ENEE 459-C
Computer Security

Introduction

UNIVERSITY OF
MARYLAND

Organization

- Class webpage
  - http://enee459c.github.io
  - Two lectures per week, MW11am – 12.15 pm
  - EGR 108
  - Attendance and participation is important
- My information
  - cpap at umd.edu
  - Office hours: Monday, 2pm-3pm, AVW 3409
- Teaching assistants
  - Mitchell Arnett (`marnett@umd.edu`)
  - Evripidis Parakevas (`marnett@umd.edu`)
  - Office hours
    - marnett: TBA
    - evripar: AVW 1143 (Wed 1pm to 2pm)

Homeworks and lectures

- Final grade
  - 5 homeworks (40%)
  - Midterm (20%) --- either Oct 14 or Oct 21
  - Final (35%) --- Dec 16 at 8am
  - Class attendance (5%) --- ask at least two question throughout the semester (I will remember!)
- Lectures will be published on the webpage after class
- Homework 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.

Extra credit (research project): up to 10%

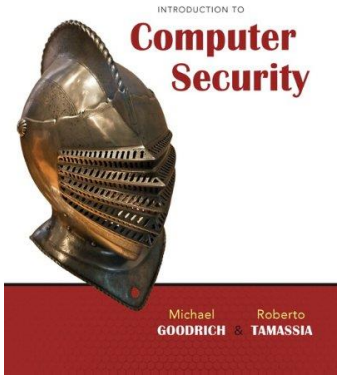
- You will work on a project related to End-to-End encryption that was recently introduced by Google
- You will be expected to modify code at https://github.com/google/end-to-end to enhance the security of the current Google chrome plugin
- JavaScript knowledge is a plus
- Main goal will be to add searchable encryption
- I would expect serious commitment
- Email me if you are interested

Prerequisites

- ENEE150 or CMSC132
- 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

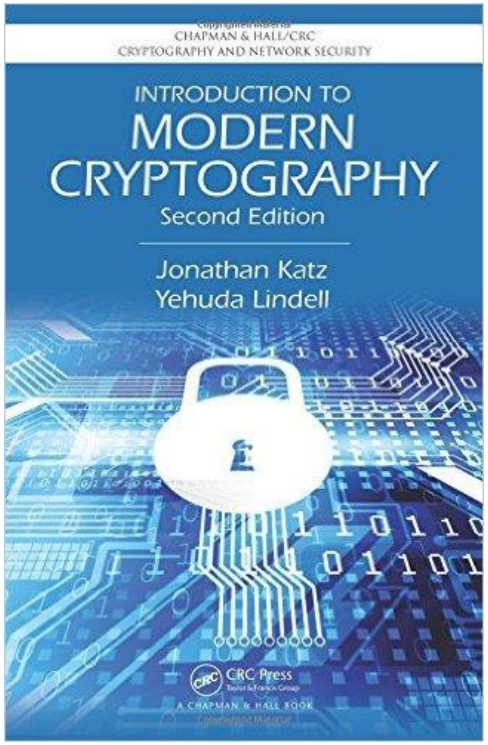
- Most of the class is based on the following textbook (GT):

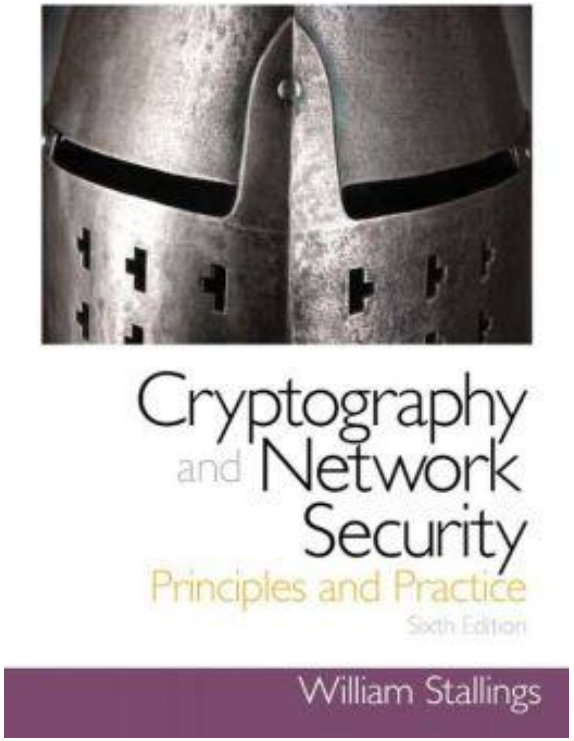


- Thanks to Michael Goodrich and Roberto Tamassia for making the content available
- We are going to be using the board too, so it is advisable you keep notes as well
- The library has copies of the book

Other readings

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





What is this course about?

- Introduction to Computer Security
  - Goals of Computer Security
  - Threats
  - Defenses
- Fundamental concepts in Computer Security
  - Confidentiality
  - Integrity
  - Authentication
  - Access control
- Practical Computer Security
  - Web security
  - Cloud security
  - Network security
  - Systems and software security

What is Computer Security?

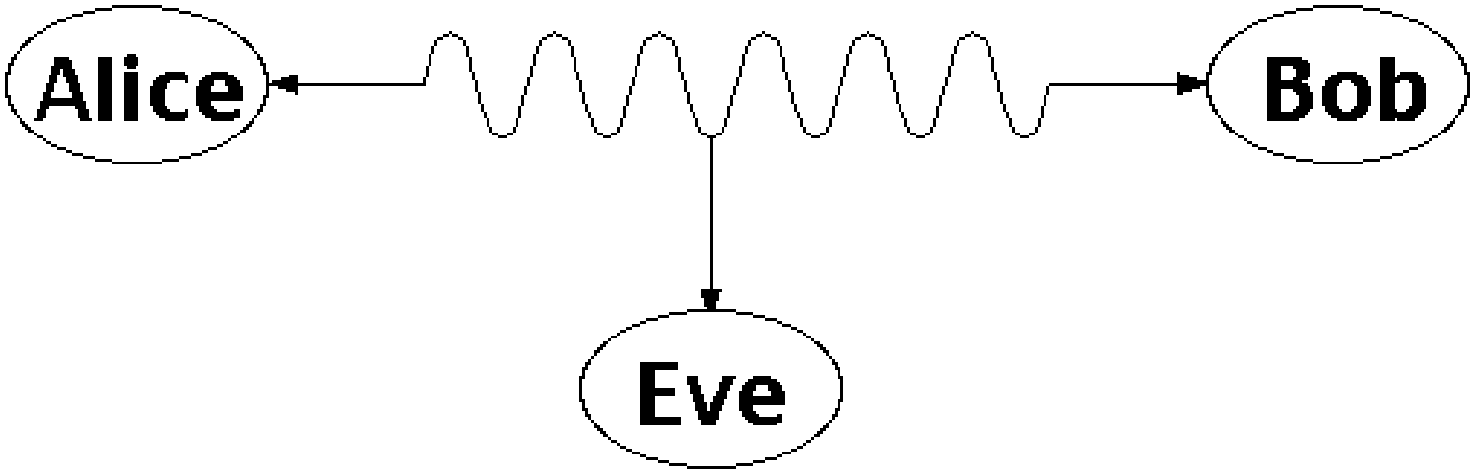
Computer Security
is the prevention of, or protection against

- 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).

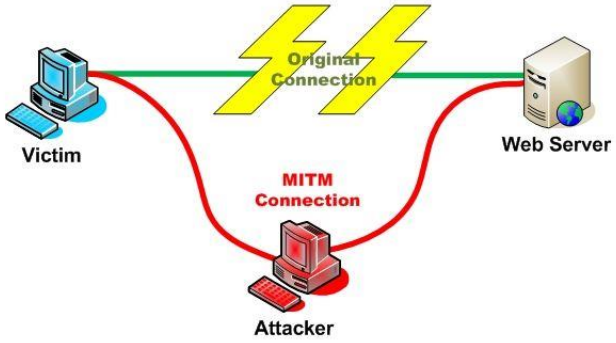
Threats and defenses

- **Eavesdropping:** the interception of information intended for someone else during its transmission over a communication channel



Threats and defenses

- **Alteration:** unauthorized modification of information
  - **Example:** the man-in-the-middle attack, where a network stream is intercepted, modified, and retransmitted

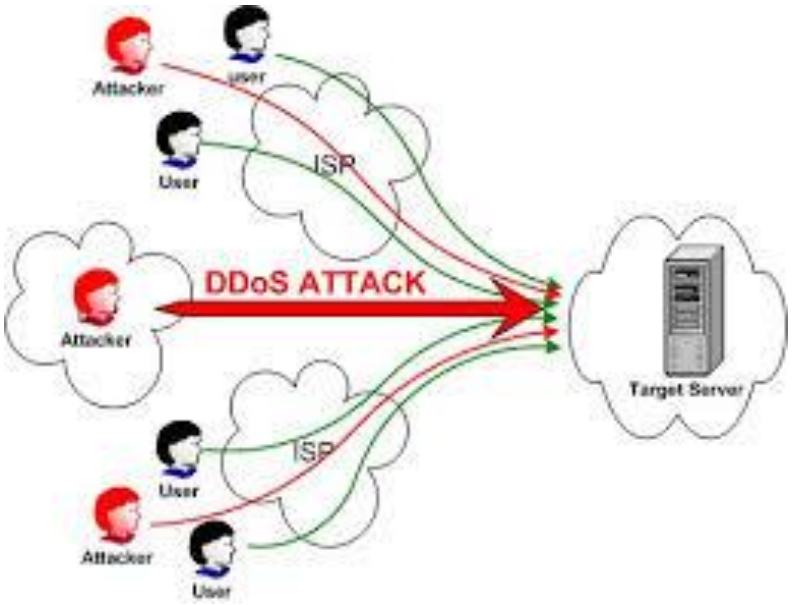


Threats and defenses

- **Software bugs:** Code is not doing what is supposed to be doing
  - **Example:** Some application code is mistakenly using an algorithm for encryption that has been broken
  - **Example:** There is no checking of array bounds

Threats and defenses

- **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



Threats and defenses

- **Masquerading**: the fabrication of information that is purported to be from someone who is not actually the author
- **Repudiation:** the denial of a commitment or data receipt.
  - This involves an attempt to back out of a contract or a protocol that requires the different parties to provide receipts acknowledging that data has been received

Threats and defenses

- **Correlation** and **traceback:** the integration of multiple data sources and information flows to determine the source of a particular data stream or piece of information

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

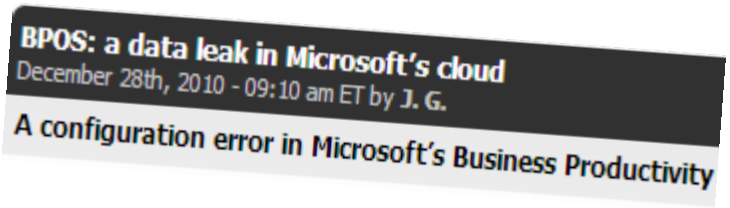

Gmail Corrupting Attachments

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?**

Dropbox data loss

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.

- **Problem**: Not sufficient back-ups

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

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

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