ENEE 457: Computer Systems Security
8/29/16

Lecture 1
Introduction and Attacks from the Real World

Charalampos (Babis) Papamanthou

Department of Electrical and Computer Engineering
University of Maryland, College Park

Organization

- Class webpage
  - http://enee457.github.io
  - Two lectures per week, MW 11am – 12.15 pm
  - EGR 1104
  - Attendance will be graded
- Professor
  - Charalampos (Babis) Papamanthou (cpap@umd.edu)
  - Office hours: Mon 3pm-4pm, AVW 3409
  - www.ece.umd.edu/~cpap
- TA
  - Evripidis Parakevas (evripar@umd.edu)
  - Office hours: Wed 5pm-6pm and Thu 4pm-5pm, AVW 1145
  - VERY IMPORTANT: GO TO THE TA SYSTEMATICALLY

Grading

- Final grade
  - 5 homeworks (20%)
  - 5 programming assignments (30%)
  - Midterm (20%): Wed Oct 19 in class
  - Final (25%): Fri Dec 16 in class (from 8am to 10am)
  - Class attendance (5%): At least two questions throughout the semester (I will remember!)
- Lectures will be published on the webpage after class
- Homeworks and programming assignments will be published on the class webpage, but should be submitted through Canvas
- No late homework submissions will be accepted
- Discussions will be managed at Canvas

Grading

- Final grade
  - >90% A-,A,A+
  - >80% B-,B,B+
  - >70% C-,C,C+
  - >60% D-,D,D+
- Do not assume that there will be a curve

Extra credit up 10% (research project): Fair cloud storage with Bitcoin

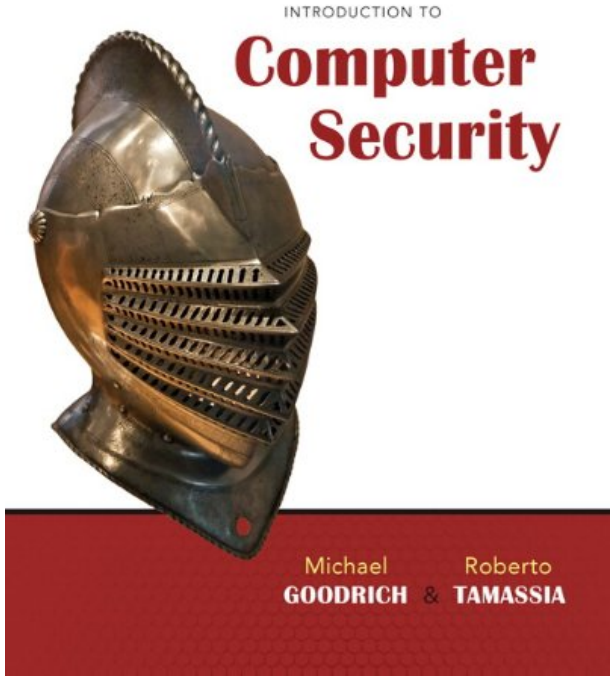
- You will work on a project related to Bitcoin
- Bitcoin is a currency that is completely decentralized and automated
  - 1 BC = $570 (27 Aug)
  - Main novelty: Money can move around when a condition (expressed as a program) is satisfied
  - You can write this program, easily entering into a monetary agreement with someone
- Your research project: Fair Cloud Storage
  - Google drive asks you to pay for more than 15 GB of storage
  - When you pay, do you get any guarantees about your bits? No!
  - Develop a protocol between Google Drive and yourself such that
    - You will be paying in Bitcoins at the end of every month only if Google Drive can prove to you that all files are stored intact
    - In particular you need to post a Bitcoin transaction that will execute only if Google posts the files
    - Email me if interested

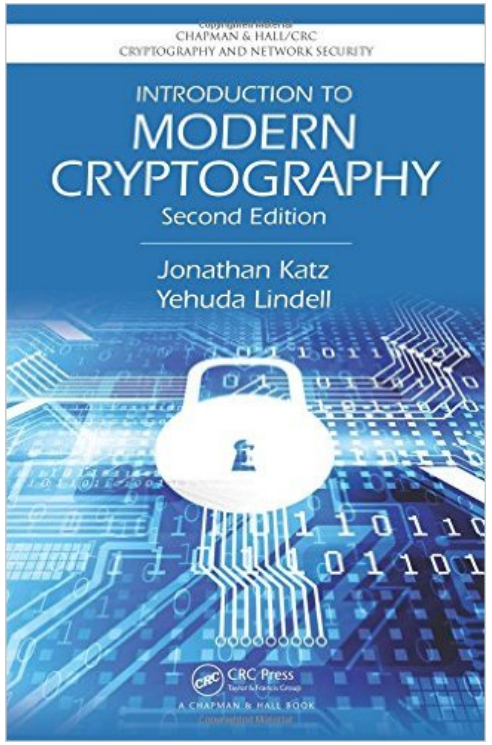
Prerequisites, CS classes and programming

- ENEE150 or CMSC132
- IMPORTANT: If you have taken CMSC414 in the past, I STRONGLY RECOMMEND AGAINST TAKING THIS CLASS
- MORE IMPORTANT: If you are currently taking CMSC414, please drop one of either CMSC414 or ENEE457
- The course will have a significant programming component
- Sample programming projects (FUN, FUN, FUN):
  - Writing code to break an encryption algorithm that I am going to give you
  - Writing code to log into a server (without credentials) which will be running a buggy version of Linux
  - Inspecting buggy code that I will give you and try to exploit its vulnerabilities
  - Writing code to crack passwords
- Knowledge of algorithms and data structures is desirable

Readings

- Most of the class will be based on the following textbooks (GT) and (KL):

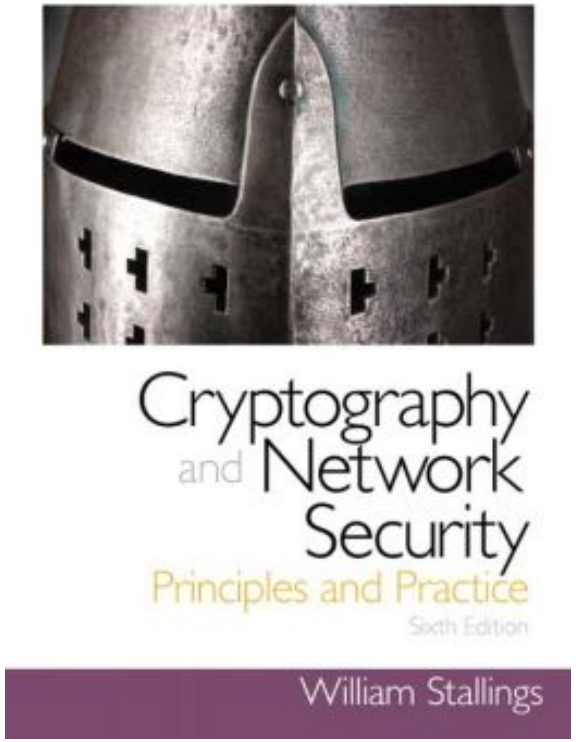


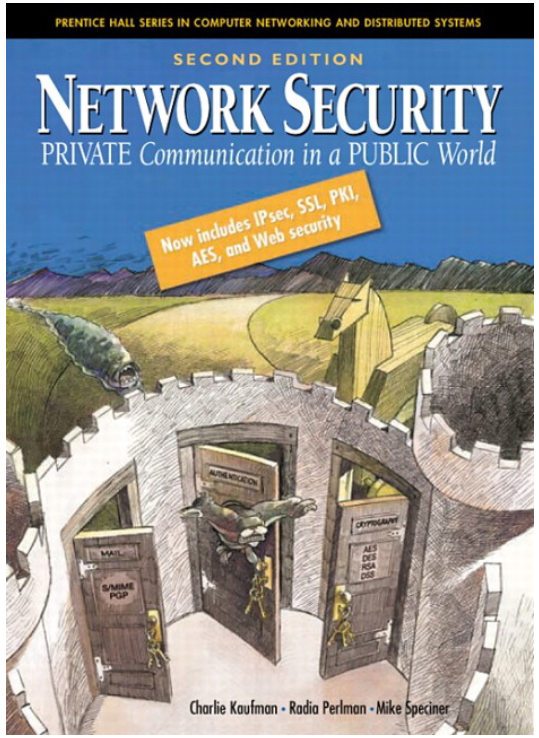


- We are going to be using the board too, so it is advisable you keep notes as well
- The library has copies of the book

Other readings

- Other recommended readings are (WS) and (KPC)





General subjects that will be covered

- Attacks from the real world
- Main principles when designing secure systems
- Fundamentals of computer security
  - Confidentiality (**highlights**: semantic security and AES algorithm)
  - Integrity (**highlights**: digital signatures and number theory)
  - Authentication (**highlights**: password cracking)
  - Access control (**highlights:** information flow control and SETUID programs)
- Practical computer security
  - Web security (**highlights:** Cross-site scripting attacks)
  - Cloud security (**highlights:** Securing your bits at Amazon and how to add numbers you never get to see)
  - Network security (**highlights:** TCP-IP and syn-flooding attacks, Bitcoin)
  - Systems and software security (**highlights:** buffer overflow attacks)

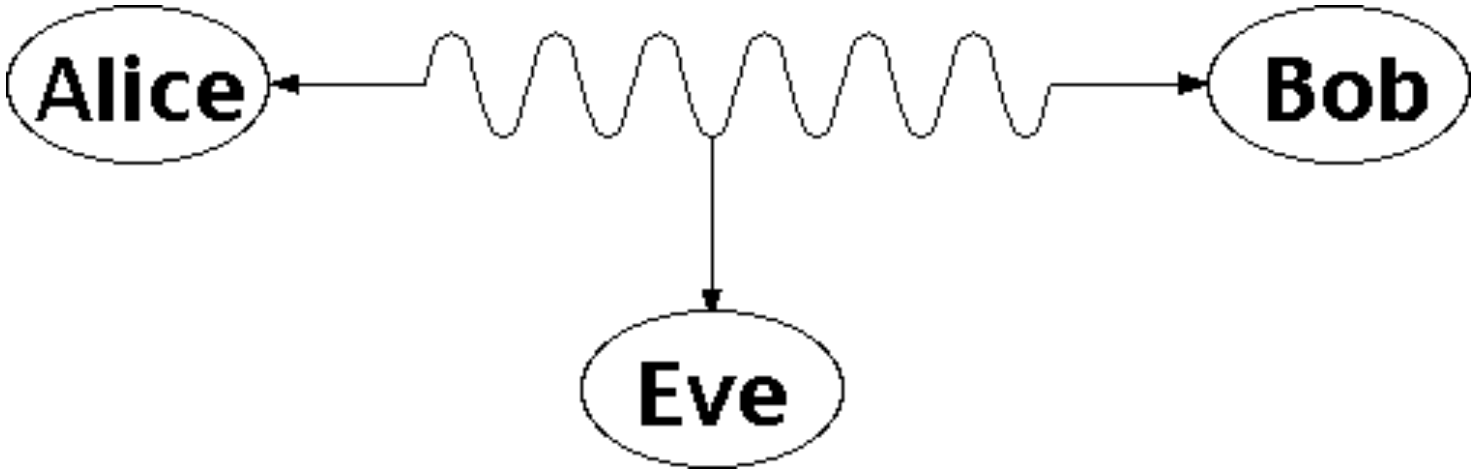
What is Computer Security?

- Computer Security is the prevention of, or protection against
    - access to information by unauthorized recipients
    - intentional but unauthorized destruction or alteration of that information

    - Definition from: Dictionary of Computing, Fourth Ed. (Oxford: Oxford University Press, 1996).

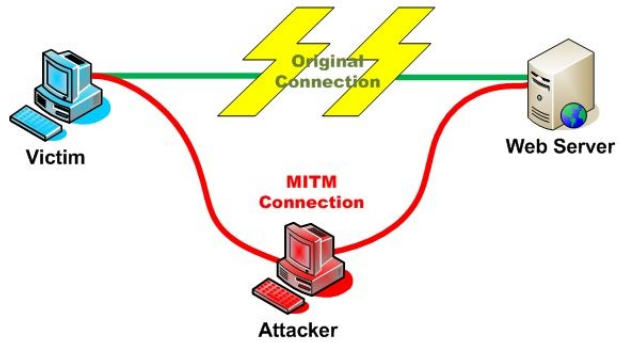
Threat #1: Eavesdropping of information

- The interception of information intended for someone else during its transmission over a communication channel
  - DEFENSE?



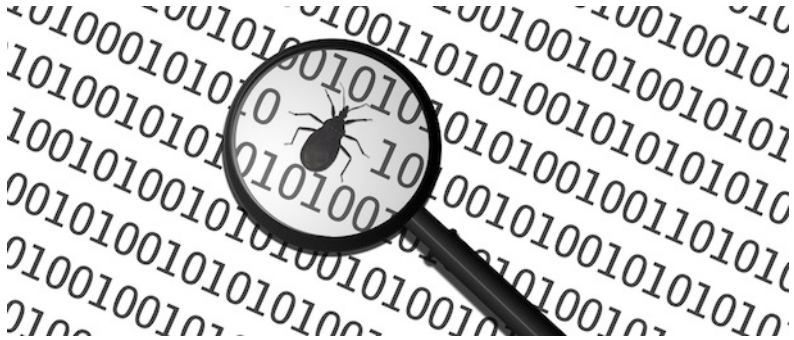
Threat #2: Alteration of information

- Unauthorized modification of information
  - Example: the man-in-the-middle attack, where a network stream is intercepted, modified, and retransmitted
  - DEFENSE?



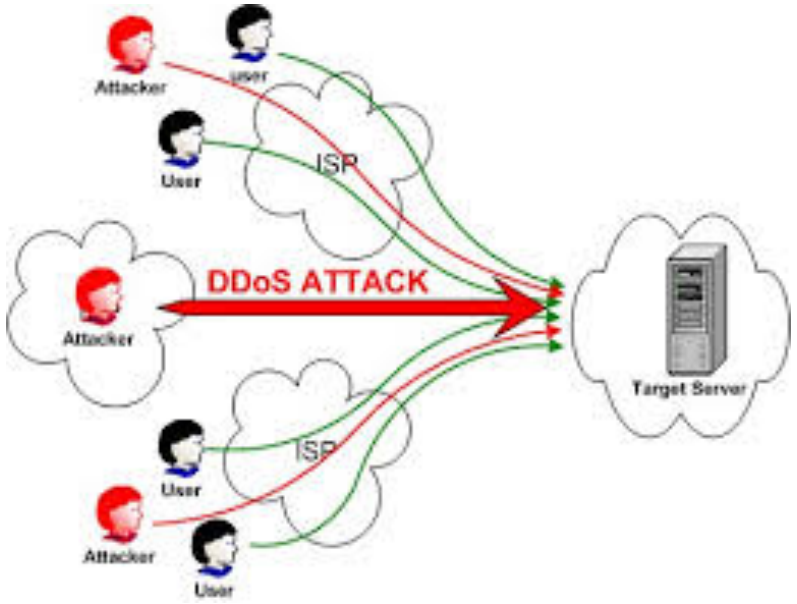
Threat #3: Software bugs

- Code has some bugs that do no affect functionality but can be exploited by an attacker
  - Example: Some application code is mistakenly using an algorithm for encryption that has been broken
  - Example: There is no checking of array bounds
  - DEFENSE?



Threat # 4: Denial of service

- The interruption or degradation of a data service or information access
  - Example: email spam, to the degree that it is meant to simply fill up a mail queue and slow down an email server
  - DEFENSE?



Threat # 5: Breaking passwords

- Defenses?

Threat #6: Sensitive data in the cloud

- Storing files in the cloud. Cloud gets to access data. How do we make sure cloud does not get to see data (e.g., Gmail)?
  - DEFENSE?
- We have 1,000 files and we encrypt them and then we store them in the cloud. While not the cloud cannot see the content, it can see the access patterns. How do we prevent that?

Attacks in the real world


WEB & COMMUNICATION SOFTWARE security

Hotmail Data Loss Reveals Cloud Trust Issues

By Keir Thomas, PCWorld

Jan 3, 2011 11:56 AM


News

Amazon struggles to restore lost data to European cloud customers

Developers vent frustration on Amazon support forum

By Jon Brodkin, Network World

August 09, 2011 11:17 AM ET


« Security Recommendat... | Main | Solaris Security

Amazon S3 Silent Data Corruption

By user12606733 on Jan 28, 2009

While catching up on my reading, I came across an interesting article focused on tl

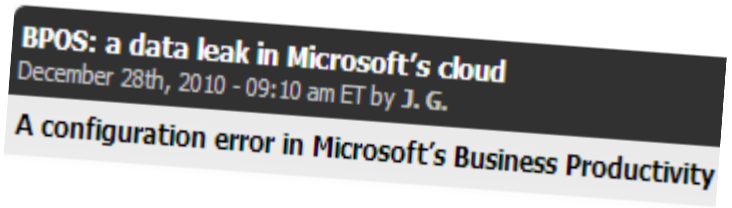

Gmail Corrupting Attachments

I recently received a report that attachments sent to Gmail from some servers


01 August 2012, 12:39

Dropbox confirms data leak

Cloud storage service provider Dropbox has acknowledged that a file


BPOS: a data leak in Microsoft's cloud

December 28th, 2010 - 09:10 am ET by J. G.

A configuration error in Microsoft's Business Productivity

ILOVEYOU worm

- Computer worm that affected million of users on May 5th 2000
- It was an email that contained a “text file” as an attachment
- Opening the attachment would activate a script, which would overwrite image files, and would send a copy of itself to the first 50 addresses in the address book
- http://en.wikipedia.org/wiki/ILOVEYOU
- How can you prevent this? **BE CAREFUL WHAT YOU CLICK**

Dropbox data loss

- In 2009, T-Mobile and Danger, the Microsoft-owned subsidiary that makes the Sidekick, announced that they lost all user data that was being stored on Microsoft's servers due to a server failure
- http://techcrunch.com/2009/10/10/t-mobile-sidekick-disaster-microsofts-servers-crashed-and-they-dont-have-a-backup/
- Problem: Not sufficient back-ups
- How can you prevent this?
  - **ERROR CORRECTING CODES**

One user, Michael Armogan, shared the contents of an email he received from Dropbox:

> We're reaching out to let you know about a Selective Sync issue that affected a small number of Dropbox users. Unfortunately, some of your files were deleted when the Dropbox desktop application was shut down or restarted while you were applying Selective Sync settings.
>
> Our team worked hard to restore files that were deleted from your account. You can see which of your files were affected and whether or not we've been able to restore them on this personalized web page.
>
> We're very sorry about what happened. There's nothing more important to use than making sure your information is safe and always available. Our team has fixed the issue and put additional tests in place to prevent this from happening in the future.

LinkedIn passwords leaked

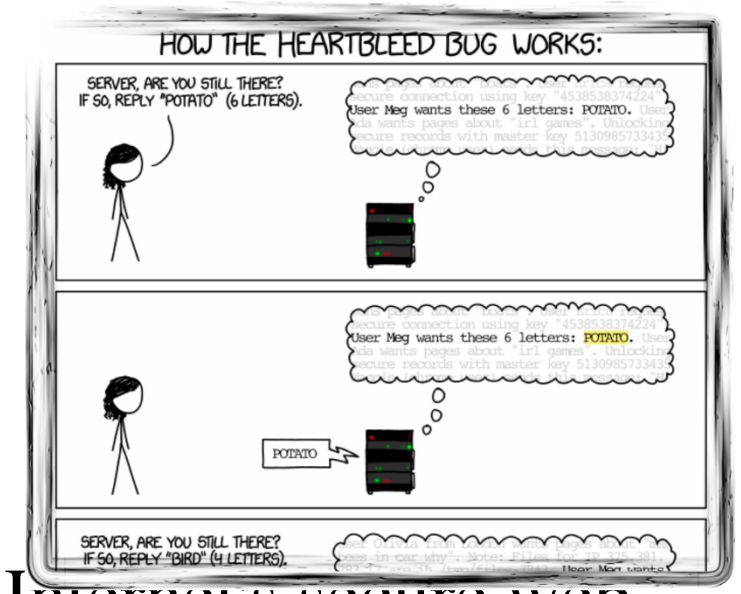
- In June 2012, it was announced that almost 6.5 million LinkedIn passwords were leaked and posted on a hacker site
- http://www.huffingtonpost.com/2012/06/07/linkedin-password-hack-check_n_1577184.html
- Problem: Linkedin did not use salt when hashing the passwords!
  - http://www.stormpath.com/blog/how-linkedin-could-have-secured-hacked-passwords
- How can you prevent this?
  - **ALWAYS USE SALT**

(when using salting, one cannot use preexisting tables to crack passwords easily)

Factoring RSA keys

- Researchers recently showed that a bunch of cryptographic keys used in hardware devices are insecure
- Companies shipped new updates after notified
- https://factorable.net/
- Problem: Same randomness used across devices to generate the keys
- How can you prevent this?
  - **MAKE SURE YOU USE DIFFERENT SEEDS FOR YOUR RANDOM GENERATORS**

Heartbleed



- April 2014
- Bug in the openssl library
- Affected all hosts running TLS protocol
- At the time of the disclosure, around half a million of the Internet's secure web servers certified were believed to be vulnerable to the attack
- Bug in the heartbeat feature http://tools.ietf.org/pdf/rfc6520.pdf
- There was no bound check in the bytearray that the sender would send to the receiver
- So the receiver would send the payload back along with some contents of its memory
- How can you prevent this?
  - **CHECK ARRAY BOUNDS**

WEP standard CRC check

- Security algorithm for privacy and integrity of wi-fi communications
- Introduced in 1997
- Completely broken
- To send a message 1011101:
  - Represent it as a polynomial (x^6+x^4+x^2+x+1)
  - Divide with x^2+1
  - Send the remainder (010) and the message
  - The receiver takes the message and can verify
- What is the problem here?
- How can you prevent this?
  - **USE A CRYPTOGRAPHICALLY SECURE MESSAGE AUTHENTICATION CODE**

Order Preserving Encryption

- Type of deterministic encryption such that
  - If x > y then Enc(x) > Enc(y)
  - Very useful for encrypted databases
  - Used by many systems such as CryptDB, Cipherbase, Google's BigQuery and Microsoft SQL Always Encrypted
- First problem: Deterministic encryption
  - Why this is bad?
  - If I give you bunch of ciphertexts that are names, how can you decrypt?
- Second problem: The order is revealed
  - How can you do better?
- See recent paper describing attack paper http://cs.brown.edu/~seny/pubs/edb.pdf
- How can you prevent this?
  - **USE RANDOMIZED ENCRYPTION…BUT?**