Course Logistics

- **Classroom:** EERC 226
- **Meeting time:** TR 3:35 pm-4:50 pm
- **Office hours:** TR 5:00pm-6:00pm
  Other time by appointment
- **Instructor Office:** EERC 712
- **Email:** cchigan@mtu.edu
- **Phone:** 487-2494
- **Course website:** http://www.ece.mtu.edu/ee/faculty/cchigan/EE5723-Security/index-spring11.html

Course Coverage

- Truly a **Network Security** course
- NOT focus on…
  - Database Security
  - Operating System Security
  - Program Security

Prerequisites

- You should have taken Computer Network class such as EE4272 or EE5722
- Medium-level of Programming (C or C++, Java, ns2, OPNET, etc.) Skill
Textbooks & References

- Required texts -
  - *Network security: PRIVATE communication in a PUBLIC world* by C. Kaufman, et al
  - I will follow it for the fundamental network security topics

- References
  - Fundamentals of Computer Security Technology, by Edward Amoroso, 1994
  - The Practice of Network Security, by Allan Liska, 2003
  - Research Papers on MANET, WSN, Smart Grid, Cloud Computing Security

Course Objectives

- Understanding of fundamental *issues, concepts, principles, and mechanisms* in network security
  - Cryptography, authentication.
  - Key Distribution & Management
  - Well known network security protocols such as IPSec, SSL, WEP

- Advanced topics: Preparation for graduate/senior level research in network security
  - Original research on MANET (including VANET) security
  - Wireless sensor network (WSN) security
  - Cyber-security for critical infrastructures (e.g., Power Infrastructure)
  - Cloud Computing security

Structure of the Course

- Fundamental principles of cryptography & network security *(week 1~10)*
  - I will lecture this part of the material
  - HWs & Midterm exam will be given

- Advanced topics in MANET & WSN security *(week 11~15)*
  - Each student is required to lead a 60-minutes presentation on one advanced topic
  - Followed by a 10-minute discussion led by the instructor (and/or the speaker)
  - The topic list will be given by the instructor on week 3

- Student Project Final In-class Presentation/Demo *(week 15)*

Grading System

- Homework 20%
- Midterm 30%
  - 6:00pm~8:00pm on March 3rd (tentative)
  - Cover the fundamental topics only

- Student Presentation 20%
  - Focus on the advanced topics for MANET, WSN, Smart Grid, or Cloud Computing Security

- Project 30%
  - Phase I (5%): 1 page project proposal
  - Phase II (5%): 2~3 pages mid-term report
  - Phase III (20%): 8~10 pages final report; In-class final presentation (and demo)
Course Outline: Fundamental Topics

- **System View** of Network Security Model
  - Security Threat Model: Identify network vulnerabilities
  - Security Services Model

- **Security Basis: Cryptography**
  - Secret key cryptography
  - Hashes and message digests
  - Public key cryptography
  - Key distribution and management

- **Network Security Applications:**
  - Authentication and security handshakes pitfalls
  - Well known network security protocols such as Kerberos, IPSec, SSL/SET, PGP& PKI, WEP

Course Outline – Advanced Topics

- Mobile Ad Hoc Network (MANET), Wireless Sensor Network (WSN), Smart Grid, or Cloud Computing Security (tentative): presented by students & the instructor

  - Threat Model in MANET & WSN
  - Secure routing in MANET
  - Denial-of-service attacks and countermeasures
  - Energy-aware security mechanisms
  - Distributed certification authority & self-organized key management
  - MAC misbehavior & countermeasures in MANET
  - Countermeasure selfish attacks and trust establishment in MANET
  - Distribution and revocation of cryptographic keys and light-weight security primitives
  - Security bootstrapping & secure neighbor discovery in WSN
  - Secure data aggregation in WSN
  - Location privacy in WSN
  - Cyber-security for Critical Infrastructures (e.g., Power Infrastructure)
  - Cloud Computing Security

Advanced Topic Presentation

- The finalized list of the advanced topics will be provided by the instructor by the end of the 3rd week. The students have to choose their topics by the end of the 6th week. The topic bidding procedure will follow the First Come First Serve rule.

- Each student will be required to give a 60-minute presentation on one advanced research topic in the area of MANET, WSN, Smart Grid, or Cloud Computing security, followed by a 10-minute discussion led by the instructor (and/or the speaker).

- The presentation should follow the style of teaching fellow students on the selected topic as an expert.
  - The presentation should have good balance of the width and depth on the selected topic.
  - Critique the paper(s) by identifying: open research problems; limitations in the papers and explore solutions;
  - Relate the presented work to the big picture and other relevant topics: problem setting, problem assumptions, results, possible extensions
  - Reflect the work on its strength and weakness: assumptions; key ideas & performance data/analysis

- The slides draft is due 1 week before the scheduled presentation. The instructor will provide feedbacks by going through the slides with the speaker 1~2 times before the presentation.

Course Projects

- The course research project can be a design of new secure algorithms/protocols; an analysis/evaluation/implementation of existing secure algorithms, protocols, or systems; identifying new attacks and vulnerabilities in MANET, WSN, Smart Grid, or Cloud Computing security algorithms or protocols.

  - Potential project topics will be distributed and discussed in the 4th week. Students are encouraged to identify the topics based on their own background and interests.

  - With a chosen topic, the students should identify an open problem, formulate a concrete proposal to address the problem, research the related work, propose a new scheme or develop a novel analysis, and obtain results to evaluate their ideas.

  - A 1-page proposal is due on 6th week which describes with a clear statement of the specific problem of your focused topic, and the expected results. A 2~3-page mid-term project progress report is due on week 10, which describes the research topic, prior work relevant to the problem, the methodology to be followed, and preliminary results. A 6~10-page high-quality final report is due on week 15. A final in-class presentation from all project teams will be given in week 15.

  - Often a research project will demand performance evaluation via simulation. You are free to use whatever programming language (C/C++/Java, ns2, OPNET) for your project implementation.

- Each project team is formed up to 1~2 students. The project teams should be formed by the end of 4th week.

- The projects will be graded on the basis of both team success and individual effort.
Programming-based Project Alternative

- DES/IDEA Programming  
  - Due on 6th Week
- Secure Instant Messenger with RSA  
  - Due on 10th Week
- Self-selected Application  
  - Upon the approval of the instructor

Outline

- What is network security?
- Network Attacks & Classifications vs. Security Services
- Security Policy, Mechanism, and Protocols
- System Views of Network Security

Friends and enemies: Alice, Bob, Trudy

- well-known in network security world
- Bob, Alice want to communicate “securely”  
  - Trudy (intruder) may intercept, delete, add messages

First Step to Network Security
Who might Bob, Alice be?
- ... well, real-life Bobs and Alices!
- Web browser/server for electronic transactions (e.g., on-line purchases)
- on-line banking client/server
- DNS servers
- routers exchanging routing table updates

There are bad guys (and girls) out there!
Q: What can a “bad guy” do?
A: a lot!
- eavesdrop: intercept messages
- actively insert messages into connection
- impersonation: can fake (spoof) source address in packet (or any field in packet)
- hijacking: “take over” ongoing connection by removing sender or receiver, inserting himself in place
- denial of service: prevent service from being used by others (e.g., by overloading resources)

Security Threats and Attacks
- A threat is a potential violation of security.
  - Flaws in design, implementation, and operation.
- An attack is any action that violates security.
  - Active adversary.

Attack on Privacy
- Intercept communication attendants’ identity information (Usually refers to IP addresses of communication attendants)

Eavesdropping - Message Interception
(Attack on Confidentiality)
- Unauthorized access to information
- Packet sniffers and wiretappers
- illicit copying of files and programs
**Integrity Attack - Tampering With Messages**
- Stop the flow of the message
- Delay and optionally modify the message
- Release the message again

**Authentication Attack - Fabrication**
- Unauthorized use of other’s identity
- Generate and distribute objects under this identity

**Related Issues**
- Non-repudiation: offer of evidence that a party indeed is the sender or a receiver of certain information
- Access control: Service is only provided to authenticated user

**Attack on Availability**
- Destroy hardware (cutting fiber) or software
- Modify software in a subtle way (alias commands)
- Block packets in transit
- Blatant denial of service (DoS):
  - Crashing the server
  - Overwhelm the server (use up its resource)

**What is network security?**
- **Anonymity**: identity of sender or receiver is hidden.
- **Confidentiality**: protection of communication content privacy.
- **Authentication**: Identity confirmation.
- **Message Integrity**: communication attendants want to ensure message not altered.
- **Non-repudiation**: non-repudiation prevents either sender or receiver from denying a transmitted message.
- **Access and availability**: Services must be accessible and available to eligible users.
Outline

- What is network security?
- Network Attacks & Classifications vs. Security Services
- Security Policy, Mechanism, and Protocols
- System Views of Network Security

Types of Attacks

Active Attacks: Attackers need to gain physical access control of a portion of the communications link and be able to insert and capture transmissions.

Passive Attacks: Attackers merely need to be able to observe transmissions.

Close-knit Attack Family

All attacks can be related and are dangerous!

- Passive attacks
  - sniff for content
  - traffic analysis - who is talking
  - who to impersonate

- Active Attacks
  - re-target
  - jam/cut it
  - capture & modify
  - pretend
  - I need to be Bill

More on Attack Classification

- Classification of attacks depending upon
  - Passive and Active Attacks
  - Security Services
  - Layer in OSI Protocol stack
  - Cost/Damage of Attack
  - Node side and Link side Attacks
Network Security Services

- Confidentiality
- Integrity
- Authentication
- Availability
- Access control
- Non-repudiation
- Anonymity
- ...  

Anonymity:
- Identity of sender is hidden from receiver
- When receiver receives message \( m \), receiver has no clue about the sender of \( m \).

Security Services vs. Attacks

- Different Classes of Attacks vs. Security Services
  
<table>
<thead>
<tr>
<th>Security Service</th>
<th>Class of Attack</th>
<th>Feature of Attack</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrity</td>
<td>Modification/Fabrication</td>
<td>Alter Information for Malicious or Selfish Purposes</td>
</tr>
<tr>
<td>Authentication</td>
<td>Impersonation</td>
<td>Pretend as good node to launch various kinds of attacks</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>Eavesdropping</td>
<td>Eavesdrop on traffic to see confidential information and to find out network topology</td>
</tr>
<tr>
<td>Availability</td>
<td>Denial-of-Service</td>
<td>Exhaust Vandalism, computation, and power resources</td>
</tr>
<tr>
<td>Non-repudiation</td>
<td>Denial of Origin and Denial of Receipt</td>
<td>Source and Destination nodes can keep the origin and recipient of messages in the absence of signatures</td>
</tr>
<tr>
<td>Co-operation Fails</td>
<td>Overuse of Network Resources and not co-operating as Network Function</td>
<td>Use network resources for selfish and malicious purposes</td>
</tr>
</tbody>
</table>

Each attack class can have various implementations across multiple layers.

Security Provisioning Strategy

Since the list of security attacks is endless, security design and provisioning should be security service oriented rather than individual attack countermeasure oriented.

Protecting security services (properties) rather than counter against various security attacks.

Security Services

- Confidentiality: protection of information from being exposed to unintended entities
  - Information content.
  - Parties involved.
  - Where they are, how they communicate, how often, etc.
Security Services - Cont’d

- **Authentication**: assurance that an entity of concern or the origin of a communication is authentic - it’s what it claims to be or from

- **Integrity**: assurance that the information has not been tampered with

- **Non-repudiation**: offer of evidence that a party indeed is the sender or a receiver of certain information

Security Services - Cont’d

- **Access control**: facilities to determine and enforce who is allowed access to what resources, hosts, software, network connections

- **Monitor & response (Intrusion Detection/Tolerant)**: facilities for monitoring security attacks, generating indications, surviving (tolerating) and recovering from attacks

Security Services - Cont’d

- **Security management** *(system level)*: facilities for coordinating users’ service requirements and mechanism implementations throughout the enterprise network and across the Internet
  - Trust model
  - Trust communication protocol
  - Trust management infrastructure

Outline

- What is network security?

- Network Attacks & Classifications vs. Security Services

- Security Policy, Mechanism, and Protocols

- System Views of Network Security
Security Policy, Mechanism & Protocol

- **Policy**: a statement of what is, and is not allowed.
  - Application related!
- **Mechanism**: a procedure, tool, or method of enforcing a policy
- **Security mechanisms**: implement functions that help prevent, detect, and respond to recover from security attacks.
  - Security functions are typically made available to users as a set of security services through APIs or integrated interfaces.
  - Cryptography underlies many security mechanisms.
- **Security protocols**: A set of security policies and related mechanisms

Outline

- What is network security?
- Network Attacks & Classifications vs. Security Services
- Security Policy, Mechanism, and Protocols
- System Views of Network Security

Systematic View of Network Sec: Security Model

- **Definition**: A framework wherein the security policies are developed
- **Various Security Models**
    - Applicable to various companies w/ various network infrastructures
  - CISCO SAFE - specifically defined for VPN & Internet: www.cisco.com/go/safe
    - http://www.niap-ccEvS.org/cc-scheme/
  - OCTAVE - hybrid of ISO15048 & RFC2196: www.cert.org/octave/
    - (Operationally Critical Threat, Asset, and Vulnerability Evaluation)
- Build asset-based threat profiles
- Identify Infrastructure vulnerabilities
- Develop security strategy & plans

The Security Life-Cycle

- **Security Model**
  - Policy
  - Threats
  - Specification
- **Design**
- **Implementation**
- Operation and Maintenance