1 Summary

CprE 537 provides an overview of the special issues associated with the security of wireless systems. The course starts by introducing wireless communications basic concepts and vulnerabilities, it discusses some basic security solutions – from spread-spectrum to cryptography – with specific protocol examples, and ends with an information-theoretic perspective on security – which provides insights into coding, encryption and physical-layer secrecy.

Instructor:
George T. Amariucai, Ph.D.
Office: 212N Nuclear Engineering Bld.
Phone: (515) 294-6982
Office Hours: M: 11-12; R: 3-4; F: 9-10
email: gamari@iastate.edu

Location and Time:
Online Lectures will be uploaded on Blackboard Learn

2 Class Website

The class website can be found at:
http://home.engineering.iastate.edu/~gamari/CprE537_S13/
The website contains important information for this class and will be updated regularly. Please keep up with the website changes, so that you become aware of any posted assignments, notes or announcements.

3 Course Description and References

I. Wireless Communications Basics

- wireless transmission basics (propagation, antennas, modulation);
- wireless system modeling (noise, fading, interference);

II. Spread Spectrum Communications

- spread spectrum basics (models, FH, TH, DS);
- classical systems and their anti-jamming properties;

III. Introduction to Wireless Cryptographic Security

- brief introduction to ciphers and secrecy (scramblers, stream ciphers, block ciphers);
- specific security problems of wireless networks;
IV. The Cryptographic Protocols Behind Common Wireless Applications

- WiFi: WEP, WPA, weaknesses and attacks;
- Bluetooth;
- GSM and 3G;

V. RFID Security
[D. M. Dobkin, The RF in RFID: Passive UHF RFID in practice, Newnes, 2008]
[F. Thornton et al., RFID Security, Syngress, 2006]
- introduction to the RFID technology;
- security problems of RFID;
- RFID standards and associated security protocols;

VI. Information-Theoretic Perspective
[T. M. Cover, J. A. Thomas, Elements of Information Theory, John Wiley and Sons, 2006]
- introduction to information theory (entropy, information);
- secrecy, source coding and channel coding (redundancy, error-correction, equivocation)
- about physical-layer secrecy, common randomness, and their applications.

4 Assignments and Grading

<table>
<thead>
<tr>
<th>Evaluation</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Homeworks</td>
<td>60%</td>
</tr>
<tr>
<td>Project</td>
<td>20%</td>
</tr>
<tr>
<td>Final Exam</td>
<td>20%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Grade</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>[90,100]</td>
</tr>
<tr>
<td>- B +</td>
<td>(80,83)</td>
</tr>
<tr>
<td>- C +</td>
<td>(70,73)</td>
</tr>
<tr>
<td>- D +</td>
<td>(60,63)</td>
</tr>
<tr>
<td>F</td>
<td>[0,60]</td>
</tr>
</tbody>
</table>

- Homeworks will be assigned throughout the semester. Unless otherwise specified, the deadline for turning in a homework is exactly two weeks after the date it was assigned (on the same day of the week, before class).
- Projects involve teams of no more than three people, and the association and topic are at your discretion. You must report your team and your chosen topic to the instructor, for approval, as soon as you pick them, but no later than Friday, February 22 (the sixth week).
- Late homework will be accepted only within one week of the deadline. A penalty of 20% will be applied towards any late work, except in the case of university-approved absences, when adequate extensions will be granted.
- The final exam will be take-home and comprehensive.

5 Special Accommodation

Iowa State University complies with the American with Disabilities Act and Section 504 of the Rehabilitation Act. Any student who may require special accommodation under such provisions should immediately contact the instructor of this course, and the Disability Resources (DR) office, for information on appropriate policies and procedures. The Disability Resources (DR) office is located in the Student Services Building, Room 1076, phone: 515-294-7220.