program one of the largest in the country. The college offers more than 200 courses each quarter, many in the evening, in several locations: the Loop Campus, the Lincoln Park Campus, the O'Hare Campus, the Naperville Campus, and the Rolling Meadows Campus. Many of the degree programs are also available exclusively online.

Current offerings at the undergraduate level include:

School of Computing

Computer Games Development
Computer Graphics and Motion Technology
Computer Science
Computing
Information Assurance and Security Engineering
Information Systems
Information Technology
Interactive Media
Math and Computer Science
Network Technology

School of Cinema and Interactive Media

Animation
Computer Games Development
Computer Graphics and Motion Technology
Digital Cinema
Interactive Media

Current offerings at the graduate level include:

School of Computing

Applied Technology
Business Information Technology
Computer Graphics and Motion Technology
Computational Finance
JD/MS in Computer Science Technology
JD/MS in Computer Science Technology
Computer Information and Network Security
E-Commerce Technology
Human-Computer Interaction
Information Systems
Information Technology
Instructional Technology Systems
IT Project Management
Software Engineering
Telecommunications Systems

School of Cinema and Interactive Media

Computer Games Development
Computer Graphics and Motion Technology
Digital Cinema – MS
Digital Cinema – MFA
Human-Computer Interaction

INSTITUTE FOR PROFESSIONAL DEVELOPMENT

The Institute for Professional Development was formed by the college in 1984 to assist both individuals and businesses in keeping pace with the rapid development of computer technologies. The Institute currently offers a variety of intensive certificate programs in these areas:

- Advanced SQL
- IT Project Management
- Java™ Developer
- Java™ EE Developer (formerly J2EE Developer)
- Java™ Web Services
- Lightweight Java™ Web Development
- .NET Developer
- Ruby on Rails®
- SharePoint® Developer
- SQL Server® Business Intelligence
- SQL Server® Database Administration
- Web Development with Python®

APPLICATION PROCEDURE:

Complete the enclosed application and return it with a non-refundable \$40.00 application fee (check or money order made payable to DEPAUL UNIVERSITY) to:

DePaul University
Wireless LAN Security Program
Institute for Professional Development
243 S. Wabash Avenue, Room 301
Chicago, IL 60604-2300

The words "Wi-fi Protected Access", "WPA", "SharePoint", "SQL Server", "Python", "Java", "J2EE", "Sun", and "Ruby on Rails" are either registered or unregistered trademarks in the United States of America and/or other countries. The Wireless LAN Security Program at DePaul University is an independent program of study and is not affiliated with, nor has it been authorized, sponsored, or otherwise approved by any external entities.