Cristina Nita-Rotaru


# CY2550: Foundations of Cybersecurity
# Section 03

## Introduction. Class Policy. History.

# Class resources

# Class resources

- Public webpage – public access

  https://cnitarot.github.io/courses/fc_Fall_2022/index.html
- CANVAS – main hub and quizes
- PIAZZA – main communication channel
- GRADESCOPE – assignments and grading
- Email in case of emergency - use cy2550 in subject

  c.nitarotaru@northeastern.edu

**THIS IS YOUR SECTION, please follow these links, while there are similarities with other sections, there will be differences**

# CANVAS

- Contains links to class website and piazza
- Has information that needs to be password protected such as your grades
- Will be used for quizes

# PIAZZA

- Main communication environment where I will post
  - announcements
  - questions about class, projects, etc

- You can post privately just to me and TAs
- Public questions are anonymous to your colleagues

- If you have not received an invite already email me and I will add you to piazza

# How to ask on Piazza

- Read slides, notes, or project description
- Use #hashtags (#lecture2, #project3, #hw1, etc.)
- Describe the problem clearly, using the right terms
- Add code in attached files
- Add output from compiler or debugging information
- Add any other relevant information
- **Don't post publicly solutions on piazza**
- **Anything that relates to solution post PRIVATELY**

# OFFICE HOURS

- Cristina: TF 3:30 – 4:30 (this is after class), ISEC 626
- Talha: WTh 3:30 pm - 5:00 pm
- Additional availability outside the allocated time if you have conflicts with the office hours

Schedule and links are in piazza post @6 which will be updated during the semester

# Individual meeting

- It is my policy to individually meet with you at least once per semester – this is a requirement
- Goal of the meeting is to get to know you and provide individual advice about the class
- I will update piazza with how to sign up to meet with me during office hours or outside office hours
- If needed you can set up additional  appointments by sending me a private message on piazza

# How to stay engaged during lecture and outside lecture

- **Come to lecture, having a structure helps**
- Take notes
- Ask questions
- Chat with colleagues
- Make plans with colleagues to work together on projects
  - They are individual but you can discuss them
- Ask/answer questions on piazza
- Meet with the Tas

The class is not only the slides, projects, and quizes

# Academy integrity

- It is allowed to discuss homework problems before writing them down; however, WRITING IS INDIVIDUAL
  - if you look at another student's written or typed answers, or let another student look at your written or typed answers, that is considered cheating
- It is allowed to discuss your project with your colleagues, but DO NOT SHARE CODE
- Never have a copy of someone else's homework or program in your possession and never give your homework (or password) or program to someone else.
- NO CHEATHING WILL BE TOLERATED

# Exceptional situations

- Anything that impacts you and class please let me know
- We will accommodate the situation and find a solution

- I expect that deadlines will be difficult to make if you will be impacted by covid19, so just let me know and we will work together to accommodate the situation

# Weather/Emergency

- In the event of a major campus emergency, course requirements, deadlines and grading percentages are subject to changes that may be necessitated by a revised semester calendar or other circumstances beyond the instructor's control.

# This is an in-class person

- Slides will be made available immediately before lecture
- No recording will happen in class
- If you have to miss class, read the slides, and I will be happy to meet with you and address any questions

DO NOT RECORD IN CLASS

- Massachusetts **prohibits the recording, interception, use or disclosure of any conversation, whether in person or over the telephone, without the permission of all the parties**. The state also prohibits the recording and disclosure of images intercepted in violation of its hidden camera laws.

# Class syllabus

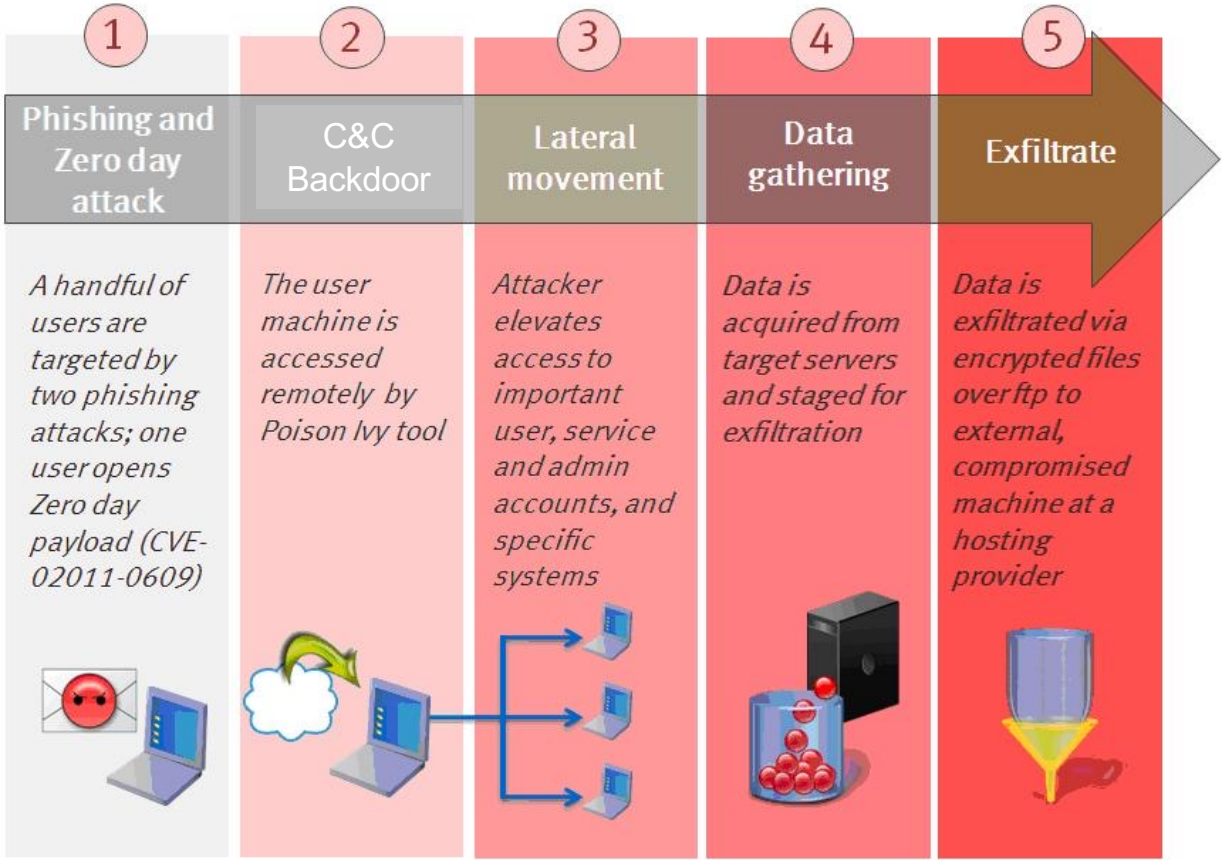
# You've seen the news

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

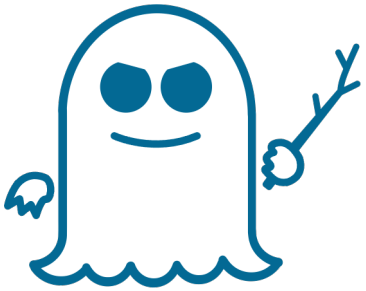
# The RSA attack 2011



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?

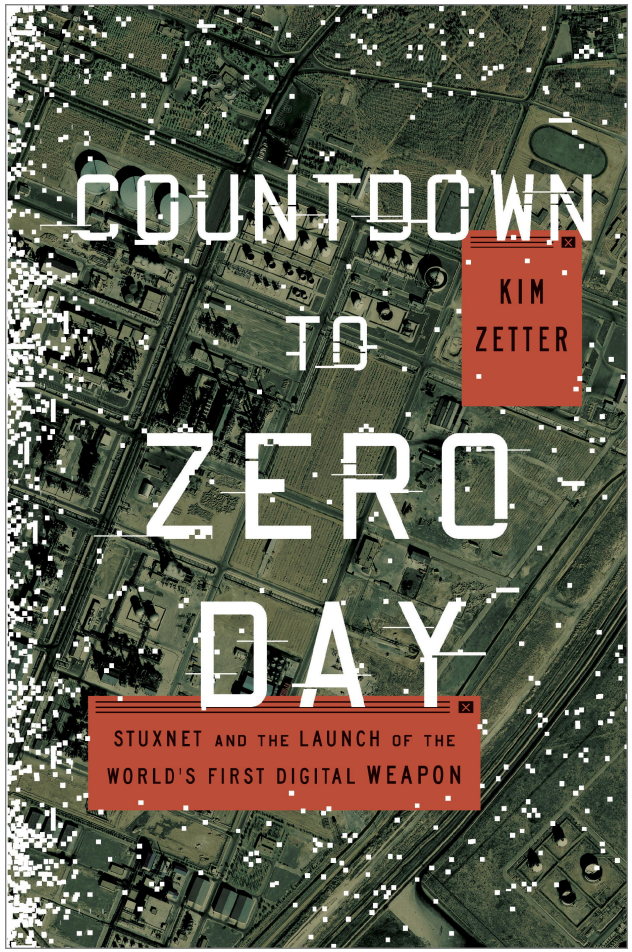
- Cybersecurity is now a fundamental aspect of life
  - It affects every person
  - It affects every company
  - It affects every nation
- Adversaries are powerful and sophisticated
  - Cybercrime is a multi-million dollar industry
  - Nations are using the Internet as a battleground
- Every computer 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
  - Classes of attacks and defenses
- Project-centric, hands on experience
  - Real projects that build concrete skills

# Books

- Required reading:
- Ghost in the Wires: My Adventures as the World's Most Wanted Hacker by Kevin Mitnick
- Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon by Kim Zetter



# Workload and grading

(about 7) programming projects (PP)
(about 5) take home quizes (QQ)

**75%*PP + 25%*QQ**

**There are no midterm or final exams**

# Projects

- This course is project-centric
  - Designed to give you real experience
  - Start early!
- ~7 projects
  - **Due at 9 pm on specified days**
  - Use gradescope to submit your code, documentation, etc.
  - **There are no extensions or late days**
- Regrade: If we made a mistake I will be happy to revisit but the entire project will be regraded

# Examples of projects

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

# Project 1

- Will be released today, due Tuesday Sept. 20, hard deadline
- We will spend next week making sure that everybody finishes this project as without it we can not continue with the other projects
- Get your VM setup and start learning command line Linux
- Project questions?
  - Post them on Piazza!

# Quizzes

- There will be five quizzes throughout the semester
- They will be announced, they are take-home exams, once you start you have to finish it in about 45 minutes
- You can not retake it

# 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

# 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 programming projects on time

# (Short) History of Cybersecurity

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

**Cybersecurity** is the practice of deploying **people, policies, processes,** and **technologies** to protect organizations, their **critical systems and sensitive information** from **digital attacks**.

https://www.gartner.com/en/topics/cybersecurity

What do you think of this definition?

# Cyberattacks

- First cyber attacks in the 1970s
  - Phone phreakers vs. the telephone networks
- Facilitated by:
  - Ubiquitous computers
  - Ubiquitous connectivity
  - Dependency of high-value or critical services of computing

# Secrecy

- Secrecy has been part of human history
- Military
- Diplomacy

- Cryptography
  - "hidden writing"
  - hide the meaning of a message
- Steganography
  - "covered writing"
  - hides the existence of a message

# Historical cryptography

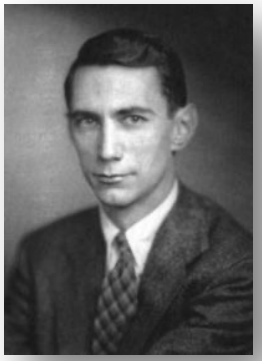
- First stage, paper and ink based scheme
- Second stage, use cryptographic engines
- Third stage, modern cryptography

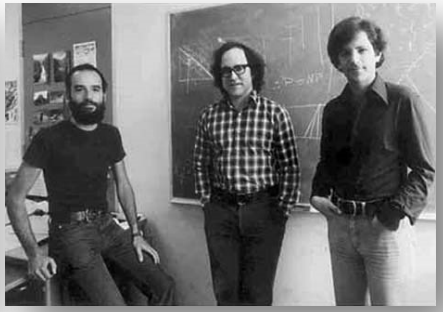



**ancient times** **world war II**

# Modern cryptography

Cryptography based on rigorous science/math





**information theory**

**public-key cryptography**

**signature schemes**

**rigorous definitions**

**multiparty-computations**

**zero-knowledge**

**threshold crypto**

**electronic auctions**

**electronic voting**

**crypto currencies**

**private info retreival**

**computation in cloud**

**...**

**post-world war II** **seventies** **now**

# Crypto and quantum computing

- Many public-key cryptography algorithms rely their security on mathematical problems that require significant computational effort to solve computational and on assumptions about the computational power of the attacker
- Quantum computing breaks these assumptions
- Quantum computers will be able to easily solve these mathematical problems and deem the corresponding crypto algorithms obsolete
- Example: RSA relies on factoring large numbers

Need different mechanisms to secure communication !

# Information assurance

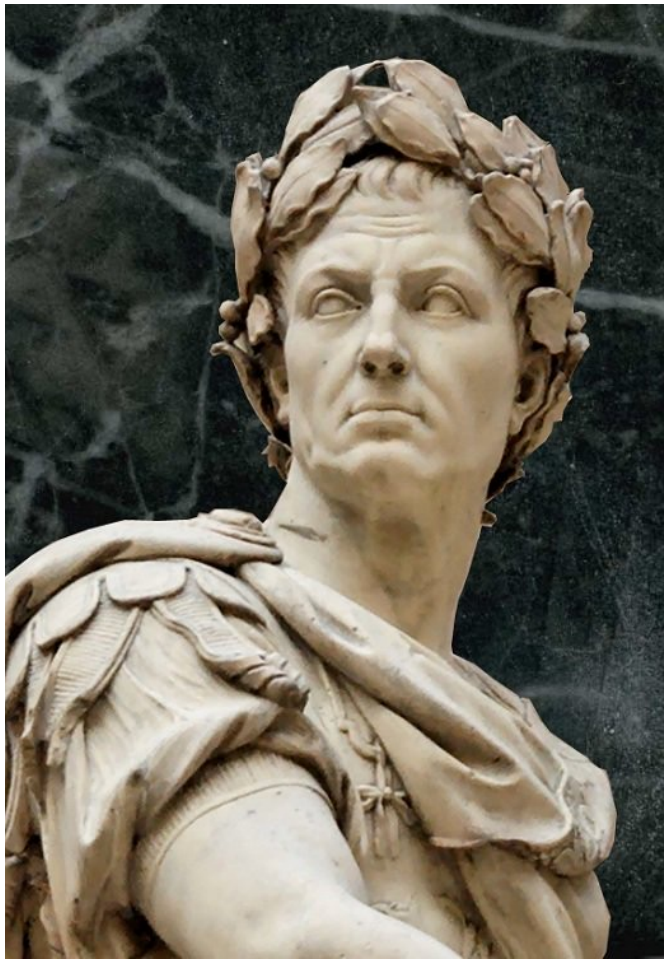
- IA is the practice of managing risks related to the use, processing, storage, and transmission of information
- Desirable properties:
  - Confidentiality – secrecy of communication
  - Integrity – no unauthorized modifications
  - Authenticity – no spoofing or faking
  - Non-repudiation – no disclaiming 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 cipher

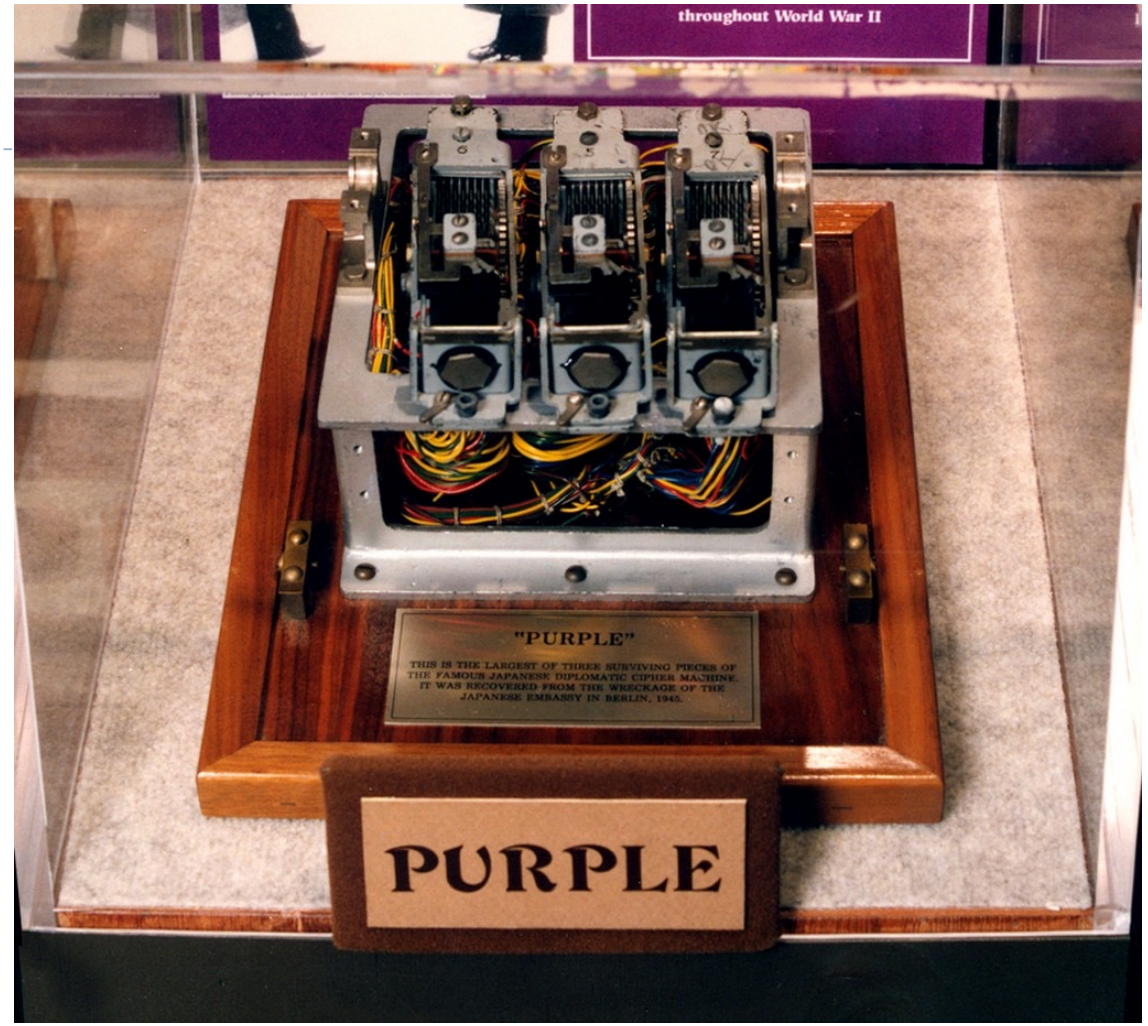
- Simple symmetric monoalphabetic substitution cipher
  - Key is number 3
  - To encrypt, "shift" each letter by *3* positions
  - To decrypt, "shift" each letter back by *3* positions



```
HEY BRUTUS BRING A KNIFE TO THE PARTY
```

```
KHB EUXWXV EULQJ D NQLIH WR WKH SDUWB
```


Polish Cipher Bureau and British Bletchley Park – Alan Turing




US Army Signals Intelligence Service - Genevieve Grotjan

# 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

Legal

- Eventually, the culture and meaning of phreaking changed
  - Referred to using exploits to get free phone calls

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

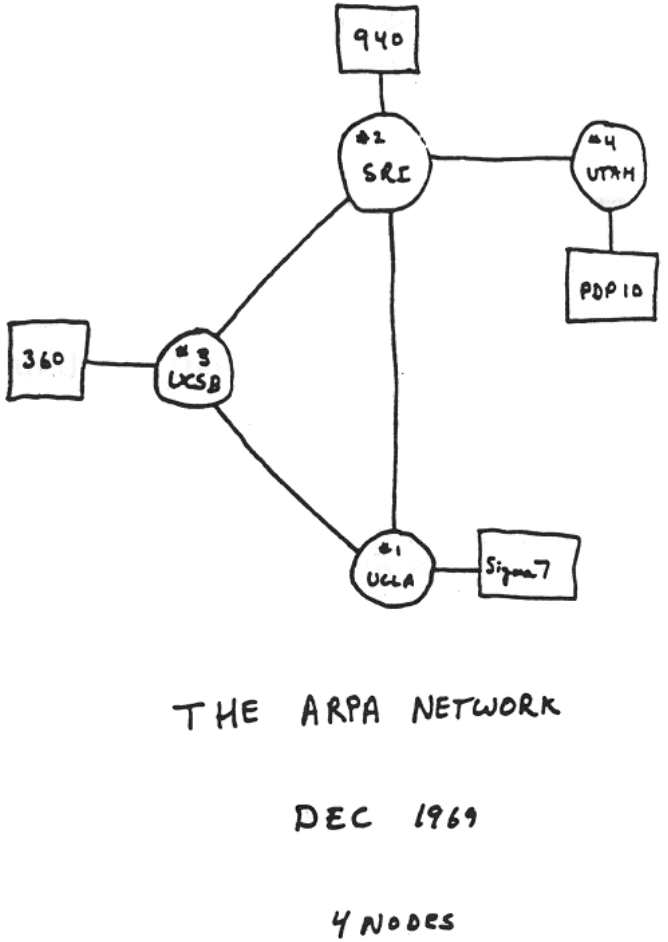
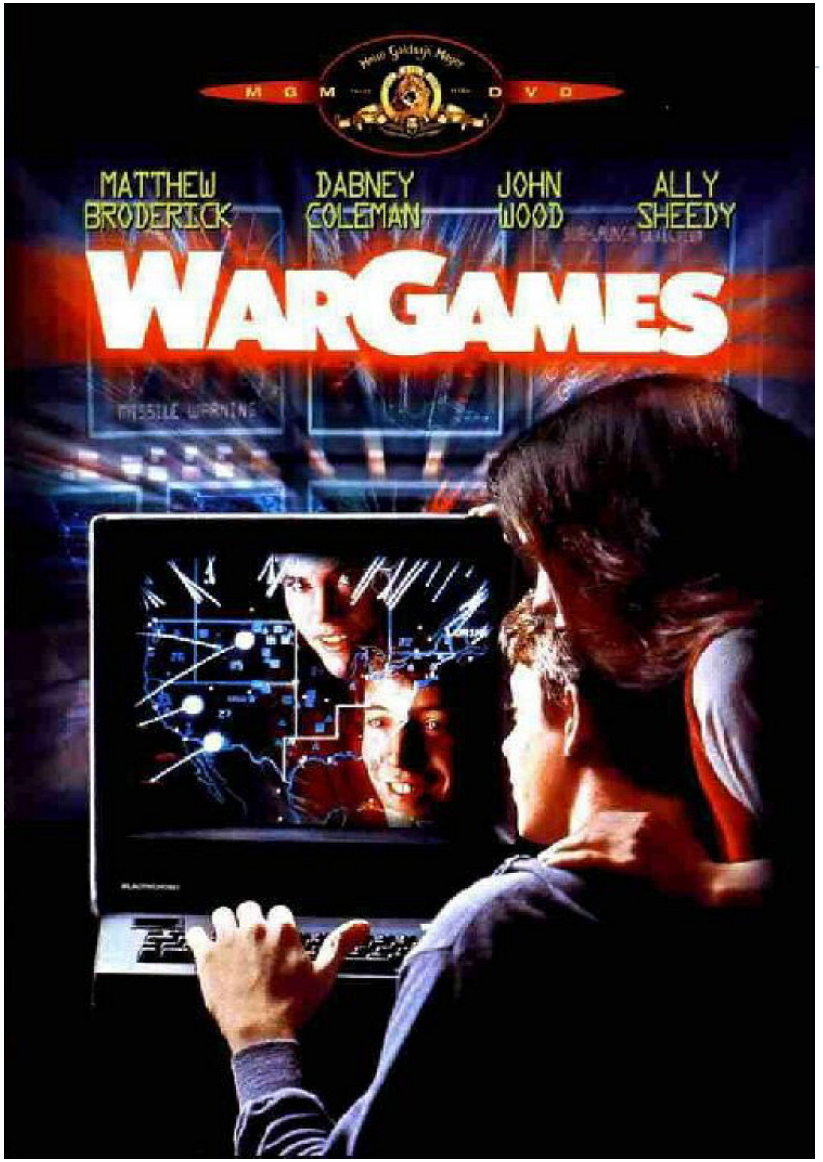



**FIGURE 6.2** Drawing of 4 Node Network (Courtesy of Alex McKenzie)




# 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

# First computer virus

- 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

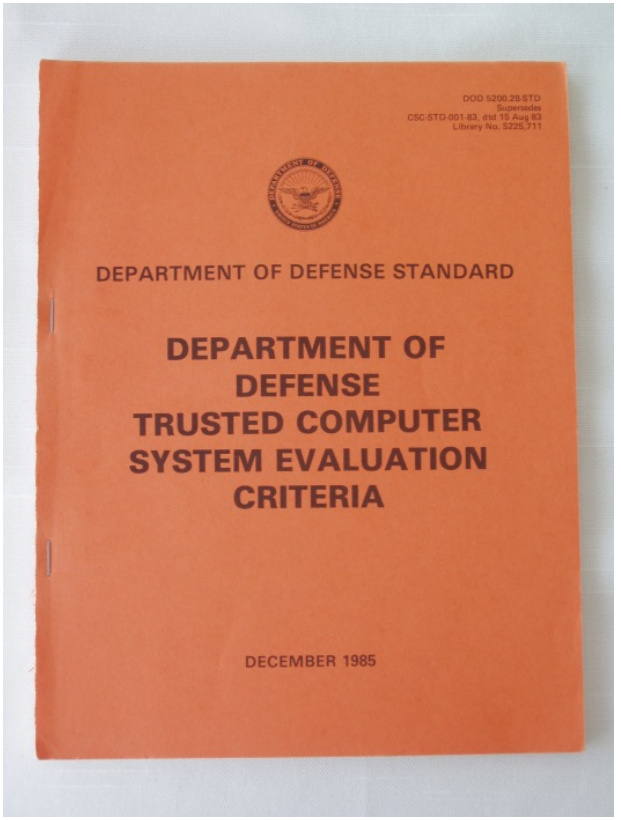
- 1999 – Melissa macro virus spreads via email attachments
- 2000 – ILOVEYOU virus released, infects millions of machines in hours
  - One of the first widespread uses of social engineering tactics
- 2000 – 15-year old "mafiaboy" invents the Denial of Service attack
  - Causes millions of damage to e-commerce 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 ceriously

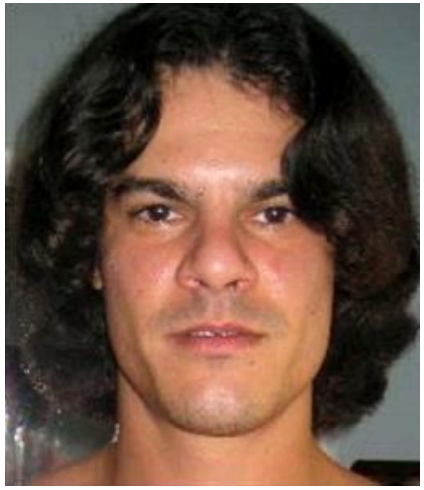
- 1987 – McAfee releases first version of VirusScan
- 1995 – Mozilla releases the Secure Socket Layer (SSL) protocol which later will become TLS
- 2001 – NIST standardizes the Advanced Encryption Standard (AES)
- 2002 – Bill Gates launches Microsoft's "Trustworthy Computing" initiative
  - Security, 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

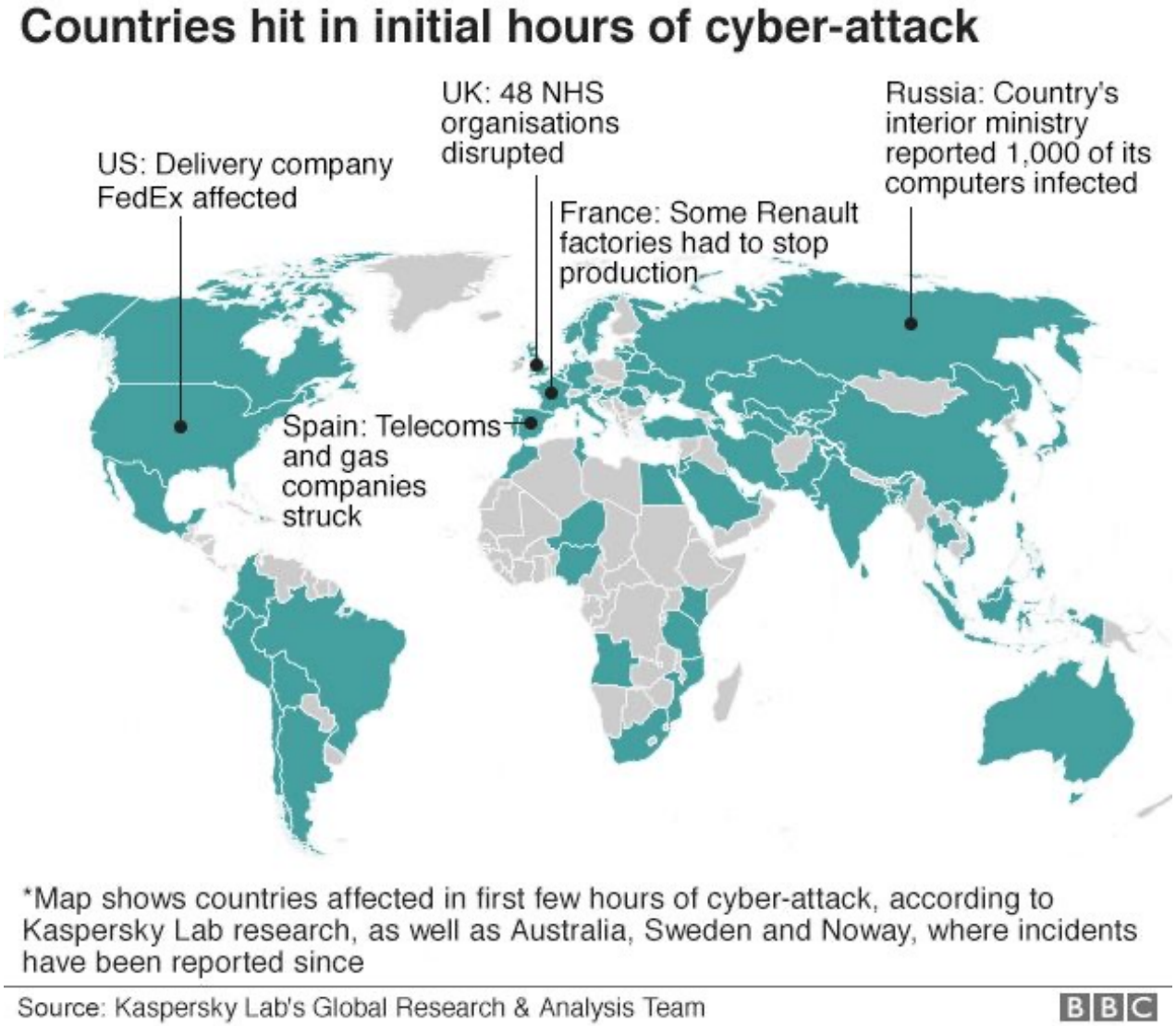
- 2005 – Albert Gonzalez steals 46 million credit cards from TJ Maxx
- 2006 – The Russian Business Network (RBN) comes online
  - Offered bulletproof hosting for criminal enterprises
- 2007 – Storm worm turns infected machines into a botnet
- 2007 – First version of Zeus banking trojan released



# Inklings of cyberwarfare

- 2009 – Chinese hackers from PLA Unit 61398 perform "Operation Aurora"
  - Serious of hacks against US government and industry targets
  - Google was targeted
- 2010 – US and Israel attack nuclear centrifuges in Iran with the Stuxnet worm
  - Designed to jump over air-gapped networks
  - Causes centrifuges to spin out of control, but report no anomalies
  - To this day, parts of the code are undeciphered
- 2011 - RSA attack, part of an espionage group uncovered by the Mandiant APT 1 report
- 2014 – "Guardians of Peace" attack Sony Pictures
  - Destroy computers, leak confidential files and unreleased movies
  - Believed to be North Korean hackers

# Self-Propagating ransomware




WannaCry ransomware

- 200K infected machines
- 150 countries
- May 12- May 15, 2017

55

# Present and 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

# Class topics

# Topics

- Cryptography
- Passwords and authentication
- Ethics
- Systems security
- Web security
- Internet security
- Wireless security
- Privacy: anonymous communication, data privacy