Fundamentals of Information & Network Security
ECE 471/571

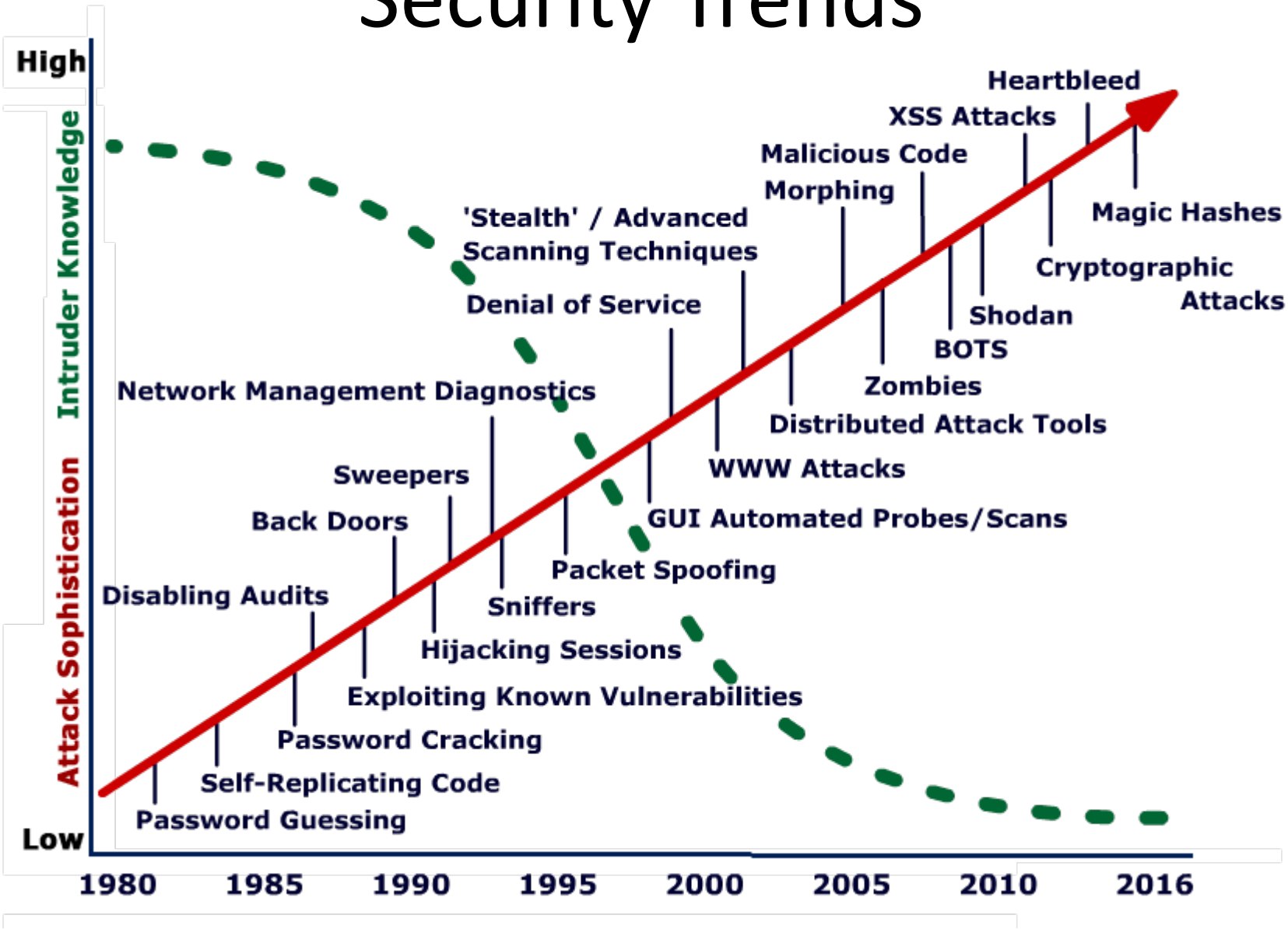
Lecture #1: Introduction to Information and Network Security

Instructor: Ming Li
Dept of Electrical and Computer Engineering
University of Arizona

Why Study Security?

- People attack systems and do damage
  - Why do they do it?
    - Financial motivation
    - Religious/political motivation
    - Industrial espionage
    - Angry employees
    - Bored teenagers
    - ….
  - How do they do it?
    - Network attacks
    - Exploit vulnerabilities in applications and security mechanisms
    - Physical access
    - ….
  - Whom do they attack?
    - Banks
    - Government agencies
    - E-commerce web sites
    - Hollywood
    - Universities (play ground)
    - ….

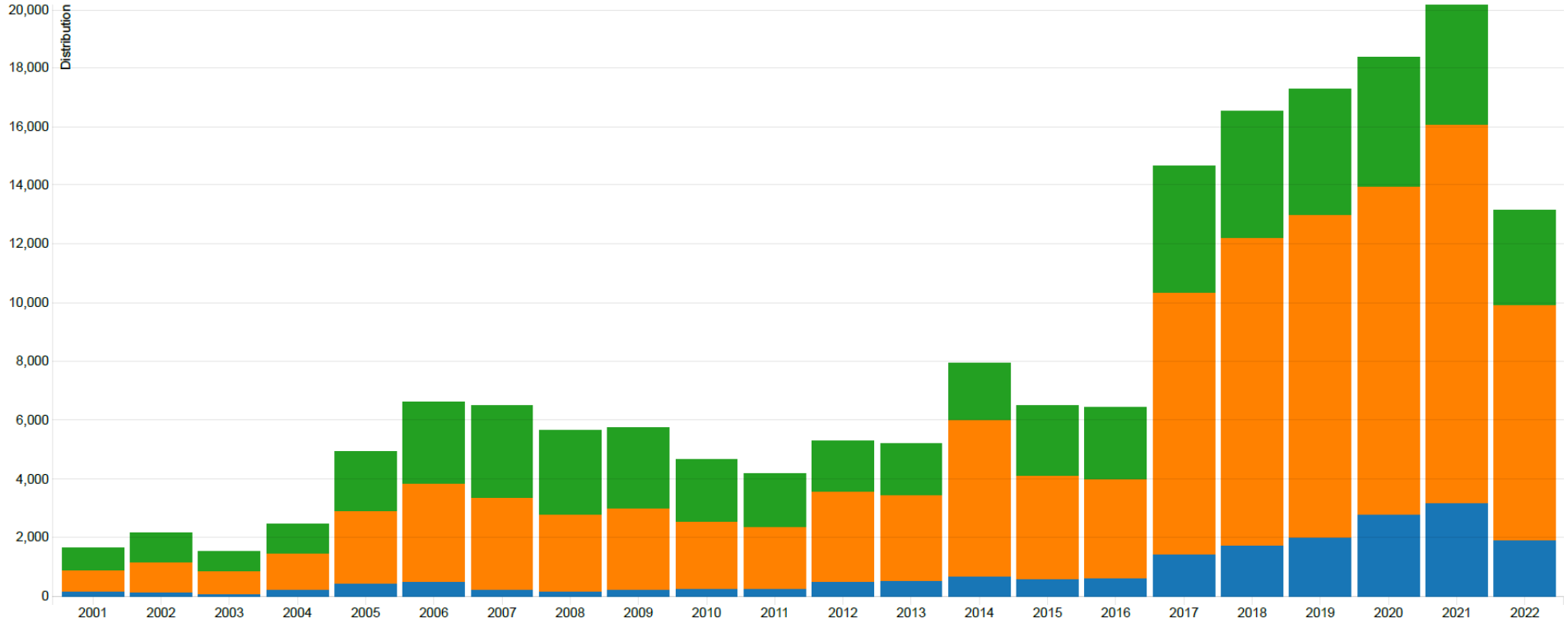
Security Trends



T. Takebe, “Trends in Industrial Standards and International Standards for Industrial Automation Contro
System Security,” Yokogawa Technical Report English Edition Vol.57 No.2, 2014.

How big is the problem?

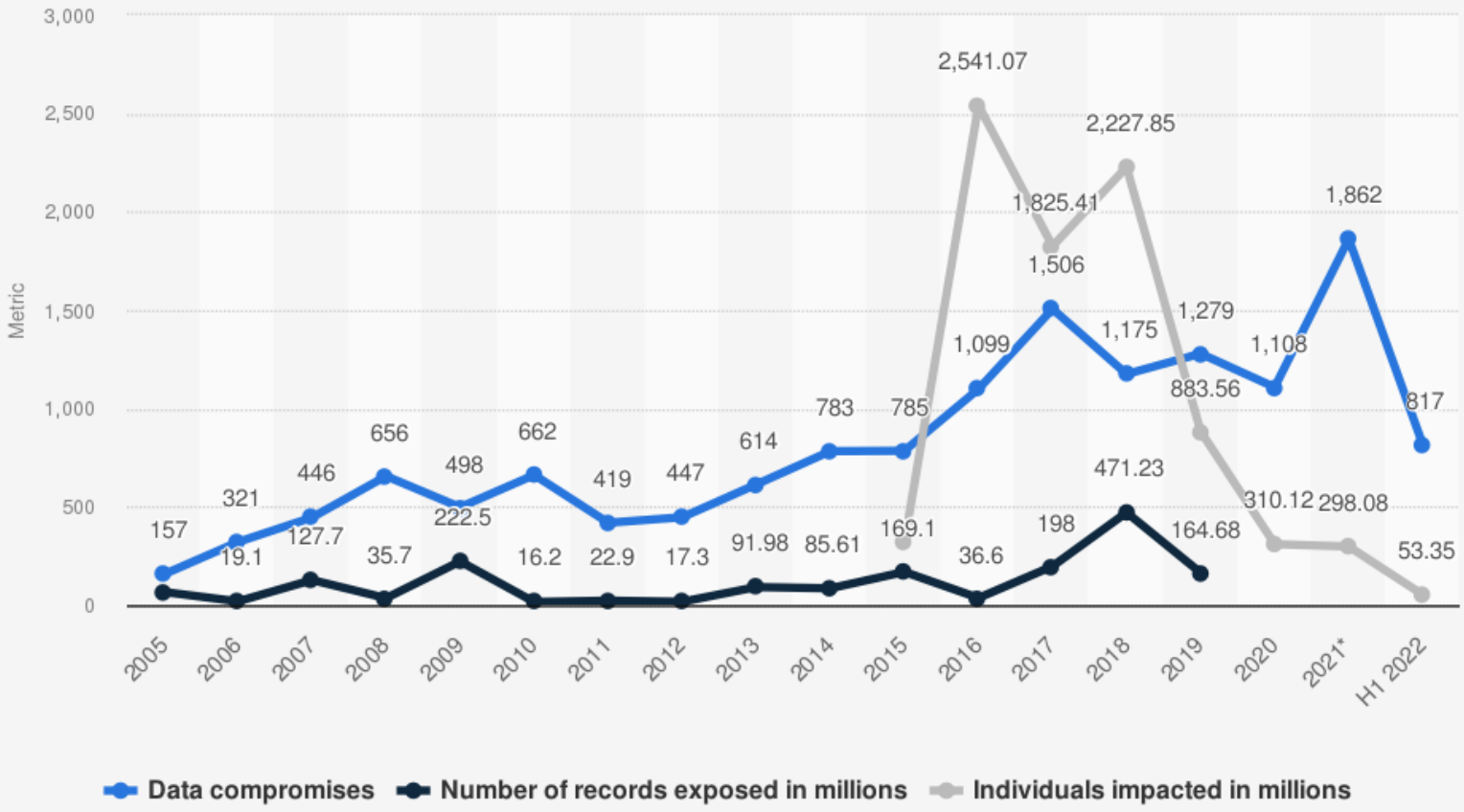
CERT Vulnerabilities reported



https://nvd.nist.gov/general/visualizations/vulnerability-visualizations/cvss-severity-distribution-over-time
https://www.kb.cert.org/vuls/

How big is the problem?

1. Y… …ail a…
2. M… …ort n…
3. E… d…
4. T… …party H… m…
5. U… (2…

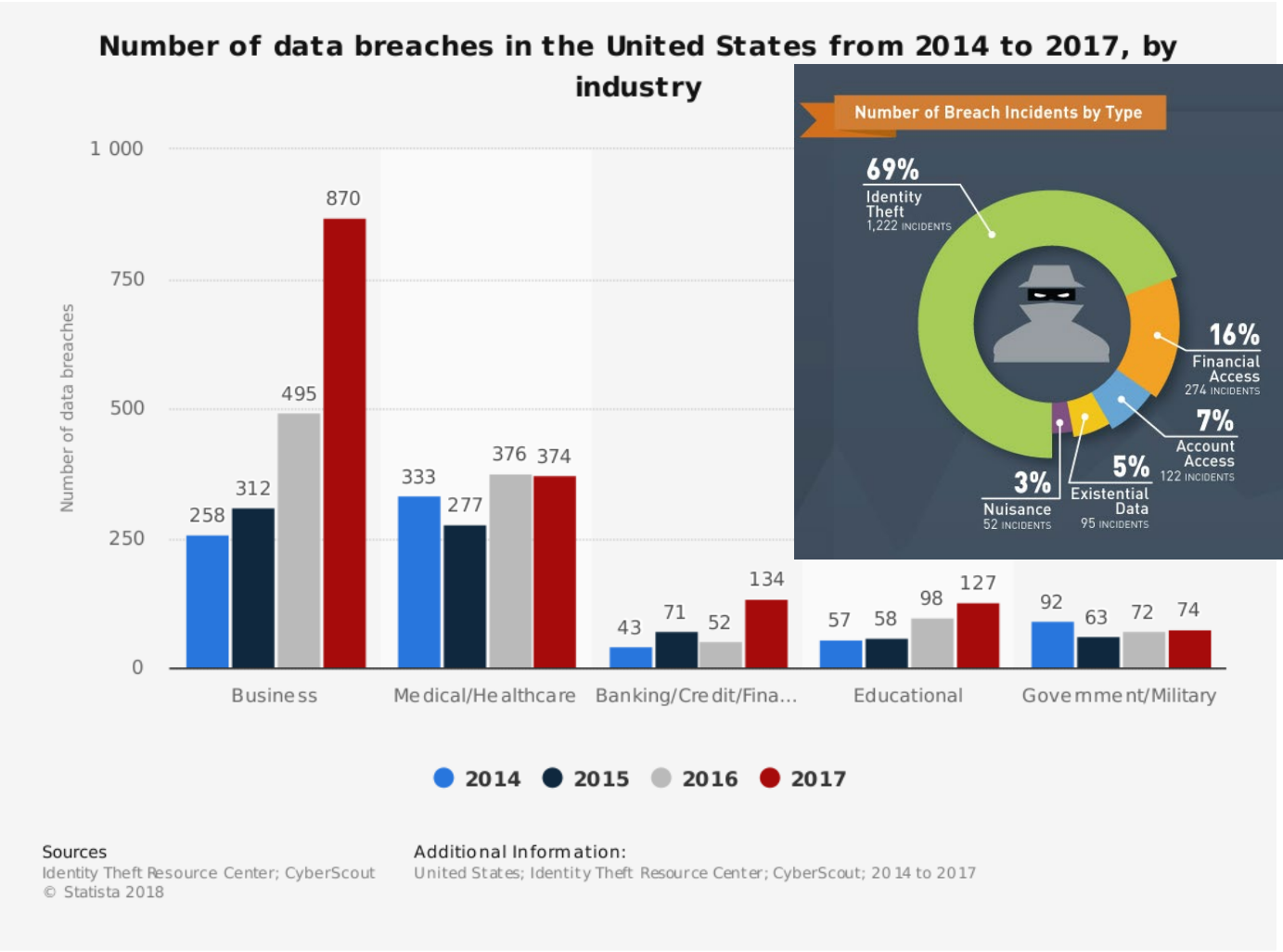


Source
Identity Theft Resource Center
© Statista 2022

Additional Information:
United States; Identity Theft Resource Center; 2005 to H1 2022; data compromises include data breaches, data exposure… impacted may go beyond the United States

How big is the problem?

Data Breach Incidents reported



How big is the problem? (cont'd)

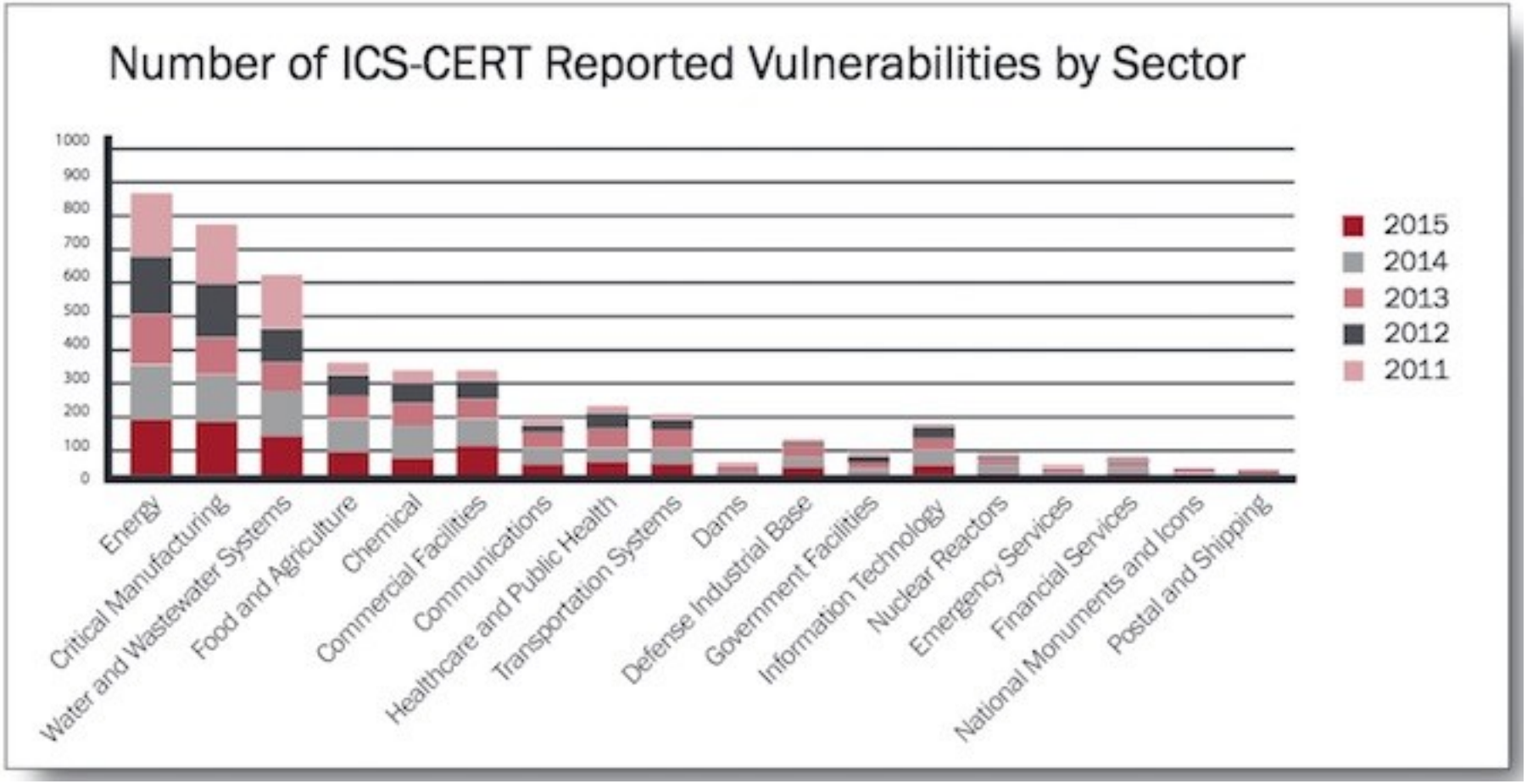
- Internet attacks are increasing in frequency, severity, and sophistication
- Denial of service (DoS) attacks
  - Cost $1.2 billion in 2000
  - Yahoo, Amazon, eBay, Microsoft, White House, etc., attacked
  - Recent significant DoS attacks:
    - The Google Attack, 2020 (2.5 Tbps peak traffic!)
    - The AWS DDoS Attack in 2020
    - The Mirai Dyn DDoS Attack in 2016
      - infiltrated IoT devices, 600K infected, 600Gbps traffic, led to Dyn attack, disrupted websites: Airbnb, GitHub, Netflix, Twitter, etc.
    - The GitHub Attack in 2018
    - A European Gambling Company, 2021

https://www.a10networks.com/blog/5-most-famous-ddos-attacks/

How big is the problem?(cont'd)

- In first half year of 2005, 237 million network attacks launched
  - IBM Global Business Security Index Report
- In 2005, U.S. businesses lost 67.2 billion dollars due to attacks
  - 2006 Computer Crime and Security Survey by FBI and CSI
- Virus and worms
  - Melissa, Nimda, Code Red, Code Red II, Slammer, Stuxnet, Flame, ILOVEYOU…
  - Cause over $28 billion in economic losses in 2003, growing to over $75 billion in economic losses by 2007.
  - Code Red (2001): 13 hours infected >360K machines - $2.4 billion loss
  - Slammer (2003): 10 minutes infected > 75K machines - $1 billion loss
  - CryptoLocker (2013): ransomeware, 500,000 victims, cost $30M in 100 days;
  - WannaCry ransomware attack (2017): spreads globally, uses NSA exploit
  - Stuxnet (2010): SCADA in nuclear plants; may destroy the centrifuge

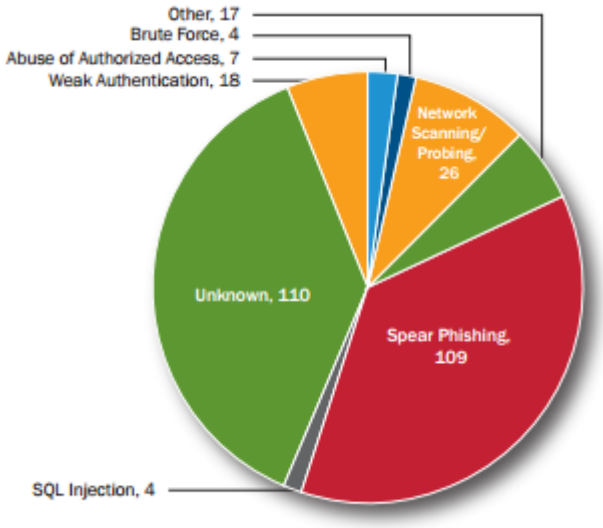
How Serious is the Problem?



E.g., December 2015 Ukraine power grid cyberattack: 230K people were left without electricity for a period from 1 to 6 hours
https://en.wikipedia.org/wiki/December_2015_Ukraine_power_grid_cyberattack

Why does this happen?

- Lack of encryption and secure protocol design
- Lots of buggy software...
- Some contributing factors
  - Few courses in computer security
  - Programming text books do not emphasize security
  - Few security audits
  - C is an unsafe language
  - Programmers are lazy
  - Legacy software
  - Security mechanisms are difficult to use
  - Security is expensive and takes time
- Insider threat
  - Easy to hide code in large software packages
  - Difficult to discover hidden malicious code
  - strict development rules and physical security help
- Human Factors
  - Social engineering



ICS attack vector breakdown

Security has become one of the hottest jobs even with downturn of economy

Example Security Incident: The Stuxnet Worm (2010)

- Targeted Iranian nuclear power plants.
- Is the first discovered malware that spies on and subverts industrial systems (supervisory control and data acquisition (SCADA))
- “The attacks seem designed to force a change in the centrifuge’s rotor speed, first raising the speed and then lowering it, likely with the intention of inducing excessive vibrations or distortions that would destroy the centrifuge.”
- The Stuxnet worm is initially spread using infected removable drives such as USB flash drives.
- http://en.wikipedia.org/wiki/Stuxnet

Notions of Security

Think as many concepts as you can relate to security in our everyday world

E.g., Add a lock to a door to control entry access
E.g., Add a watermark to a bank note to prevent counterfeiting

E.g., Hieroglyphics in ancient Egypt - a form of encryption