

EE 584 Wireless System Security Syllabus

Catalog Description:

EE 584 Wireless System Security (3-0-3)

This course addresses system security issues in wireless systems, including satellite, terrestrial microwave, military tactical communications, public safety, cellular and wireless LAN networks. Security topics include confidentiality/privacy, integrity, availability, and control of fraudulent usage of networks. Issues addressed include jamming, interception and means to avoid them. Case studies and student projects are an important component of the course.

Text Book:

“Wireless Security – Models, Threats, and Solutions,” by Nichols and Lekkas, McGraw-Hill, 2002, ISBN 0071380388.

Instructor:

Bruce McNair, Distinguished Service Professor of ECE.

Goals:

The goal of Wireless System Security is to familiarize students with the issues and technologies involved in designing a wireless system that is robust against attack. Students will gain an understanding of the various ways in which wireless networks can be attacked and tradeoffs in protecting networks. Students will gain an appreciation of the need to develop an understanding of underlying system applications and potential security issues early in the design process.

Prerequisites by Topic:

- Probability and random variables
- Calculus
- System Theory
- Switching Theory and Logical Design

Grading Policy:

Individual activities:

Three research papers	15% each
Participation in security assessments	20%
Final project report:	25%
Final project presentation:	10%

All assignments provide opportunities for extra credit work. Work that goes significantly beyond what is asked will be graded accordingly.

Course Components:

- Engineering - 100%

Course Web Site:

<http://koala.stevens-tech.edu/~bmcnair/WSS-xxx> where xxx is current semester (e.g., S04)

Schedule of Topics

This is the list of detailed topics and likely order. The specific schedule is TBD.

Common topics overview

Wireless

- Characteristics
- Channels
- Propagation
- Types of wireless systems and their parameters
 - Satellite
 - Terrestrial microwave
 - Military tactical
 - Cellular
 - AMPS
 - 2G – IS-136, GSM, IS-95
 - WLAN
 - 802.11

Security

- Definition
- Services
- Mechanisms
 - Spread spectrum
 - Frequency hopping
 - Encryption
 - Integrity check-sums
- Assessment
- Issues, specifically related to wireless
 - Jamming
 - DFing, geolocation
 - Interception
 - Spoofing
 - Fraud
 - Theft of service
 - Traffic analysis

Specific examples (case studies) – for each of these, the subject matter is covered as: context, problem, solutions, tradeoffs

Satellite

- Jamming
- Theft of service – entertainment services on downlink
- Hidden signals – theft of service – uplink
- Monitoring long distance communications

Terrestrial microwave

- Jamming
- Compromise of information and signaling

Military tactical

- Antijam (AJ)
- Low Probability of Intercept (LPI)
- Circular Error Probability (CEP)
- Spoofing
- Confidentiality of information

Traffic analysis

Cellular

Cloning of AMPs – fraudulent use/theft of service

Privacy issues

E911/Geolocation

WLAN

WEP issues

Managing a wireless LAN interconnected to wired LAN

Summary - What is the general lesson learned from these case studies?

Advanced Topics and Future Directions

Last revised: February 25, 2004