CIS 4360: Computer Security Fundamentals

Introduction

Viet Tung Hoang

The slides are based on those of Prof. Stefano Tessaro, University of Washington

Agenda

1. **What Is Computer Security**
2. Basic Terms in Computer Security
3. Ethical Aspects


VIRUS
DETECTED
NETGEAR
Google
amazon.com

Equifax data breach: How do you fix a cataclysmic crisis?

Brian Tierney, Opinion contributor Published 9:55 a.m. ET Sept. 18, 2017 | Updated 1:47 p.m. ET Sept. 18, 2017

abc NEWS

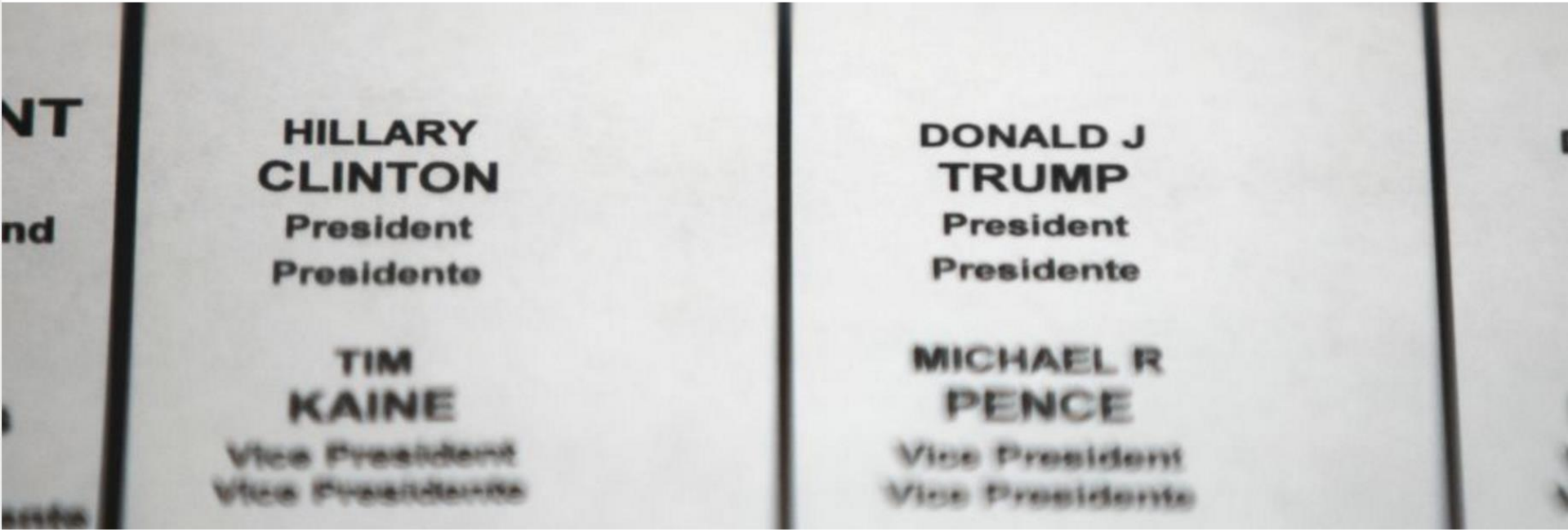
LOG IN

Federal government notifies 21 states of election hacking

By GEOFF MULVIHILL AND JAKE PEARSON, ASSOCIATED PRESS

Sep 22, 2017, 11:58 PM ET

Share with Facebook Share with Twitter



Twitter schedules meeting with U.S. lawmakers on Russia bots

https://www.zdnet.com/article/wannacry-ransomware-crisis-one-year-on-are-we-ready-for-the-next-global-cyber-attack/

EDITION: US

ZDNet

VIDEOS IPHONE WINDOWS 10 CLOUD INNOVATION SECURITY TECH PRO MORE NEWSLETTERS ALL WRI

REVIEW: Apple Watch Series 4: Best for iPhone owners, but not the best smartwatch

WannaCry ransomware crisis, one year on: Are we ready for the next global cyber attack?

WannaCry caused chaos across the world. But have its lessons been learned?

By Danny Palmer | May 11, 2018 -- 11:21 GMT (04:21 PDT) | Topic: Security

2 80

RECOMMENDED FOR YOU

The Rise of Machine Learning (ML) in Cybersecurity: How this critical capability can help prevent today's most sophisticated attacks

Personal Stories?

Anyone ever affected personally by “computer security” incidents?

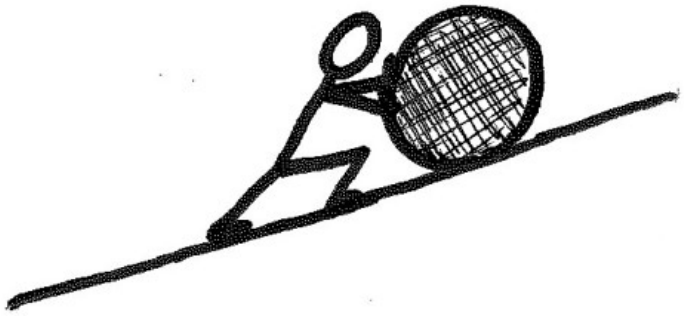
The night is dark and full of terror

Many worst-case prophecies

by computer-security researchers

are becoming true

It's a uphill battle, and you have to play your part.



Spoiler alert: We will not win this battle

Not admitting this is either naïve or malicious.

Let’s make an analogy …

Is this house “safe”?

Is this house “safe”?

We don’t build perfectly safe homes

Just reasonably secure ones within existing constraints (costs & threat models).

CIS4360

Learning the principles of building good homes

The goal of this class

Principles of Computer Security

With several applications to the real-world

Technology changes fast, but basic security issues remain the same

Acquired skills

Adversarial thinking

What would happen if I perform this one action
the system designers have not been thought of?

After taking this class: It's ok not to know all answers,
it's not ok not to know all questions!

Agenda

1. What Is Computer Security

2. **Basic Terms in Computer Security**

3. Ethical Aspects

Confidentiality

Integrity

Goals:
CIA

Availability

Confidentiality

The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Example:

- Data encryption
- Setting user rights on files on multi-user systems to prevent unwanted access

Integrity

Data integrity: The property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner.
Origin integrity: The property that the source of the data is exactly who/what it claims to be, and is not altered

Examples (Data integrity):

- Checksums for data correction on data storage (e.g., RAID)
- Cryptographic message authentication codes

Example (Origin integrity):

- Digital signatures / digital certificates

Availability

The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system

Example:

- Firewall to thwart Denial-of-Service attack

Goals – CIA

Warning:

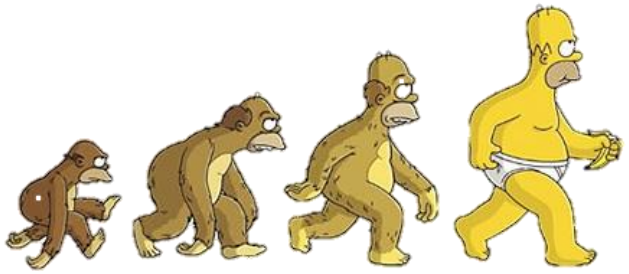
Classification can be ambiguous

A method may ensure multiple goals

Example: Storing passwords securely on a server

Is this meant to guarantee confidentiality / integrity / availability?

Who are adversaries?



Typical examples:

- Script kiddies
- Hacktivists (anonymous, etc.)
- Dissidents
- Criminals / terrorists
- Governments / military / intelligence agencies
- …

Adversaries – the fun times

Historic beginning: **phreaking** (aka, hacking phone systems), ca. 1955-1980, popular in the 70s.

https://en.wikipedia.org/wiki/Blue_box

Achievements: Lots of free calls (2600Hz Cap'n Crunch whistle, Blue Box, …)

Adversaries – cybercrime

1990s-early 2000s: Individuals

- **Kevin Mitnick**
  5 years of prison, late 90s, then became successful security consultant
- **Albert "soupnazi" Gonzalez**
  Major credit card fraud, stole 130mil CC #'s. Sentenced to 15-20 years

Today, powerful groups:

- **Russian Business Network.**

  St. Petersburg Internet hosting company involved in numerous criminal activities. Started as legitimate ISP (2006)

Adversaries – hacktivists

Examples: Julian Assange, Edward Snowden, Anonymous

Often motivated by

political/ideological

reasons, rarely any monetary gains.

Examples – State actors

Often linked to Advanced Persistent Threats (APTs):

Cluster of repeated, correlated activities, traced back to a single group due to some common patterns.

Examples:

- PLA Unit 61398 (China)
- NSA; CIA
- Russia; GRU
- Israel Unit 8200

Example – Intimate Partners

Agenda

1. What Is Computer Security
2. Basic Terms in Computer Security
3. **Ethical Aspects**

An important disclaimer

Part of what we learn in this class can be used

maliciously

Black hat vs white hat

Black hat:

cracker, a criminal

Grey hat:

sometimes criminal, or at least “bending the law”

White hat:

ethical hacker, working within legal framework to perform security evaluations

The law and ethics

- Abuse of security vulnerabilities
  - is against FSU user policies
  - is against Florida and Federal laws

- **Abuse of security vulnerabilities is unethical**
  - Think about what you're doing and the price it has on yourself, the victims, and society in general

Rules of thumb

- When in doubt … don't.
  - Come ask me

- You must have written permission from a system owner before doing any penetration testing
  - Homework will generally be on your own system
  - We will have a system available for some homework

Responsible disclosure

- **Full disclosure** means revealing everything about a vulnerability including an example exploit

- **Responsible disclosure** refers to ensuring potential victims are aware of vulnerabilities before going public