ECE 547/647: Security Engineering

Lesson 1: Introduction to Security Engineering

- Syllabus
- Some examples

Syllabus

Course Format

- Course is only May 18 – June 26 so twice the pace of a regular course
- 4 lectures per week
- Reading for each lecture
- Assignments: about 2 per week

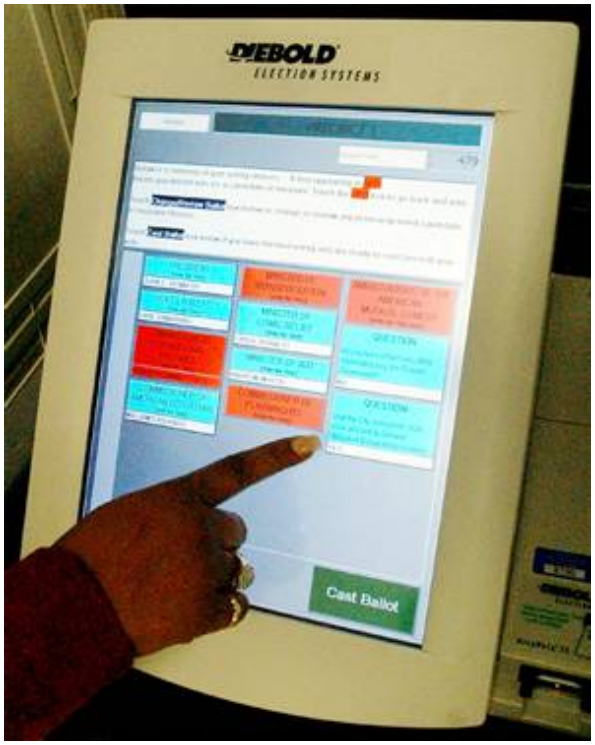
- Projects and Presentations later in the course
- Plan on 20 hours/week for this course

547/647 on-line vs. 371

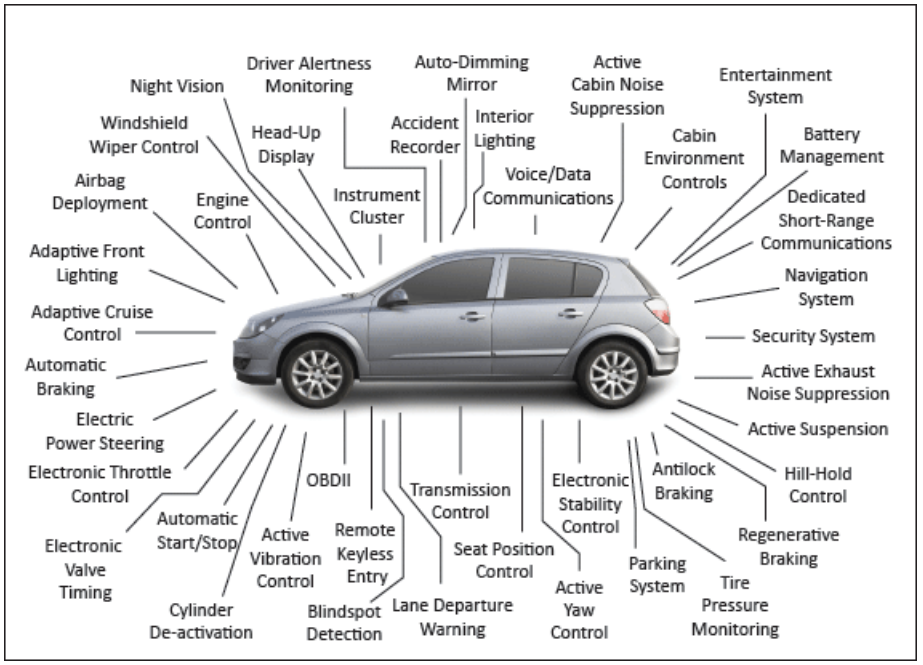
- Graduate level
- Research Papers
  - Analysis/Critique
  - Reproduction of results
  - Extensions
- More advanced math, both crypto and statistics
- Groups of 4 = 2+2
  - Individual responsibility/ contribution

- History and Terminology
- Fundamental mathematics
- Multi-disciplinarity
- Concepts and capabilities
- Simple models, implementations and experiments in groups of 2.
- Quizzes, in-class discussions
- Trends and hot topics

Examples of Secure Systems



Voting Machine



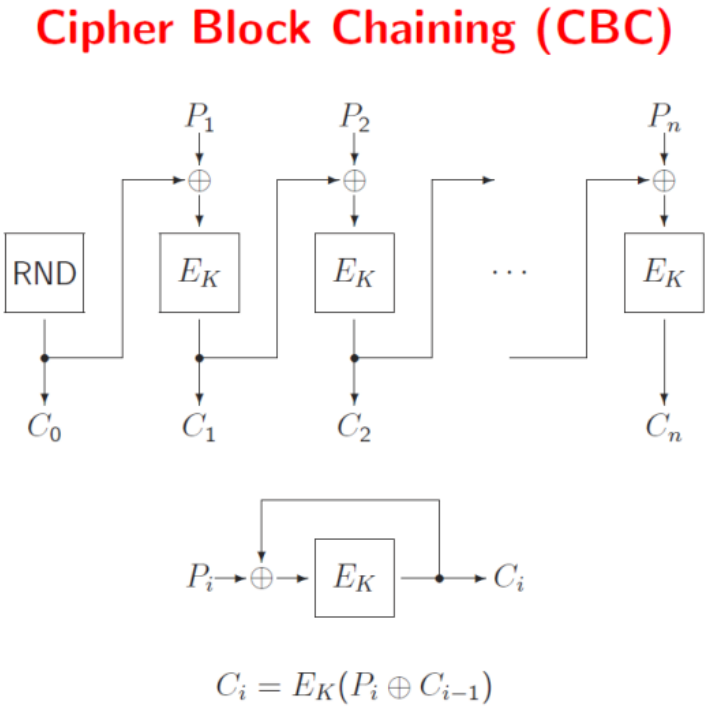
Modern automobile

Examples of Secure Systems (cont)

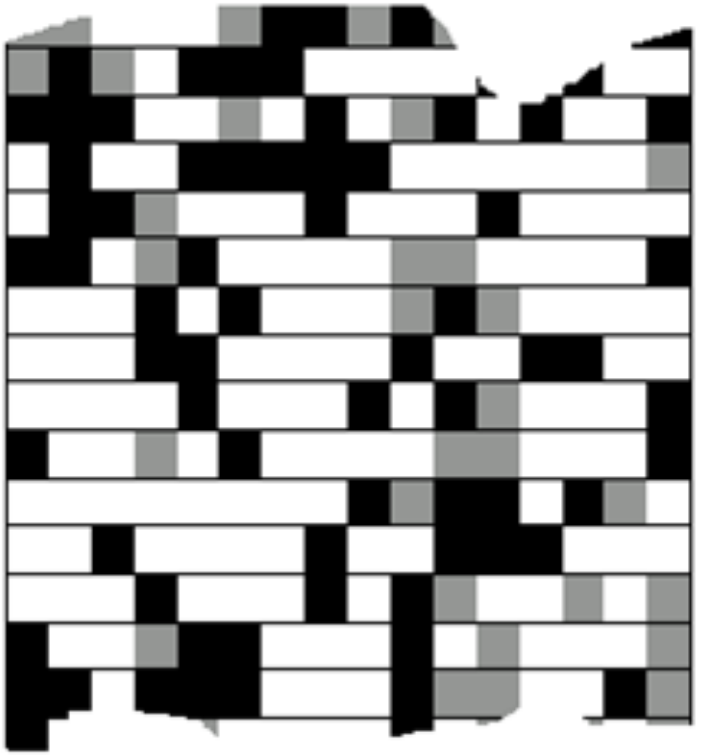
Transportation Payment System

Medical Devices

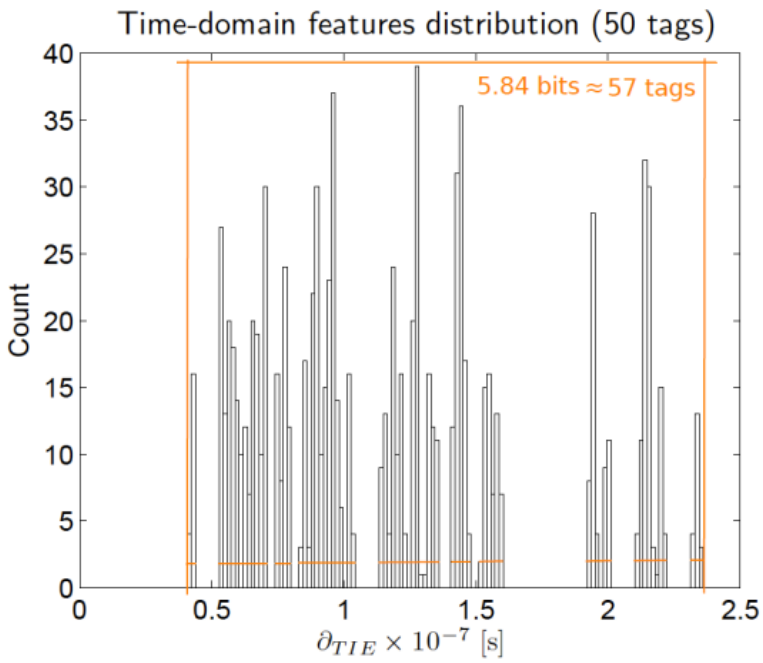
Representations of Secure Systems



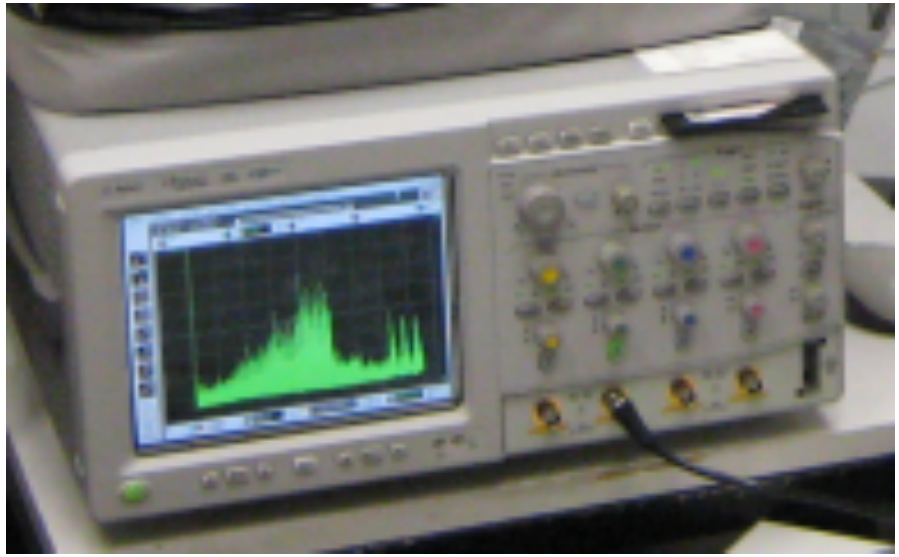
Algorithms



Information and Statistics



Data representations



Measurements

Rationale

- Introduce topics of security engineering
  - Trends
  - Threats
  - Vulnerabilities
- Review the influence of attacks in development of security engineering

Course Objectives

- Examine the foundations, challenges, and trends in security engineering
- Apply guidelines for secure system design
- Distinguish between recent vulnerabilities and defenses in security engineering
- Classify examples of hardware security issues (EE)
- Identify the importance of non-technical issues within the field of security engineering
- Discover futuristic applications of security engineering principles

Outline of Course

- Part 1
  - Introduction and Objectives
  - Motivations
  - Foundations of Security
  - Case Study: Automotive Security
- Part 2
  - Human Behavior
  - Software Security
  - Case Study: Voting Systems
  - Case Study: Smart Grids
- Part 3
  - Ciphers and Cryptanalysis
  - Case Study: Keeloq – A Practical Attack
  - Case Study: Implantable Medical Devices.
- Part 4
  - Hardware Security
  - Silicon and Physical Layer RFID and TRNG
  - Applications: Bio-sensing and Nano-Payments
- Part 5
  - Side-channel and countermeasures
  - Case Study: AES chip
  - Hot Topics
  - Security Economics and Regulations
  - Where to Learn More

Definition of System Security

"The science of managing malicious intent and behavior that involves information and communication technology."

Security vs. safety engineering: focus on **intentional** rather than **accidental** behavior, presence of **intelligent adversary**.

Definition of System Security (cont'd)

- Malicious behavior can include:
  - Fraud/theft – unauthorized access to money, goods or services
  - Vandalism – causing damage for personal reasons
  - Terrorism – causing damage, disruption and fear to intimidate
  - Warfare – damaging military assets to overthrow a government
  - Espionage – stealing information to gain competitive advantage
  - Sabotage – causing damage to gain competitive advantage
  - "Spam" – unsolicited marketing wasting time/resources
  - Illegal content – illicit and/or extremist materials

Trends in System Security

- Applications
  - Digital wallet (banking, payments, medical, voting, access)
  - Business models based on security/privacy (DRM, social networking, games)
  - Data-centric computing (images, audio, video, graphics, 3D,…)
- Platforms
  - Mobile clients decreasing cost, size, power
  - Demand for increased reliability and usability
  - Constant software updates
  - Virtualization
  - Ubiquitous connectivity to cloud

Trends in System Security (cont'd)

- Hardware
  - Multi-core, heterogeneous, accelerators, configurable
  - More on-chip cache
  - More off-chip memory, increasingly non-volatile
  - Removable storage (USB, etc.)
  - Increasing Wireless Connectivity (WiFi, Cell, GPS, BT, NFC,…)
- Threats
  - Increasing global cyber-crime at all levels
  - "Attackers" include: Nation-state, terror, organized crime, petty crime, hackers, user!
  - Increasing privacy concerns for private citizens and companies

How are Systems Hacked?

- **Hack attack:** low-cost remote software attack
  - User often inadvertently approves the installation of the software that then executes the attack
    - Examples: viruses and malware downloaded to the device via a physical or a wireless connection

- **Shack attack:** low-cost hardware attack
  - Attacker uses equipment from retail electronics store with designs and components found on the Internet.
    - Example: electronic IED
  - Attackers have physical access to the device, but not enough equipment or expertise to attack within the integrated circuit packages

(ARM Limited, 2009)

How are Systems Hacked? (cont'd)

- **Lab attack:** the most comprehensive and invasive
  - Attacker can use laboratory equipment to perform reverse engineering of sensitive device parts
    - Example: Attach microscopic logic probes to silicon metal layers, and glitch a running circuit using lasers
    - Example: Monitor analog signals, such as device power usage and electromagnetic emissions, to perform cryptographic key analysis

- Rule of thumb: Every device can be broken
  - You do not defend against attack directly, but limit the damage caused

(ARM Limited, 2009)

The Rise and Risk of Embedded Devices

- **Definition:** Highly specialized device meant for specific purpose(s), usually embedded within another object or as part of a larger system
  - Example: Heart rate monitor embedded in wristwatch that connects to smartphone

- **Forecast:** 50 billion embedded devices in use by 2020
  - Connected to all aspects of life, from critical infrastructure to daily activities

- **Warning:** Embedded devices have now become the targets of criminals
  - Example: The Stuxnet worm attack in Iranian locked-down nuclear enrichment site

Group Discussion and Report Back: How to Talk about Security?

The subject of security engineering covers both problems and solutions, but that information is not always used by those with good intentions.

"In previous centuries, people objected to the publication of books on locksmithing, on the grounds that they were likely to help the bad guys more than the good guys."

- Should the topic of security "tricks" be taught without restriction? Why or why not?

What is Security Engineering?

- Optional textbook:

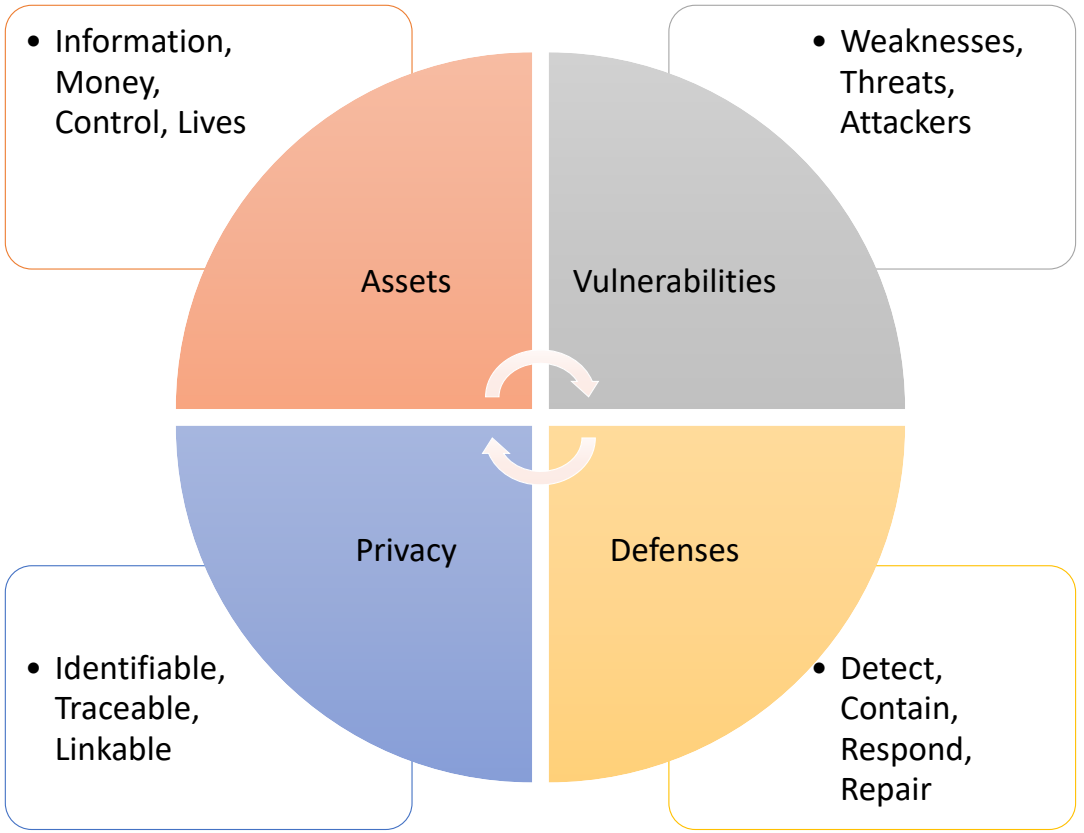
  Anderson, R. (2019). *Security engineering: A guide to building dependable distributed systems* (3rd edition). Wiley Publishing, Inc.

  Available free online!

"Security is not just about keeping the bad guys out, but increasingly concerned with tussles for power and control."

What is a Secure System?

- Assets (Information, Money, Control, Lives,…)
- Vulnerabilities (Weaknesses, Threats, Attackers)
- Defenses (Detect, Contain, Respond, Repair)
- Privacy (Identifiable, Traceable, Linkable,…)



Secure System Example: AV Box

- Assets
- Vulnerabilities
- Defenses
- Privacy

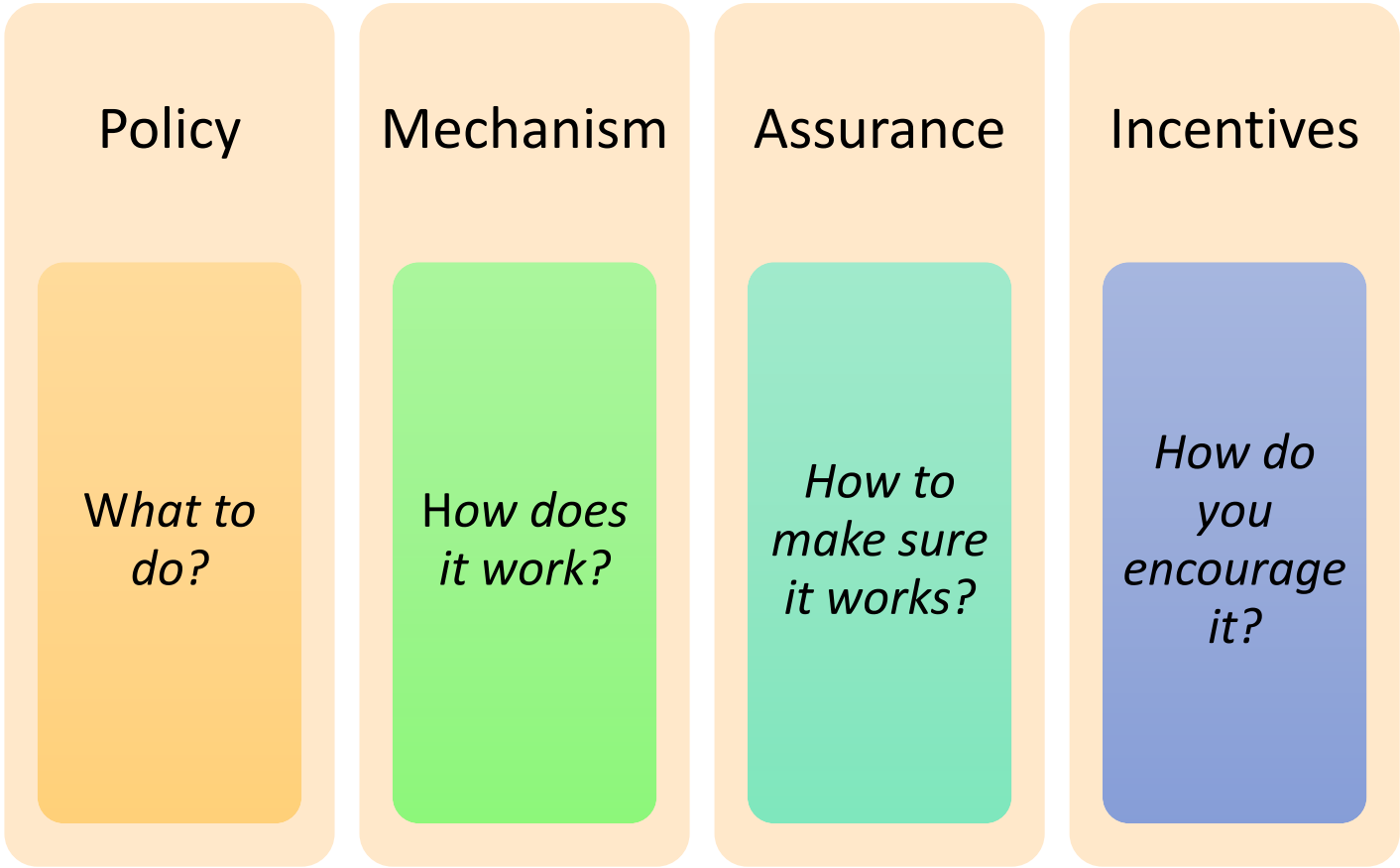
Activity: Additional Secure System Examples

- Bank
- Military base
- Hospital
- Home
- Public transit station

For each, think about 1) Assets, 2) Vulnerabilities, 3) Defenses, 4) Privacy issues

A Defense Framework

- Examples:
  - Post-9/11 Airport Security
  - Olympics 2018



Why is Information Security Hard?

- Common view:
  - Security is a difficult technical issue
  - Cryptography, tamper-proofing, law enforcement

- But other factors also make things difficult
  - Business disincentives
  - Human behavior

Security Economics

- **Remember: With enough resources, every device can be broken**

- Need to consider economics of attack and defense

Security Economics (cont'd)

- What is the **cost** of defense in terms of implementation and loss of utility?

- What is the **value** of stored assets?
  - Application-specific (payment, appliance, DRM, medical, automotive, etc.)
  - What data is being sought?
  - What is the value of the data ($$, privacy)
  - Can the data be used for further attack (e.g. keys, passwords, CC #s)
  - Other objectives besides data (e.g. control, DOS, cloning)

Security Economics (cont'd)

- Therefore, limit the damage when a device is broken and therefore make the lab attack **uneconomical**.
  - Use of *per-device unique secrets* is one example where reverse engineering a single device provides the attacker with no useful information

Incentives in Security Economics

- Who has primary responsibility when bank fraud occurs?
  - In US: the bank
  - In UK: the customer

- Guess who has the more effective security system?

Plan for Lesson 2

- Before next class, read:
- **Self-encrypting deception: weaknesses in the encryption of solid state drives (paper on Moodle)**