Mobile and Wireless Security
CSCE 496/896
Lecture # 1
Introduction

Instructor: Nirnimesh Ghose
Computer Science and Engineering
Lecture Set Overview

Course objective

Grading

Course outline

Literature review project

Final project

How to read and present a paper
Course Objective

Understand and articulate the meaning of security properties (such as secrecy, privacy, authentication, integrity, etc.) in context of wireless and/or mobile security.

Identify hard open-problems in the area and understand why they are hard.

Explain the research methods employed by a paper and why they were appropriate (or not).

Propose novel research idea within areas of wireless and/or mobile security.

Give one or more technical talk(s).

Write a high-quality review of wireless and/or mobile security conference/journal papers.
Class Timings

Tuesday and Thursday

9:30AM to 10:45AM

101 Louise Pound Hall
Course Website

Canvas - Quizzes

https://cse.unl.edu/~nghose/csce496896.php - Reading material
<table>
<thead>
<tr>
<th>Event</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Ideas Presentations</td>
<td>September 05, 2019</td>
</tr>
<tr>
<td>Work on Lit Review Project (outside class)</td>
<td>September 06 -- October 30, 2019</td>
</tr>
<tr>
<td>Project Due</td>
<td>October 31, 2019</td>
</tr>
<tr>
<td>Work on Final Proposal (outside class)</td>
<td>November 01 – December 02, 2019</td>
</tr>
<tr>
<td>Final Presentations</td>
<td>December 03 -- 12, 2019</td>
</tr>
<tr>
<td>Final Proposal Due</td>
<td>December 13, 2019</td>
</tr>
</tbody>
</table>
Grading Policy

Presentation  20%

Quizzes and/or Paper Summary  20%

Literature Review Project  25%

Final Proposal  25%

Class participation  10%
<table>
<thead>
<tr>
<th>Course Outline</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview of course and syllabus</td>
<td>1 day (week 1)</td>
</tr>
<tr>
<td>Basics of cryptography and security</td>
<td>2 days (weeks 1 and 2)</td>
</tr>
<tr>
<td>Project ideas presentations</td>
<td>1 day (week 2)</td>
</tr>
<tr>
<td>Wireless Security -- Context based key extraction and evolution</td>
<td>2 days (week 3)</td>
</tr>
<tr>
<td>Wireless Security -- Secret free confidentiality</td>
<td>2 days (week 4)</td>
</tr>
<tr>
<td>Mobile Security -- Hardware/embedded security</td>
<td>2 days (week 6)</td>
</tr>
<tr>
<td>Mobile Security -- Device fingerprint (hardware/channel)</td>
<td>2 days (week 7)</td>
</tr>
<tr>
<td>Wireless Security -- MAC layer misbehavior</td>
<td>2 days (week 8)</td>
</tr>
<tr>
<td>Wireless Security -- Denial-of-service/Jamming attacks</td>
<td>2 days (weeks 9 and 10)</td>
</tr>
<tr>
<td>Mobile Security -- Malware threats/Intrusion detection</td>
<td>2 days (weeks 10 and 11)</td>
</tr>
<tr>
<td>Mobile Security -- Device compromise</td>
<td>2 days (weeks 11 and 12)</td>
</tr>
<tr>
<td>Mobile Security -- VANET/Aircraft communication security</td>
<td>2 days (weeks 12 and 13)</td>
</tr>
<tr>
<td>Wireless Security -- 5G LTE security</td>
<td>2 days (weeks 13 and 14)</td>
</tr>
<tr>
<td>Final project presentation</td>
<td>4 days (weeks 15 and 16)</td>
</tr>
</tbody>
</table>
Homework

Quizzes and/or paper summaries will be due for each class meeting.

**Undergraduates** will be responsible for quizzes per class meeting.

**Graduate students** will be responsible for a quiz and a full paper summary per paper assigned.
Each student will complete a literature review on an area of wireless or mobile security of their choice.

A tentative list of topics will be provided on the course website. This review will establish the related work for their final project.

**Undergraduate students** should have a minimum of 5 papers in their literature review and **graduate students** should have a minimum of 10 papers.

This might mean needing to identify far more papers that seem to be of interest and carefully pruning to those of greatest interest.
Annotated Bibliography: A complete BibTex library should be submitted, including: PDFs of papers, a complete citation entry for each paper, and a summary for each paper (with the paper content in the Notes section and the critique in the Research Notes section).

Draft Literature Review: A draft of your literature review showing progress on tying the papers together and understanding open research questions.

Final Literature Review: The final draft to be graded for completeness.
Each student will produce a short research proposal on an open research topic in Wireless and/or Mobile Security, and how they would approach an exploration of this topic.
Ideas Presentation: This presentation will allow you to solicit feedback from your coursemates on the topic of your choosing early in the process of your literature review. You will have a time slot to present the idea you have chosen to explore for both the literature review, and later proposal.

A draft of your proposal, incorporating your ideas from your literature review to address an open research question.

Final Proposal: The final draft to be graded for completeness.
Tentative List of Project Topics

Identity-based encryption/attribute-based encryption schemes

Comparison of key distribution schemes for wireless sensor networks – Random vs. deterministic deployment, resource overhead, complexity, security evaluation.

Cellular network security, for example, security in GSM, or 4G/LTE/5G networks.

Mobile device/smart-phone security, e.g., user authentication or continuous authentication (beyond password)

Security in emerging wireless networks/technologies, such as vehicular ad hoc networks, mobile social networks, near-field communications, etc.

Establishment of security associations/device pairing protocols in wireless networks

Jamming/anti-jamming techniques in wireless networks

Location privacy in wireless networks

VANET/Aircraft security

IoT Security
Preferred Conferences and Journals

2014-

Conferences:
- IEEE Symposium on Security and Privacy
- ACM Conference on Computer and Communications Security
- Usenix Security Symposium
- ISOC Network and Distributed System Security Symposium
- European Symposium on Research in Computer Security
- ACM Symposium on Information, Computer and Communications Security
- IEEE Conference on Communications and Network Security
- ACM Conference on Wireless Network Security
- Symposium On Usable Privacy and Security
- IEEE International Conference on Computer Communications
- ACM SIGCOMM Conference
- IEEE International Conference on Communications
- IEEE GLOBECOM
- IEEE Vehicular Technology Conference

Journals
- IEEE Security and Privacy Magazine
- IEEE Transactions on Dependable and Secure Computing
- IEEE Transactions on Information Forensics and Security
- IEEE Transactions on Mobile Computing
How to read a technical paper?
How To Read a Technical Paper

Abstract

What is the application?

What is the problem?

What is the contribution of the authors?
Introduction:

Why is the application important?

What is the problem addressed?

Why is the problem important in the context of the application?

Has anyone in the past attempted to address the problem?

What are the problem with existing solution?

What are the novel contribution by the authors?
How To Read a Technical Paper

Related works:

Details of the existing solutions?

How is the work presented in the paper different from existing solutions?
How To Read a Technical Paper

System models:

What is the exact application of the proposed work?
  Capabilities of the legitimate entities

Threat model:

What are the capabilities of the adversarial entities?

What is the exact attack scenario addresses by the proposed solution?
How To Read a Technical Paper

Proposed solution/protocol:

This is the most important section to understand.

What are the steps of solving the problem.
How To Read a Technical Paper

Security analysis:

Next most important section to understand.

How do the steps presented in the proposed solution solves the problem?

Is security is quantified?

How much security is claimed by the authors.
How To Read a Technical Paper

Experiments and Conclusion

What is the experimental setup?

Does the setup mimics real-world application?

What are the results?

Do authors achieve the claimed level of security?
How To Read a Technical Paper

Can you improve this work:

- Can you add more constraints to the threat model?
- Can you simplify the protocol and still attain same level of security?
- Can you improve the security?