

Wireless Networks Security and Design

College/Division: Chicago State University, Department of Technology and Education

Course Designator/Number: IT 4350

Credit Hours: 3.0

Instructor/Originator Name: Dr. Moussa Ayyash

Course Description: This course covers the basics of the well-known *Wireless Fidelity* (Wi-Fi) technology, wireless communications theory, security vulnerabilities, and techniques/protocols used for securing Wi-Fi networks.

Today's wireless networking products are ubiquitous and cover many areas of our life. The advances in our current information technology infrastructures can be easily noticed in both wired and wireless applications. The widespread usage of networking solutions, in general, and wireless networks, in particular, makes it extremely important to pay attention to how to secure these networks. Due to the open nature of wireless networks, providing information security is challenging.

This course mainly concentrates on the design and security aspects of *wireless local area networks* (WLAN) -- Wi-Fi (short for "Wireless Fidelity"). Also, the course will discuss Wi-MAX (short for "Worldwide Interoperability for Microwave Access") networks which is the technology for wireless "metropolitan area networks". Wi-MAX can provide broadband wireless access up to 30 miles for fixed stations and 3 - 10 miles for mobile stations.

The course will provide students with the necessary knowledge on these wireless networks and technologies, configuration procedures, threats, and security algorithms and protocols.

In addition to the theoretical content of the course, the course is supported by hands-on exercises (software and hardware). Each student is required to purchase his own equipment to be able to do the lab assignments. A list of the needed equipment is included below.

Prerequisites: None

Restrictions/Suggestions: A background in network and data communications theory is preferable.

Rationale: This course will introduce students to one of today's very important and growing wireless technologies. It will provide students with necessary skills and terminologies that are needed to deal with wireless networks technologies security and design issues.

Intended Audience: Individuals interested in homeland security topics that are mainly related to how to secure and design wireless networks.

Expected Student Outcomes:

- 1) Display knowledge of the theoretical aspects and necessary basics of wireless communications.
- 2) Identify security vulnerabilities and threats in wireless networking solutions.
- 3) Assess all risks involved in using wireless networking environs.
- 4) Design and diagram efficient and reliable wireless networks. Reliability will be addressed through planning for emergency actions in case of unexpected failures.
- 5) Apply various security techniques for information safety for private and public networks.
- 6) Synthesize safe and security information in order to create a safe and secure wireless networks. This includes introducing students to several security algorithms and protocols.
- 7) Design and diagram efficient and reliable wireless networks. Reliability will be addressed through planning for emergence actions in case of unexpected failures.

Texts:

Required: Mark Ciampa, CWSP Guide to Wireless Security. Course Technology Incorporated, 2007, ISBN: 1-4188-3637-0. ISBN-13: 978-1-4188-3637-5

Recommended: Wireless Network Security by Y. Xiao, X. Shen, and D. Du.

(ISBN:0387280405) and WiMAX: Standards and Security (WiMAX) by S. Ahson (ISBN: 1-4200-4523-7)

Required Hardware and Software:

To perform the hands-on exercises of this course, each student is required to have the following:

- 1) One Wi-Fi certified IEEE 802.11b, a, g, or n **wireless network adapter**. Linksys USB wireless adapter such as WUSB54G or WUSB600N is recommended.
- 2) One Linksys WRT54G (or WRT160N) Wireless Router or equivalent.
- 3) A computer with Windows XP professional/home or Vista.
- 4) Internet connection to download free software.

All required hardware can be easily purchased online. The cost of all needed hardware should not exceed \$100.

Topical/Subject Matter Outline/Course Content:

- 1) Introduction to Networking Theory: Historical background, wired versus wireless, and Open Systems Interconnection (OSI) model overview.
- 2) Wireless Theory Background: Key terms include (Signals, Frequency, Analogue, Digital, Binary, coding and encoding, antenna types and structures).
- 3) Overview of Wireless Networks Types and Technologies: Cellular, wireless LANs, Bluetooth, and sensor networks.
- 4) Details on Wi-Fi and WiMAX basics and implementation issues. Both types will be compared.
- 5) Security Vulnerabilities: Physical layer, MAC layer, IP layer, Transport layer, and the Application layer.
- 6) Layered Security Techniques and Protocols: Intrusion detection, secure PHY/MAC/IP protocols, attacks and prevention, key management, secure group communications/multicast, secure location services, monitoring and surveillance.
- 7) Basic Skills for Designing and Securing Wireless Networks.

Course Activities:

- Lecture and group discussions of key ideas through Elluminate Session.
- Real-life examples will be posted on Blackboard.
- Reading assignments from textbook chapters.
- Students will be asked to present their thoughts regarding wireless networking challenges.
- Prepare short research papers on: “Current Challenges to Wi-Fi Networking” and “Security Challenges for Wi-MAX networks”.
- “Current Challenges to Wi-Fi Networking.”
- Homework problems will be assigned.
- Students will be introduced to several simulation tools, such as Netstumbler.
- Final project: Design a wireless network while considering security and reliability aspects that are discussed in the course. The design should be presented using a report and a network diagram. Details of the project will be posted on Blackboard during the second week of classes.

Evaluation/Assessment:

Item	Points
Online tests - using Blackboard Testing Tool	15
Homework – Submitted using Turn-It-In inside Blackboard	10
Short Research Papers	15
Lab activities	15
Participation in discussion boards and Elluminate sessions	15
Final Project (Site Survey Analysis) – Submitted using Turn-It-In inside Blackboard	15
Final Exam – Using Blackboard Testing Tool	15
Total	100

Each student’s grade will be calculated based on the following weighting scale:

Range	Letter Grade
90–100	A
80–89.99	B
70-79.99	C
60-69.99	D
Below 60	F

Instructor’s Course Syllabus**Bibliography/References:**

- www.blackboard.com
- Guide to Wireless Network Security; by J. Vacca
- Wireless Communications Security; by H. Imai, M. Rahman, and K. Kobara
- www.privacyrights.org
- www.Qualnet.com
- Netstumbler.com