CY 2550 Foundations of Cybersecurity

Logistics

Alina Oprea
Associate Professor, Khoury College
Northeastern University

Hello!

- Welcome to CY 2550
  - Are you in the right classroom?
  - Okay, good.
  - This is first section of CY 2550
- Who am I?
  - Associate Professor Alina Oprea
  - a.oprea@northeastern.edu
  - Office: ISEC 625
  - Office Hours: Thursdays 2-4pm or by appointment
  - Working in various areas of cyber security, including threat detection, adversarial machine learning, privacy, and cloud security

Say Hi to the TAs

- TAs:
  - Simon Bruklich
  - Kathrine Driscoll
  - Samir Elhelw
  - Matthew Kline
  - Byron Kress
  - Fiona McCrae
  - Martin Petrauskas
  - Donald Sea
  - Rahul Toppur

- Office hours (every day): Will be announced on class website
- http://www.ccs.neu.edu/home/alina/classes/Spring2020

Why Take This Course?

RSA

Target

TJ Maxx

Yahoo

Ashley Madison

Sony Pictures

The Office of Personnel Management

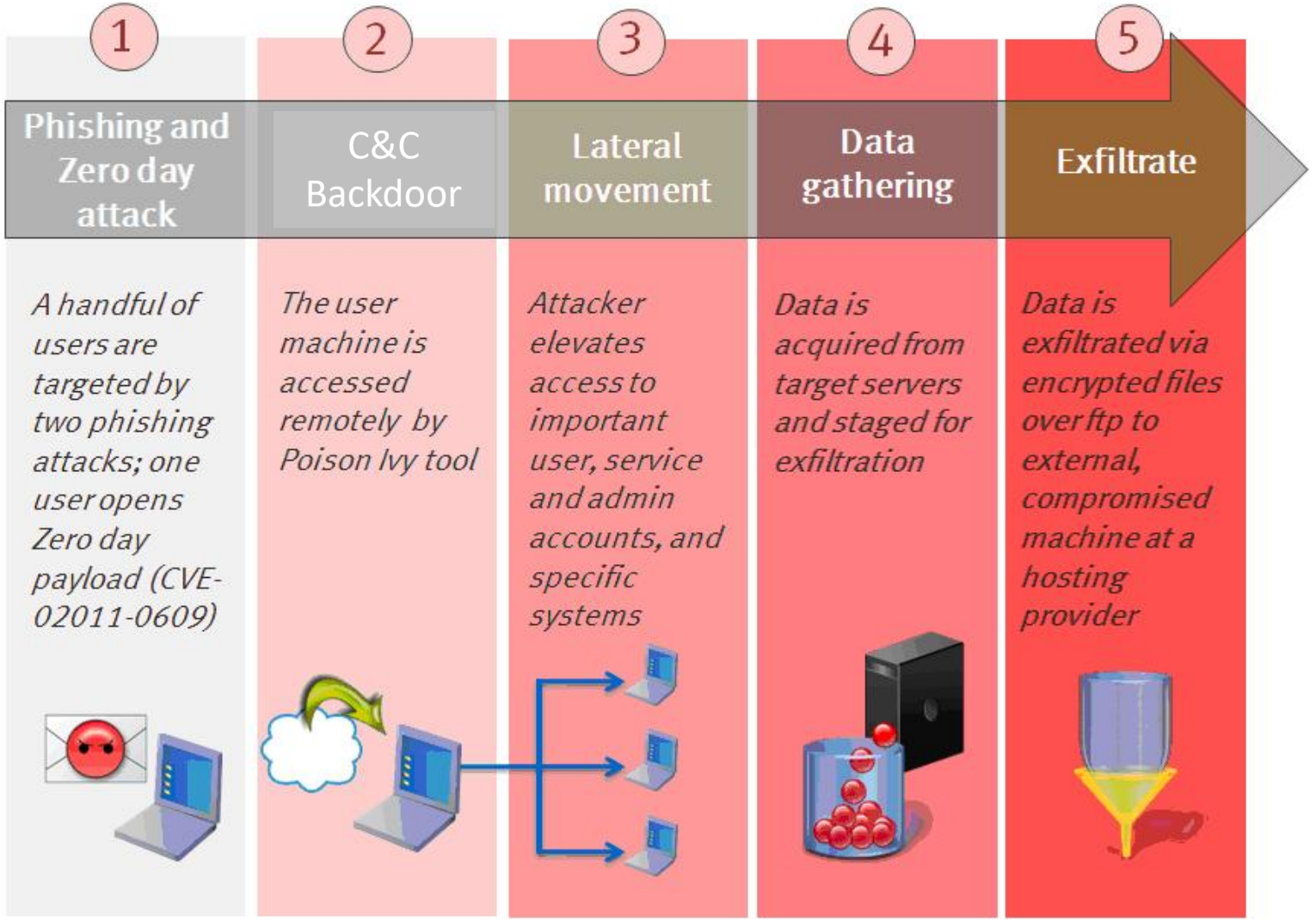
Equifax

The Democratic National Convention

- What do they all have in common?
  - Victims of massive data breaches
- Every company is now a tech company, and every company is now vulnerable

- Exfiltration of sensitive information
- Loss of intellectual property
- Financial losses

The RSA attack 2011

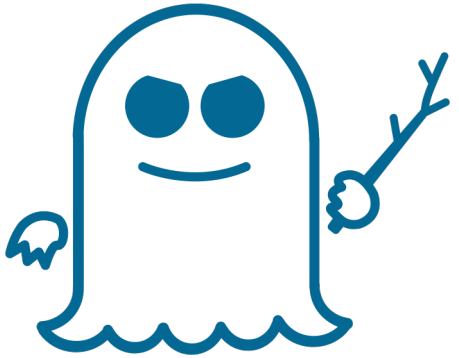


Why Take This Course?

Heartbleed

Shellshock

Meltdown



Spectre

- What are these?
  - Software vulnerabilities that enable malicious exploits
- Software is so critical to our way of life that massive security vulnerabilities now achieve celebrity status

Why Take This Course?

- Cybersecurity is now a fundamental aspect of life
  - It affects every person
  - It affects every company
  - It affects every nation
- Adversaries are powerful and sophisticated
  - Cybercrime is a multi-million dollar industry
  - Nations are using the Internet as a battleground
- Every computer scientist needs to understand cybersecurity
  - Whether we like it or not, we are on the front lines
  - Enormous opportunity to help people navigate a hostile internet

Goals

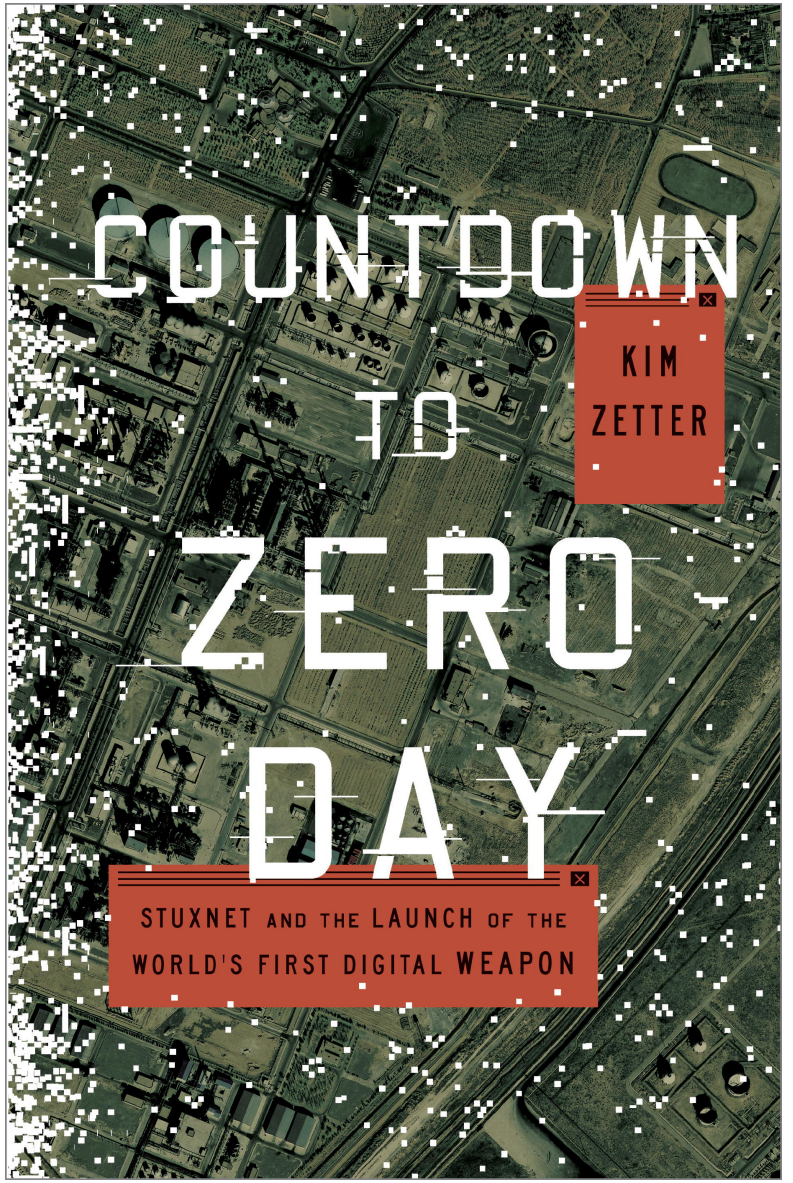
- Fundamental understanding about cybersecurity
  - Ability to “think like an attacker” and model threats
  - Knowing essential security principles, practices, and tools
  - Grappling with ethical, legal, and social issues
- Focus on software and tools
  - Not hardware
  - Some theoretical foundations (crypto)
  - Classes of attacks and defenses
- Project-centric, hands on experience
  - Real projects that build concrete skills

Online Resources

- Class website: http://www.ccs.neu.edu/home/alina/classes/Spring2020
- Class forum is on Piazza
  - Sign up today!
  - Install their iPhone/Android app
  - www.piazza.com/northeastern/spring2020/cy2550
- When in doubt, post to Piazza
  - Piazza is preferable to email
  - Use #hashtags (#lecture2, #project3, etc.)

Books

- Textbook available online:
  - Computer Security and the Internet: Tools and Jewels by Paul C. van Oorschot, 2019
  - https://people.scs.carleton.ca/~paulv/toolsjewels.html
- One required reading:
  - Countdown to Zero Day by Kim Zetter
  - Stuxnet attack



Workload and Grading

Projects (~7)	50%
Quizzes (5)	2% each
Midterm	20%
Final	20%
Total	**100%**

Projects

- This course is project-centric
  - Designed to give you real experience
  - Start early!
- ~7 projects
  - Due at 11:59:59pm on specified days
  - Use turn-in scripts to submit your code, documentation, etc.

- Linux/command line basics
- GPG key generation and essential cryptography
- Password generation and cracking
- Social engineering (essay assignment)
- Mini-Capture the Flag, exploit development

Policies

- Your responsibilities
  - Please be on time, attend classes, and take notes
  - Participate in interactive discussion in class (state your name when asking a question)
  - Submit assignments/ programming projects on time
- Late days for assignments
  - 5 total late days, after that loose 20% for every late day
  - 1 second late = 1 hour late = 1 day late
  - Assignments are due at 11:59pm on the specified date

Project 0

- Released later this week
- Get your VM setup and start learning command line Linux
- Project questions?
  - Post them on Piazza!

Quizzes

- There will be five in-class quizzes throughout the semester
- Given on random days
- Roughly 10-15 minutes long
- Goals of the quizzes:
  - Make sure you are paying attention and understanding key concepts
  - To incentivize attendance
- Non-goals:
  - Shredding your mind with super hard questions

Exams

- Midterm and Final
  - Midterm will be in-class, final date/time will be announced later
  - The final will be **cumulative**
- All exams are:
  - Closed book, leave the laptop at home
  - You are allowed to bring an 8.5x11 one-side cheat sheet
- Question format:
  - Short answer
  - Conceptual
  - Pseudocode

Participation

- This is a college course
  - Not taking attendance
  - But beware missing quizzes!
- Please come and participate!
  - Ask questions!
  - Ideally, I want to know everyone’s name by the end of the semester
  - Make it interactive!

Ethics and the Law

- We will discuss sensitive topics in this class
  - Brazen criminal activity
  - Offensive hacking techniques
- The goal is to help you understand the capabilities and motivations of attackers
- **Do not, under any circumstances, use these skills offensively**
  - Run exploits on Khoury College machines
  - Use scanning or attack tools against public servers or websites
  - Infiltrate your roommates computer and spy on them
  - Etc.
- Failure to comply may result in expulsion and/or arrest

Academic Integrity

- Homework is done individually!
- Rules
  - Can discuss with colleagues, instructors, and TAs
  - Can post and answer questions on Piazza
  - Code or written assignment cannot be shared with colleagues
- NO CHEATHING WILL BE TOLERATED!
- Any cheating will automatically result in grade F and report to the university administration
- http://www.northeastern.edu/osccr/academic-integrity-policy/

Questions?

(Short) History of Cybersecurity

"Those who cannot remember the past are condemned to repeat it." – George Santayana

- Cybersecurity has changed immensely over the years and continues to change
- How did we get here?

Cybersecurity

- Cybersecurity, arguably, traces its origins to the 1970s
  - Phone phreakers vs. the telephone networks
- It's hard to have cybersecurity without:
  - Ubiquitous computers
  - Ubiquitous connectivity
- However, many fundamental concepts are much, much older

Historical cryptography

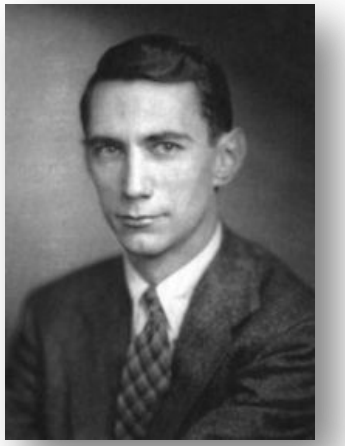
Cryptography ≈ Encryption

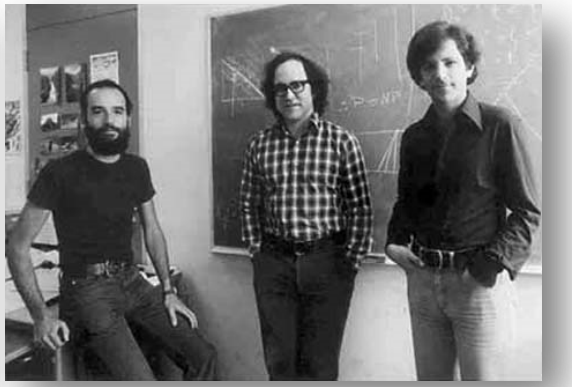
Main applications: **military and diplomacy**

ancient times → **world war II**

Modern cryptography

Cryptography based on rigorous science/math





multiparty-computations

zero-knowledge

threshold crypto

electronic auctions

electronic voting

crypto currencies

private info retreival

computation in cloud

...

information theory

public-key cryptography

signature schemes

rigorous definitions

post-war **sevenites** **now**

Information Assurance

- IA is the practice of managing risks related to the use, processing, storage, and transmission of information
- Desirable properties:
  - Confidentiality – secrecy of communication
  - Integrity – no unauthorized modifications
  - Authenticity – no spoofing or faking
  - Non-repudiation – no disclaiming of authorship
- Properties are often achieved (assured) through cryptography

Ancient Origins

- 1500 BCE – Encrypted tablets from Mesopotamia
- 600 BCE – First use of monoalphabetic substitution ciphers
- 400 BCE – Kama Sutra describes cyphers for protecting communications between lovers
- 800 AD – Al-Kindi uses frequency-analysis to break monoalphabetic substitution ciphers

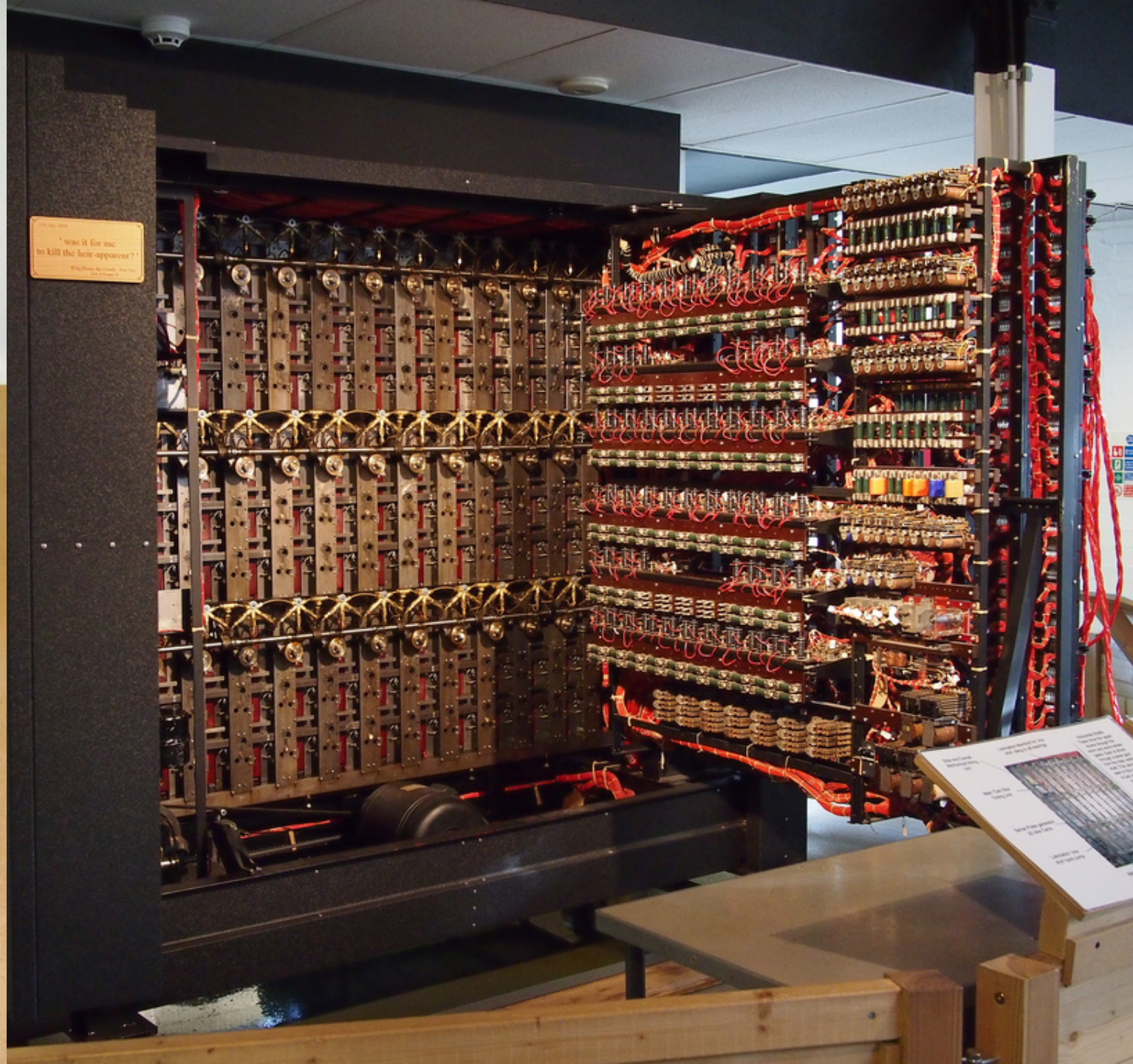
Caesar Shift

- Simple symmetric monoalphabetic substitution cipher
  - Key is a number *k*
  - To encrypt, “shift” each letter by *k* positions
  - To decrypt, “shift” each letter back by *k* positions

HEY BRUTUS BRING A KNIFE TO THE PARTY

KHB EUXWXV EULQJ D NQLIH WR WKH SDUWB


Geheim!
Zur Beachtung!
Geheim!


' was it for me
to kill the heir-apparent? '

World War II as Catalyst

- Ushers in modern cryptography and cryptanalysis
  - Never again will ad-hoc cryptography (like Enigma) be secure
- Spurs the creation of the first digital computers
  - Turing's Bombe
- Leads to the birth of computer science

Phone Phreaking

- The term hacker was introduced in a 1963 MIT student newspaper article about hacking the telephone system
  - Original meaning: somebody who enjoyed exploring, playing with, or learning about computers
- 1960-1970's: golden age of phreaking
  - Curious nerds who explored the telephone network

Changing Norms

- The original phreaks were tinkerers and explorers
  - Looping calls around the planet
  - Setting up “party lines” for group chat
  - Locating strange corners of the phone system
- Eventually, the culture and meaning of phreaking changed
  - Referred to using exploits to get free phone calls

Legal

Illegal

ARPANET

- 1969 – ARPANET comes online
- 1973 – Robert Metcalfe warns that ARPANET is insecure
  - High-school kids are poking around on the network
- 1983 – Fred Cohen invents the term computer virus
- 1983 – ARPANET adopts TCP/IP

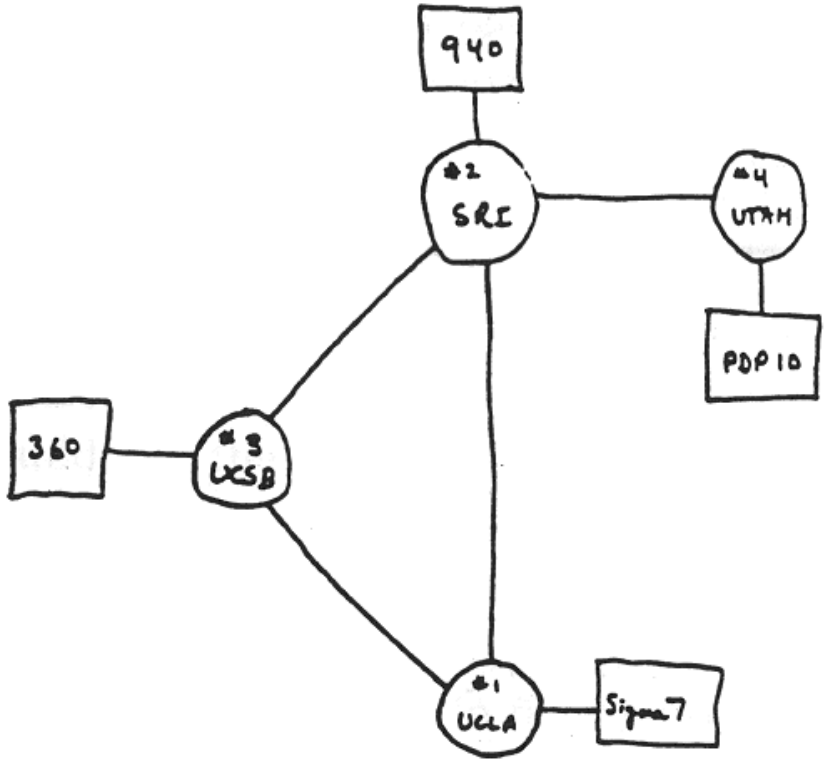
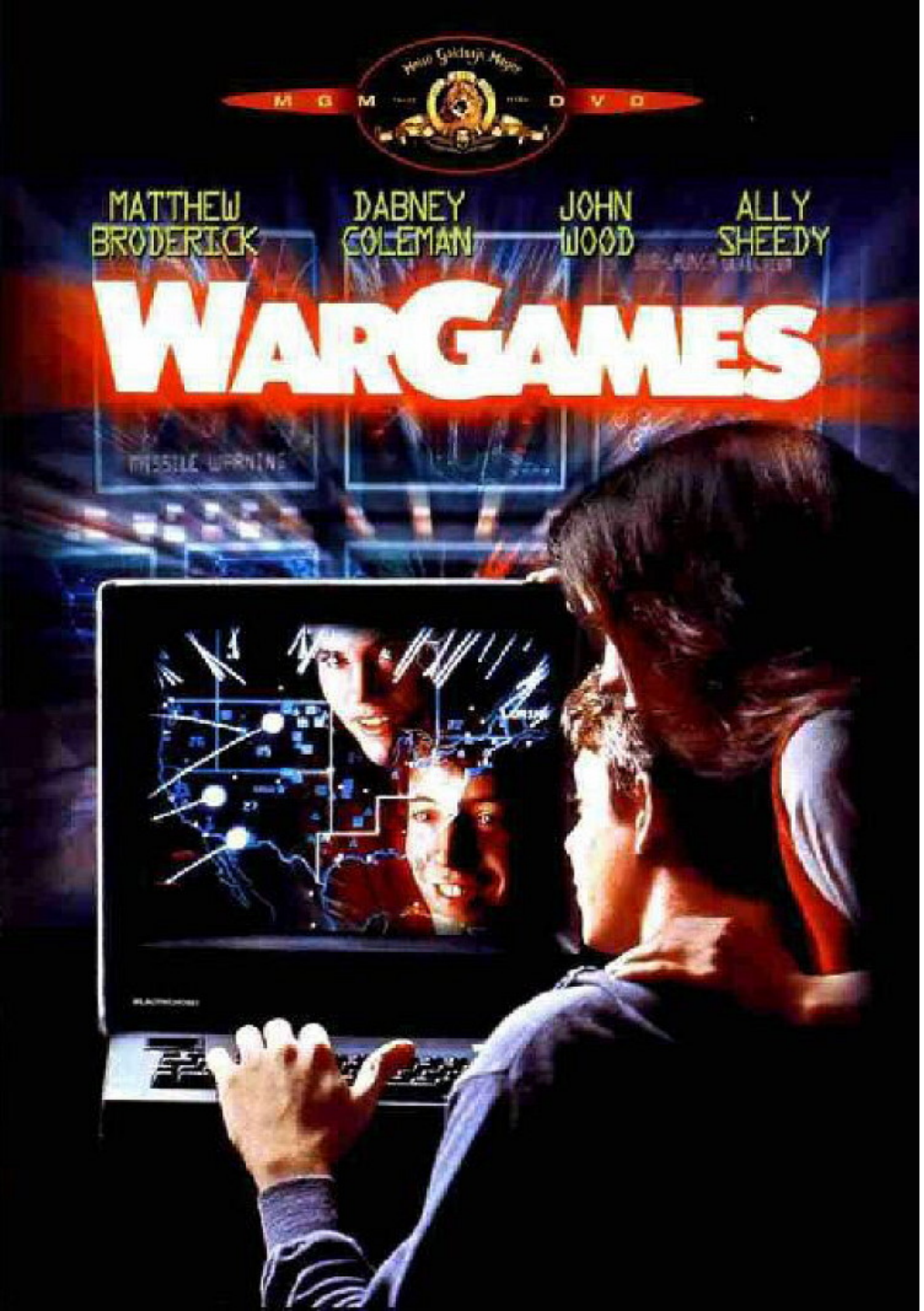


FIGURE 6.2 Drawing of 4 Node Network (Courtesy of Alex McKenzie)



WarGames (1983)

Towards Cybercrime

- 1986 –Marcus Hess breaks into Arpanet
  - Breaks into 400 military computers, including mainframes at the Pentagon
  - Goal: sell secrets to the KGB
- Caught by a honeypot
  - Machine set up to look like a tempting target…
  - … but in reality is a trap designed to surveille the intruder
  - One of the most effective ways of observing attackers

CFAA

- 1986 – Congress passes the Computer Fraud and Abuse Act
  - First major anti-computer crime legislation
  - Criminalizes “unauthorized access” to “protected computer systems”
  - Some claim the law was passed in direct response to WarGames

Portents of Things to Come

- 1988 – Robert Morris inadvertently releases the first worm
  - Leveraged a bug in *sendmail* to remotely exploit vulnerable servers
  - Copied itself to the server
- Released as a research experiment
  - A bug in Robert's code caused the program to replicate out of control
- Crashed 10% of the computers on the ARPANET
- Morris was convicted under the CFAA, 3 years probation + $10k fine
- First documented use of a buffer overflow exploit

From ARPANET to Internet

- 1993 – NCSA Mosaic is the first web browser
- 1994 – Internet becomes totally privatized
- 1999 – Beginning of the first .com bubble
- 2000 – Broadband internet starts becoming widely available

- Widespread, always on internet connections become the norm
- Problems
  - Software is wildly insecure, not designed for a connected world
  - People are unprepared to manage their own security

Havoc on the Internet

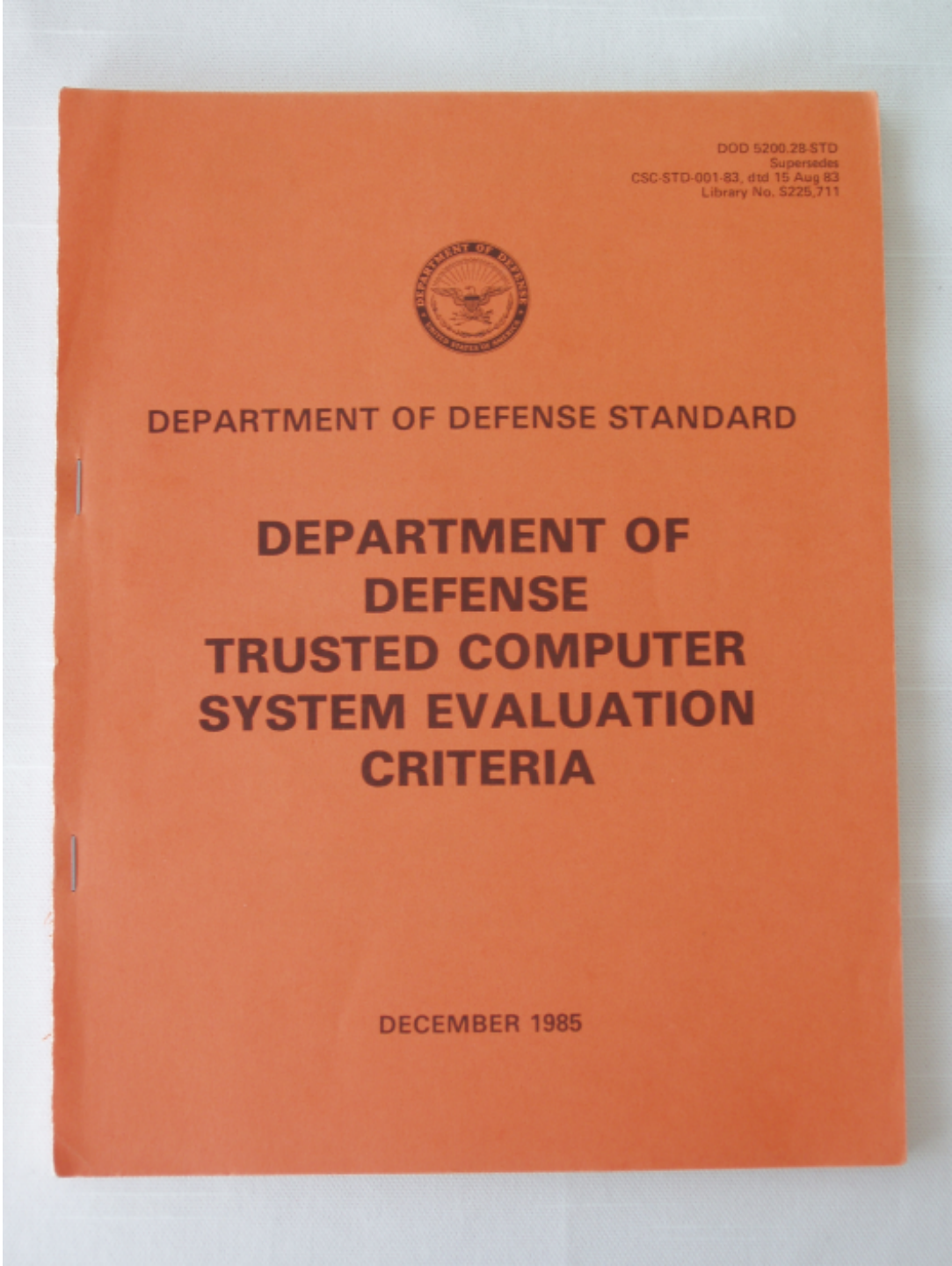
- 1999 – Melissa macro virus spreads via email attachments
- 2000 – ILOVEYOU virus released, infects millions of machines in hours
  - One of the first widespread uses of social engineering tactics
- 2000 – 15-year old “mafiaboy” invents the Denial of Service attack
  - Causes millions of damage to e-commerce websites
  - Yahoo becomes unavailable for an hour
- 2001 – Code Red worm spreads via Microsoft IIS exploit
- 2003 – SQL Slammer and Blaster spread exponentially via exploits in Microsoft products

Defacement and Hacktivism

- Culture of breaking into and “tagging” websites
  - Throughout the 1990s and early 2000s
  - Demonstration of 31337 skills
- Hacktivism: defacement for political ends
  - 2003 – Anonymous
  - 2011 -- LulzSec

Reevaluating Cybersecurity

- 1983 – The Orange Book
  - Developed by NSA, published by DOD
  - Primarily concerned with specifying security models and access control
  - Designed to mitigate insider threats
- Does not consider:
  - Vulnerabilities and exploits
  - Networked threats
  - Social engineering
- Provides levels of certification
- Common Criteria for Information Technology Security Evaluation, 2005



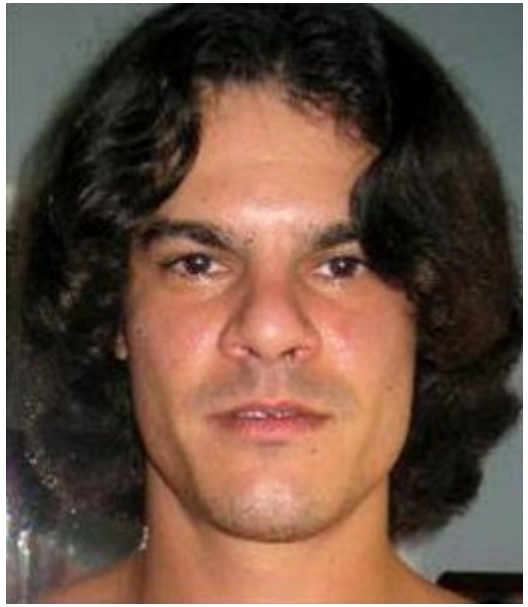
Taking Cybersecurity Seriously

- 1987 – McAfee releases first version of VirusScan
- 1995 – Mozilla releases the Secure Socket Layer (SSL) protocol
- 2001 – NIST standardizes the Advanced Encryption Standard (AES)
- 2002 – Bill Gates launches Microsoft's "Trustworthy Computing" initiative
  - Security, Privacy, Reliability, and Business Integrity
  - Watershed moment for secure software development

From Hacking to Organized Crime

- Hacking culture throughout the 1990's and early 2000's was driven by the quest for respect
  - Virus writers, web hackers, etc. competed to be the most 31337
  - Destructive, unethical, and illegal…
  - … but still driven by a sense of technological exploration
- By late 2000's, hacking culture was largely dead
- In its place was organized cybercrime

The Modern Criminal



- 2005 – Albert Gonzalez steals 46 million credit cards from TJ Maxx
- 2006 – The Russian Business Network (RBN) comes online
  - Offered bulletproof hosting for criminal enterprises
- 2007 – Storm worm turns infected machines into a botnet
- 2007 – First version of Zeus banking trojan released

The Future?

- Automated attacks carried out by adversarial AIs
- Remote and deadly hacks of robots and autonomous cars
- Cryptocurrency anarchy
- Widespread social engineering via targeted propaganda
- Actual warfare in cyberspace
- Complete loss of individual privacy

… Training more security experts could prevent these!