Course Overview

Anupam Datta

CMU
Fall 2007-08
Plan for Today

- Course logistics
- Overview of topics
- Basic cryptographic primitives
Course Staff

- Instructor: Anupam Datta
  - Office: CIC 2118
  - Email: danupam@cmu.edu
  - Office hours: Tue, Th 4:30-5:30PM

- TA: Joseph Slember
  - Office: CIC 2225B
  - Email: jslember@ece.cmu.edu
  - Office hours: Mon, Wed 2-3PM
Logistics

- Location: BH A51
- Days: Tuesday & Thursday
- Time: 10:30-11:50AM

- Web page: http://www.ece.cmu.edu/~ece739/
- Course blackboard (linked from web page)
- Course work:
  - Homework (20%), scribing (20%), class participation (10%), course project (50%)
Logistics

☐ Course Project:
  - Teams of 2-3 (form team by end of week)
  - 2 presentations (proposal, final)
  - Written report
  - Project suggestions online (or pick your own)

☐ Reading:
  - No textbook for the course
  - Research papers on which lectures are based

☐ Lab Space:
  - Use Linux machines in HH 1107 cluster for homework and projects
Logistics

- Section:
  - Friday: 2-4PM
  - CIC Room 1301
- First few weeks of the course
- TA (s) will discuss and demo various security analysis tools
- Should be useful for projects
- First section this Friday
Prerequisites

- An introductory course in computer security such as 18-487 or 18-730 is recommended, but not required.
- Some background in logic, programming languages, verification is recommended, but not required.
- Quick class poll
10,000-foot View

SO WE’LL CALL THIS API, THEN—WAIT WAIT WAIT. THIS IS TOO LOW-LEVEL.

I NEED CONTEXT. THE 10,000-FOOT VIEW.

OK.

SO WE HAVE TWO APPLICATIONS THAT—NO. NO. PULL WAY BACK. THE REALLY HIGH-LEVEL VIEW.

IT ALL BEGAN FOUR BILLION YEARS AGO ON A PLANET CALLED “EARTH.” OK, THAT’S HIGH ENOUGH.
Four broad topics

1. Security Protocols
2. Distributed Access Control
3. Privacy
4. Language-based Security
Web Purchase
Secure communication using SSL/TLS

SSL uses cryptography:

• Public and symmetric key encryption, digital signatures, hash functions, message authentication codes

Provides

• Secrecy
• Authentication
• Data integrity
**802.11i Wireless Authentication**

- **Supplicant**
  - UnAuth/UnAssoc
  - 802.1X Blocked
  - No Key

- **802.11 Association**
  - EAP/802.1X/RADIUS Authentication
    - 4-Way Handshake
    - Group Key Handshake
    - Data Communication

- **MSK**
  - Widely used in wireless LANs

- **Supplicant**
  - Auth/Assoc
  - 802.1X UnBlocked
  - PTK/GTK

- Will discuss a number of industrial protocols
The Problem: Is a given network protocol secure?

First define:
- Model of protocol
- Model of attacker
- Security properties
  - Secrecy, confidentiality
  - Authentication, integrity
  - Denial of service
Methods

- Bug finding
  - Automated model-checking techniques
  - Finite number of sessions

- Security proofs
  - Absence of bugs
  - Unbounded number of sessions
  - Many approaches
    - Will cover: Paulson’s Inductive Method, Protocol Logics, Process Calculi
Modeling Cryptography

- **Symbolic Model**
  - “Perfect crypto”: No attacker can break, e.g. can decrypt encrypted message iff has decryption key
  - Proof technique: Induction

- **Complexity-theoretic Model**
  - Primitives secure with high probability against probabilistic polynomial time attackers
  - Proof technique: Reduction

- Will cover recent work combining methods
Modular Analysis

- Goal: Prove security properties of complex protocols by combining proofs of their components

- Will cover:
  - Composition theorems of PCL
  - IEEE 802.11i case study
Attacks on Industry Standards

- **IKE** [Meadows; 1999]
  - Reflection attack; fix adopted by IETF WG
- **IEEE 802.11i** [He, Mitchell; 2004]
  - DoS attack; fix adopted by IEEE WG
- **GDOI** [Meadows, Pavlovic; 2004]
  - Composition attack; fix adopted by IETF WG
- **Kerberos V5** [Scedrov et al; 2005]
  - Identity misbinding attack; fix adopted by IETF WG; Windows update released by Microsoft

Identified using logical methods
Four broad topics

1. Security Protocols
2. Distributed Access Control
3. Privacy
4. Language-based Security
Distributed Authorization

Goal:
Flexible and scalable access control in large-scale, open, distributed, decentralized systems
Example: Grey

I authorize access.

-Mike

Mike’s Office, D208

Slide: Bauer & Reiter
Example: Grey

I want access.
-Scott

I allow Scott to enter.
-Mike

Demonstrate that Mike authorizes access

Jon

Mike

Kevin

Jason

Scott

Mike’s Office, D208

Slide: Bauer & Reiter
Example: Grey

Mike's Office, D208

I want access.
-Scott

I delegate to Jason.
-Mike

I allow Scott to enter.
-Jason

Demonstrate that Mike authorizes access.
StateU is a university
Alice is a student
Grants access to university students
Trusts universities to certify students
Trusts ABU to certify universities
Characteristics of Distributed Authorization

- No central administration, each service makes its own decision
- No relationship between a service and a user prior to a request
  - knowing a user’s name may not help
  - must rely on information from third-party to make authorization decision (delegation)
- Authorization information is distributed
- Communication channels may be insecure
We will cover

- Access control logics
  - Lampson et al “speaks-for” logic
  - Proof Carrying Authorization and the Grey System
  - Constructive Authorization Logic
- Trust Management
  - SPKI/SDSI
  - RT
Four broad topics

1. Security Protocols
2. Distributed Access Control
3. Privacy
4. Language-based Security
Privacy

- An increasingly important concern for individuals and enterprises
Privacy

- **Scenarios:**
  - Enterprises collect personal information – email and postal addresses – in many cases through web sites
  - Organizations such as hospitals and financial institutions hold sensitive personal information

- **Fundamental questions:**
  - Policy: Under what conditions is the collected information used and distributed?
  - Enforcement: Do organizational processes actually enforce the stated policy?

- **Privacy Laws:**
  - HIPAA, GLBA, COPPA
Privacy Policy Languages

- P3P
  - Privacy policy specification for web sites.
- E-P3P/EPAL
  - Enterprise privacy policy specification and enforcement
- Contextual Integrity and LPU
  - Philosophical theory of privacy
  - Formalization in temporal logic (specification and enforcement)
  - Expressing privacy laws, e.g. HIPAA, GLBA, COPPA

Similarities with and differences from access control
Four broad topics

1. Security Protocols
2. Distributed Access Control
3. Privacy
4. Language-based Security
Type Systems for Security

- Focus on the use of type systems to improve software security
- Two representative projects
  - Jif: Enforcing information flow security properties (*non-interference* and variants)
  - Cyclone: Memory safe dialect of C, i.e. no buffer overflow attacks, format string vulnerabilities etc (or Ccured)
What is a type system?

“Now! *That* should clear up a few things around here!”
From “what” to “why”?
Why study foundations of security?

Our discipline of computer science seems to be one in which theory and practice are more intimately related than in any other field.....you can’t get very far in practical work without abstract theories that permit you to think at a higher level, and at the same time theoretical work becomes dead if it doesn’t receive fresh inspiration from practical problems in the “real world”.

D. E. Knuth
A Cautionary Word

☐ This is a theory heavy course!
☐ Litmus test on attitude toward theory

"You're not allowed to use the sprinkler system to keep your audience awake."
The End

Let’s get started…