CIS-5374
Information Security and Privacy

Class 1

Bogdan Carbunar
Outline

- Administrative Issues
- Rules of the Class
- Textbooks
- Is This Class for Me?
- Security and Privacy Overview
Administrative Issues

- **Staff**
  - Bogdan Carbunar, assistant professor

- **Communications**
  - E-mail: carbunar@gmail.com

- **Office Hours**
  - Bogdan: after class, ECS 383

- **What about you?**
Class Grading (subject to changes)

- **1 midterm** worth: 30%
  - Date of exam: December 6, 2017
  - 12-2pm, GL 139
- **Paper presentation**: 30%
- **Homework**: 20%
- **Class participation**: 20%
Class Grading: Details

- Homework
  - 2-3 homeworks
  - Around 2 weeks for each homework
  - Not intended for grade (that much), but for your training
Class Grading: Details (cont’d)

- **Class participation**: 20%
  - Class presence does not mean participation
  - But it is encouraged
  - Participation means *asking* and *answering* questions

- **Student paper presentations**: 30%
  - Papers posted on class web page
  - Let me know in time (FIFO assignment rule)
Outline

- Administrative Issues
- Rules of the Class
- Textbooks
- Is This Class for Me
- Security and Privacy Overview
Textbooks

- *Applied Cryptography – 2nd edition*
  Bruce Schneier
  Available online 😊
- You don’t need to buy it!
- Papers assigned for reading
  - See class webpage
Outline

- Administrative Issues
- Rules of the Class
- Textbooks
- Is This Class for Me
- Security and Privacy Overview
Is This Class for Me?

1. If (You Did Not Take CIS 5370 or CIS 5372 Before This Semester)
   - Then Drop this course now

2. Else If (You Did Not Get at Least a B in CIS 5372)
   - Then Drop this course now

3. Else
   - You can take this course

Caveat: If (You Do Not Understand this Pseudocode)
   Then Drop this course now
Outline

- Administrative Issues
- Rules of the Class
- Textbooks
- Is This Class for Me
- Security and Privacy Overview
Information Security

- Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction. [Source: wikipedia]
Security is about

- Honest user (e.g., Alice, Bob, ...)
- Dishonest Attacker
- How the Attacker
  - Disrupts honest user’s use of the system (Integrity, Availability)
  - Learns information intended for Alice only (Confidentiality)
Information Security

- Goals: Protect
  - Confidentiality
  - Integrity
  - Availability
- May conflict!
Confidentiality

- Information about system or its users cannot be learned by an attacker
- Data Confidentiality:
  - Private or confidential information is not revealed to unauthorized individuals
- Intersects with Privacy
Integrity

- The system continues to operate properly, only reaching states that would occur if there was no attacker

- Data Integrity
  - Information and programs are changed only in specified and authorized manner
Availability

- Actions by an attacker do not prevent users from having access to use of the system
  - Enable access to data and resources
  - Timely response
  - *Fair* resource allocation
- Conflicts with Confidentiality
Examples

- Confidentiality
  - Student grades
  - Available only to student, parents, employer

- Integrity
  - Patient information e.g., allergies
  - Can lead to loss of human life

- Availability
  - Authentication service
  - Can lead to financial loss
Privacy

- Ability of an individual or group to seclude themselves or information about themselves and thereby reveal themselves selectively [Source: wikipedia]

- Related to anonymity
  - The wish to remain unnoticed or unidentified in the public realm

- Partially intersects security
  - Information protection
Controlled Disclosure

- Right to control
  - Who has access
  - To what information

- Example: who has access to your phone number?

- Caveat
  - Once you give out information
  - You cannot control how it propagates
What is Private?

- Identity, ownership of private data
- Finances: credit, bank details
- Legal matters
- Medical conditions, drug use, DNA,
- Voting, opinions
- Preferences: religion, orientation, etc
- Biometrics: fingerprint, retina
- Performance: school records, employment ratings
- Location: travel data
What is Private? (cont’d)

- Communications: mail, e-mail, phone
- Sites you accessed
- News you read
- Things you buy
- Criminal record
- Depends on who you are
I Don’t Have Anything to Hide!

- Think again!
  - sexual, political, religious orientation
  - pregnancy
  - illnesses
  - genetic predisposition
  - sins of youth
  - controversial activities
  - personal interests
  - ...
Privacy Covered

- Zero Knowledge Proofs
- Private Information Retrieval
- Digital Payments
- Anonymizers
- Building Blocks
Zero Knowledge Proofs

- How to prove you know a secret
- Without revealing it
- Example: Story by Quisquater et al.


- See also wikipedia
Zero Knowledge Proofs

- Peggy has uncovered the secret word used to open a magic door in a cave.

- Victor says he'll pay her for the secret, but not until he's sure that she really knows it.

- Peggy needs to prove that she knows the word without telling it to Victor.
Zero Knowledge Proofs (cont’d)

- Label the left and right paths from the entrance A and B

- Victor waits outside the cave as Peggy goes in
- Peggy randomly takes either path A or B
Zero Knowledge Proofs (cont’d)

- Victor enters the cave and shouts the name of the path he wants her to use to return
  - Chose at random, A or B
Zero Knowledge Proofs (cont’d)

- If Peggy was on side A, she simply returns
- If Peggy was on side B, she opens the door and comes through A
Zero Knowledge Proofs (cont’d)

- What if Peggy was lying?
- If she is on side B (50% chance) she will be caught

Can we improve on this assurance?
- Yes! Repeat procedure 100 times
Privacy Covered

- Zero Knowledge Proofs
- Private Information Retrieval
- Digital Payments
- Anonymizers
- Building Blocks
Private Information Retrieval

Alice

Bob

Access one item

Privately! Why?

Local database
Privacy Covered

- Zero Knowledge Proofs
- Private Information Retrieval
- Digital Payments
- Anonymizers
- Building Blocks
Digital Payments

- Money exists in physical form
  - Difficult to carry
  - Can be stolen
  - Hard to trace
- Credit cards and checks
  - Easy to carry
  - Harder to steal the money
  - Easy to trace
- Best of both worlds? Yes, we can!
  - E-cash
E-Cash

- Money exchanged only electronically
  - Nothing to carry
  - Hard to steal
  - Hard to trace

Prevent double spending!

Spend $10 token

Alice
"the dealer"

Bob
"the payer"

Carol
Privacy Covered

- Zero Knowledge Proofs
- Private Information Retrieval
- Digital Payments
- Anonymizers
- Building Blocks
Anonymizers

- Anonymizer or mixnets:
  - Tool for making internet activity *untraceable*

- Proxy server
  - Intermediary between a client and the Internet
  - Accesses the Internet on the user's behalf
  - Hide the client’s identifying information
Anonymizers: Why?

- Prevent identity theft
- Protect search histories from public disclosure
- *Get objective information*
  - Avoid target marketing on Internet
  - See BBC, CNN, YouTube, Google
Anonymizers: Why? (cont’d)

- Bypass censorship
  - Not prevent persecution for access to anonymizer
  - Anonymizer = Government trap?
- Avoid government tracking
- Engage in criminal, disruptive, or socially unacceptable behavior
Privacy Covered

- Zero Knowledge Proofs
- Private Information Retrieval
- Digital Payments
- Anonymizers
- Building Blocks
Building Blocks

- Secret Splitting
- Secret Sharing
- Timestamping Protocols
- Subliminal Channel
- Bit Commitment
- Fair Coin Flips
- Mental Poker
- ...

...