Outline

- General Introduction

Announcements – cont.

- About this class
  - In-person attendance is required and is part of the grading
  - You need to participate the class discussion by sharing your thinking and ideas and is part of the grading as well

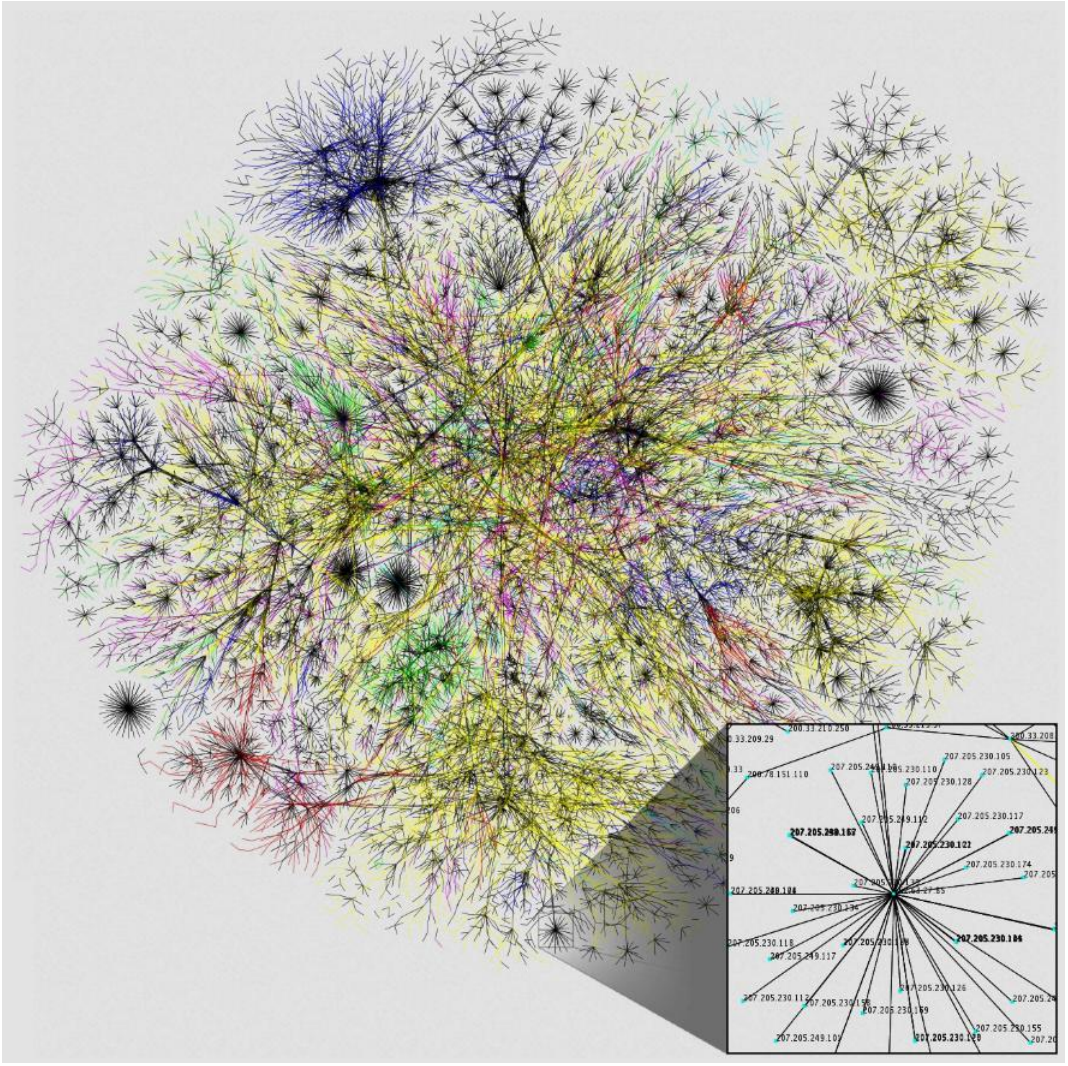
Announcements – cont.

- About the assignments
  - Homework assignments and quizzes
  - Hands-on exploitation projects
  - CTF Competitions

Questions to Be Asked

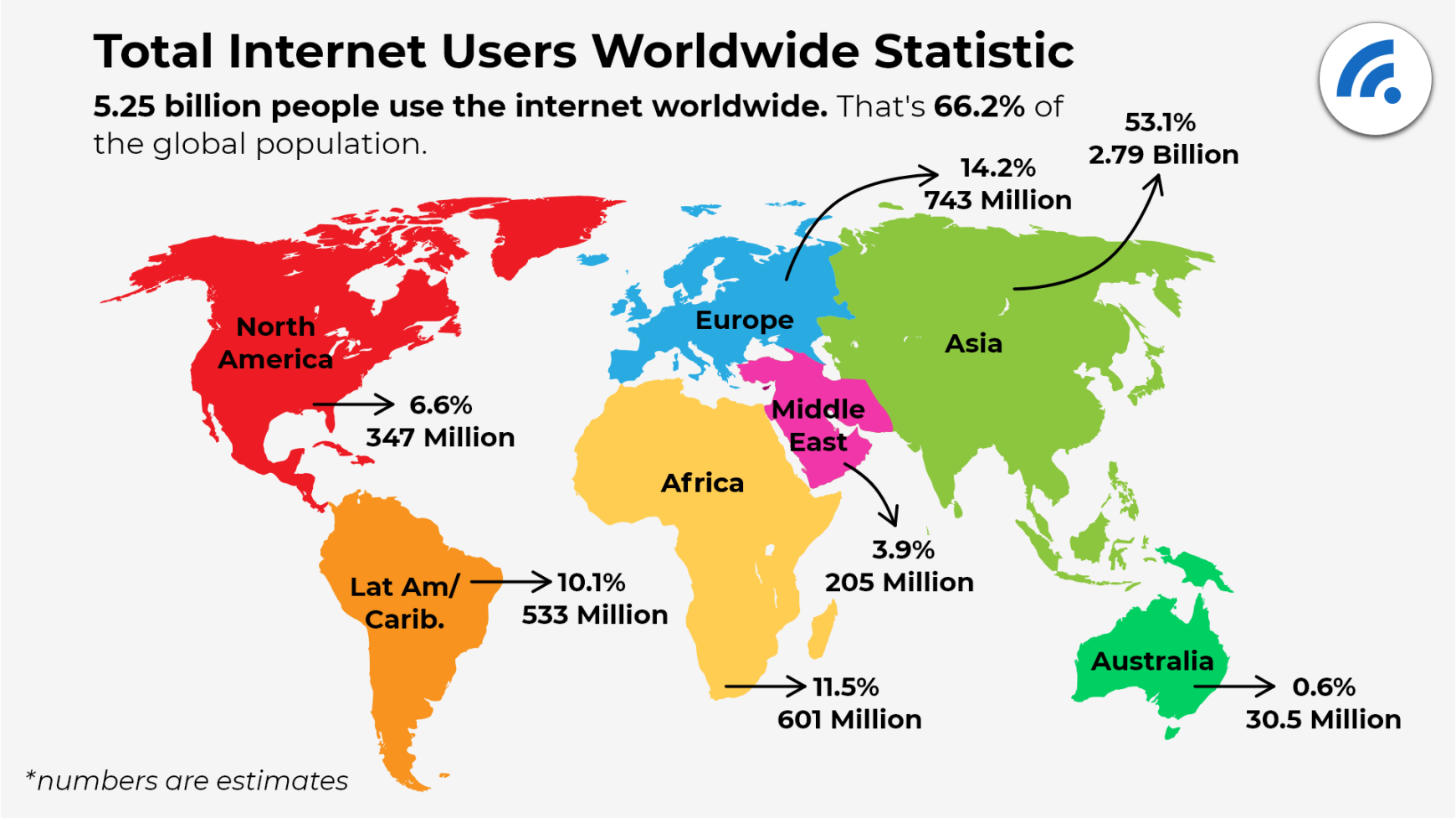
- Is computer security all about cryptography?
  - Fortunately, no. Cryptography provides one of the fundamental tools for people to solve computer security problems toward more secure systems. As in any other system implementation, it involves policy (specifications), implementation, testing, and many other system and engineering issues.
- How is this class related to cryptography?
  - As there are a number of other courses that cover cryptography, this courses focuses on how to attack implementations of cryptography systems.

The Internet



Source: https://upload.wikimedia.org/wikipedia/commons/3/3f/Internet_map_1024_-_transparent%2C_inverted.png

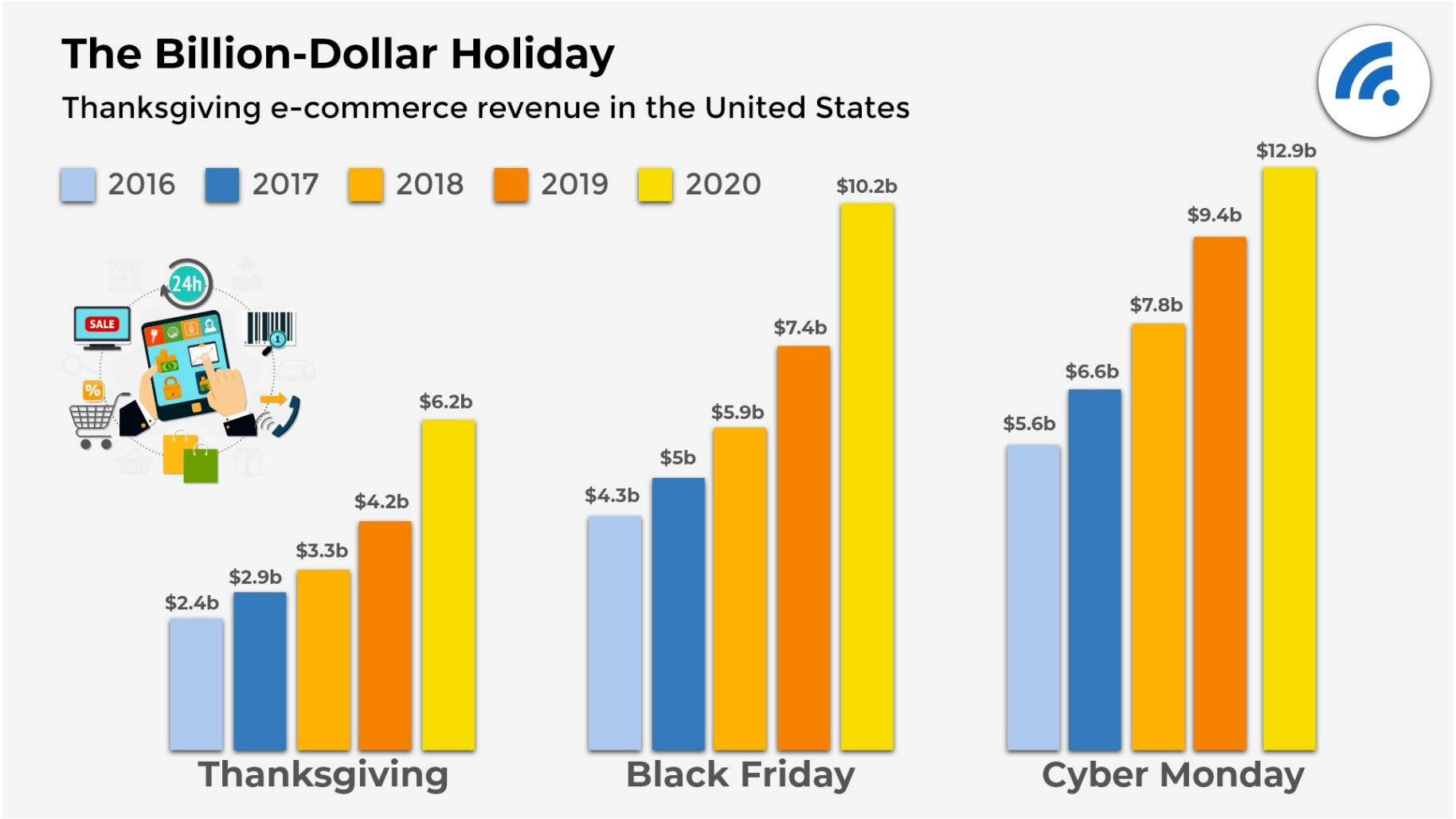
Internet and Its Usage



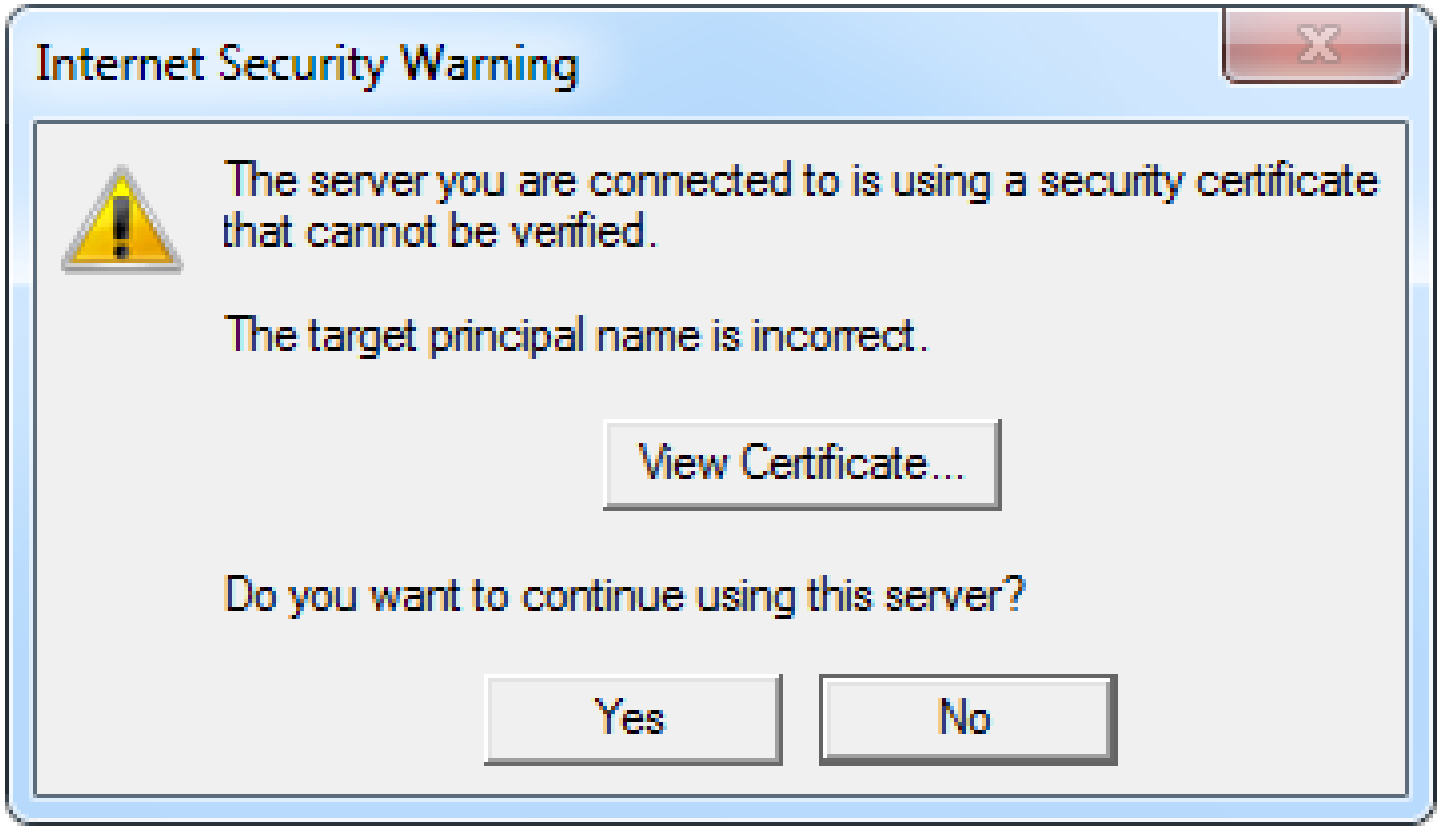
Source: https://www.broadbandsearch.net/blog/internet-statistics#post-navigation-0

Internet and Its Usage – cont.

People Are Increasingly Shopping Online



Common Internet Problems



- What shall you do and why?

Internet and Its Usage – cont.

- Critical infrastructure vulnerability and protection

Researchers who launched an experimental cyber attack caused a generator to self-destruct, alarming the government and electrical industry about what might happen if such an attack were carried out on a larger scale, CNN has learned.

Sources familiar with the experiment said the same attack scenario could be used against huge generators that produce the country's electric power.

Some experts fear bigger, coordinated attacks could cause widespread damage to electric infrastructure that could take months to fix.

CNN has honored a request from the Department of Homeland Security not to divulge certain details about the experiment, dubbed "Aurora," and conducted in March at the Department of Energy's Idaho lab.

http://articles.cnn.com/2007-09-27/us/power.at.risk_1_generator-experiment-cnn?_s=PM:US

Value of Computer Security

Source: http://i.telegraph.co.uk/multimedia/archive/02544/Graph_2544313b.jpg

Security Bounty Programs – cont.

- You could become rich by finding bugs

1. **Stéphane Chazelas**

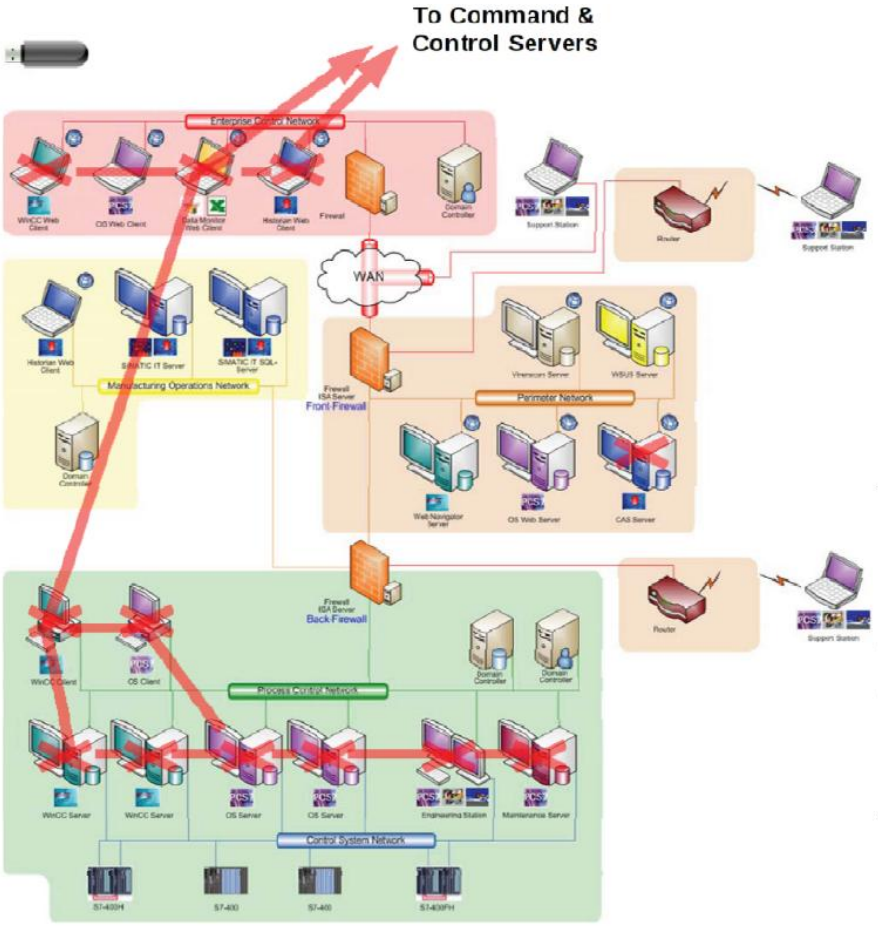
> **Stéphane is a *nix and Telecom Specialist who discovered the GNU Bourne-Again Shell (Bash) Shellshock vulnerability. He is also involved in the UNIX and Free Software/Open Source community (writings, contributions to projects). He reported Shellshock in Hackreone and was rewarded with $20,000 USD for his responsible disclosure.**

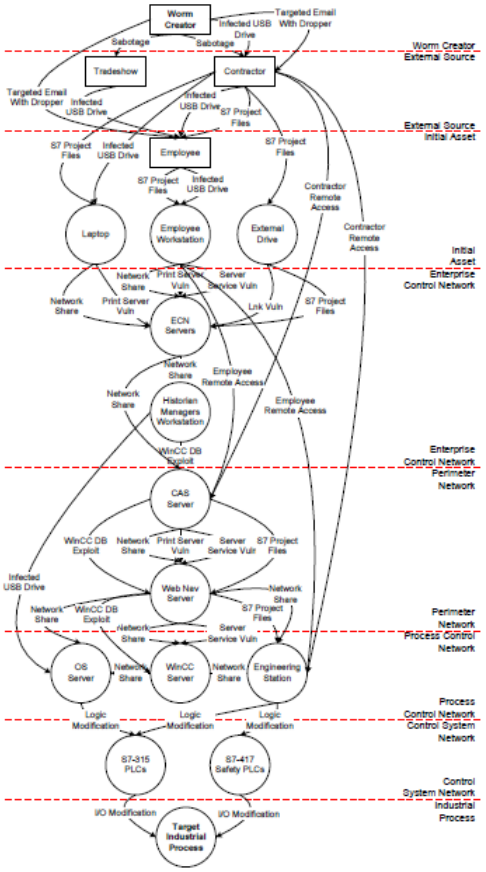
2. **Rafay Baloch**

> Rafay is a Pakistani independent security researcher who owns rafayhackingarticles.net. He once found a remote code execution vulnerability inside PayPal for which he was awarded $10,000 USD and also was offered a job by PayPal, but turned down the job offer. Rafay is an active participant in bug bounty programs and is listed in large number of hall of fames including Google, Facebook Microsoft, Twitter, and Dropbox. He is best known for discovering Android Stock Browser Address Bar Spoofing, which affected Android Lollipop and previous versions.

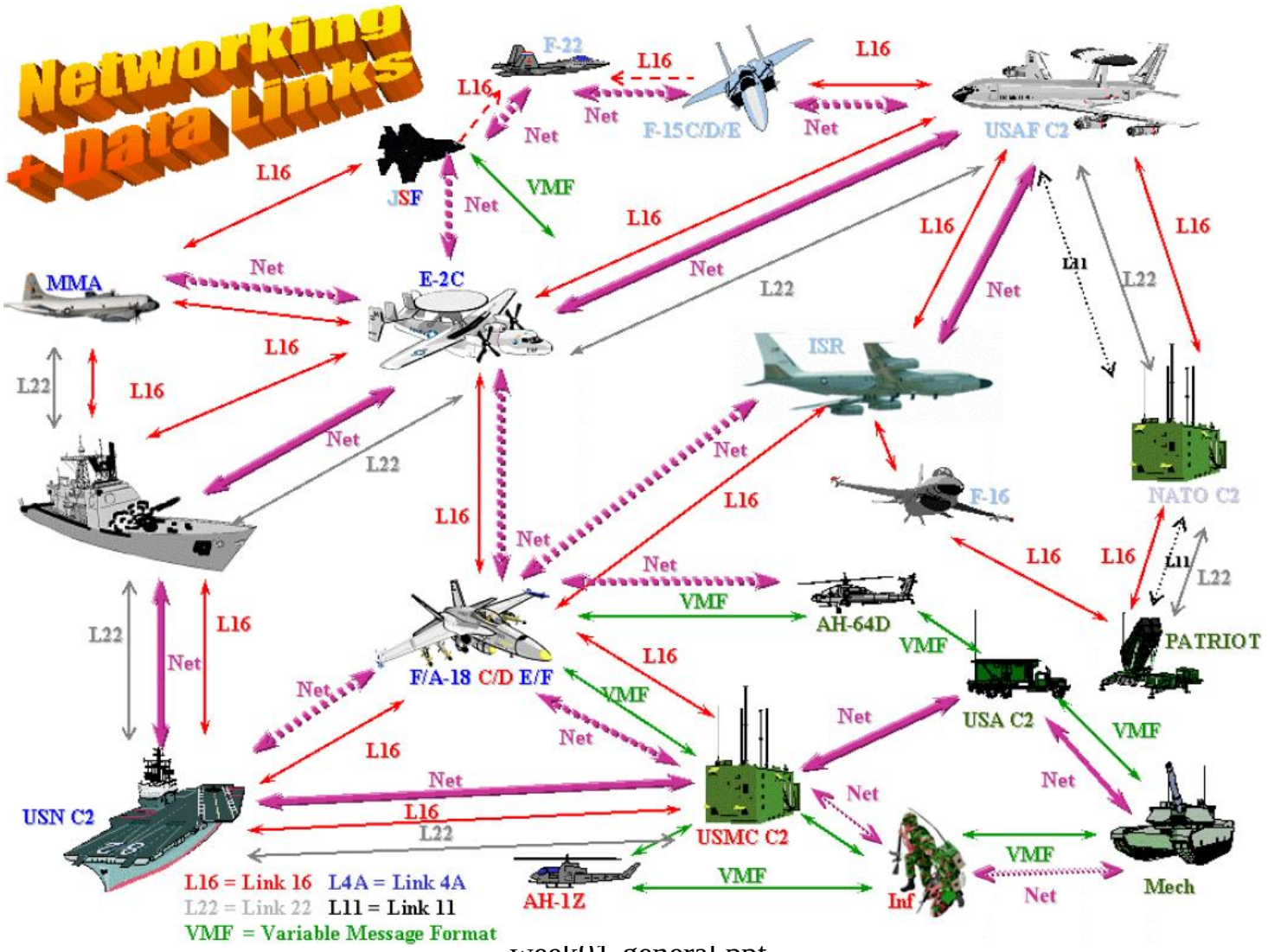
Stuxnet

- This probably is the most sophisticated worm
  - It was created to compromise nuclear facilities





Next-Generation Weapon Systems



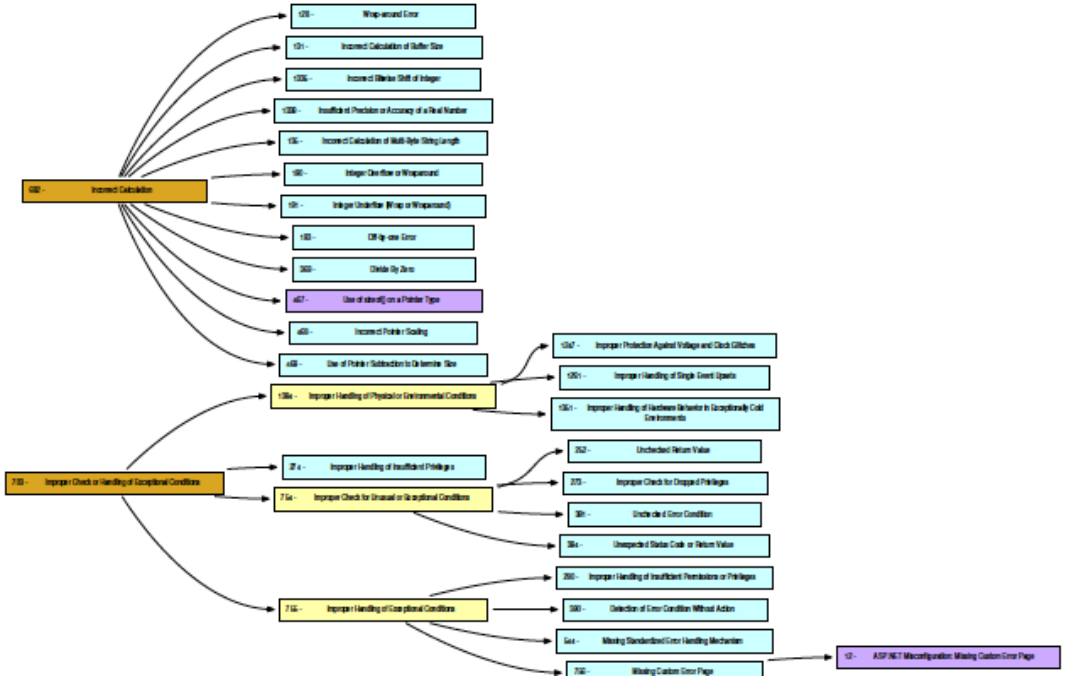
Source: http://idlsoc.com/Documents/Symposiums/IDLS2009/Day2/D2_MAIN_US_TDES_Migration_Panel_Moderator_David_Nark_Narkevicius_OASD%28NII%29.pdf

Why Do We Have So Many Breaches

- Software has bugs and some can be exploited
- (A lot of) money could be made by malicious entities
- Often people are not aware of the dangers
  - "Freedom, Security, Convenience: Choose Two"

Common Weakness Enumeration

- There are 927 different types of weakness
  - The latest version, which has 2463 pages, can be downloaded from https://cwe.mitre.org/data/published/cwe_latest.pdf



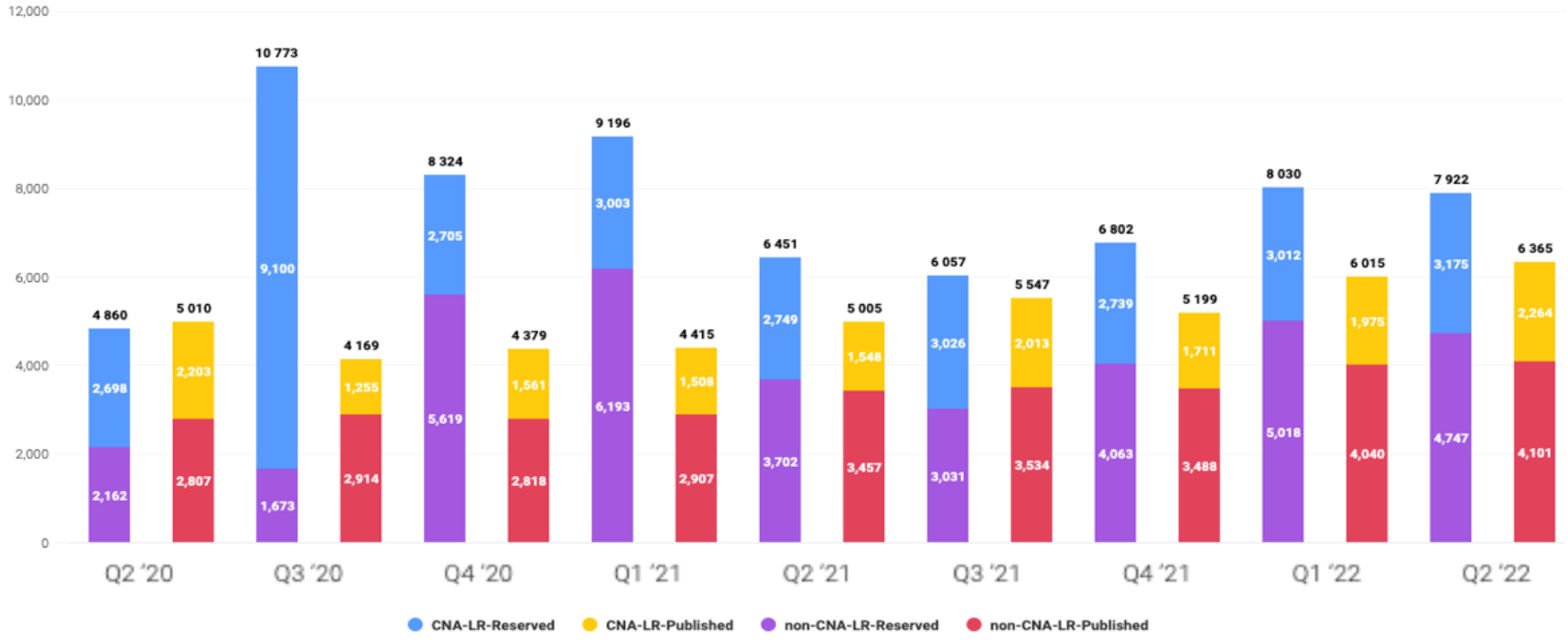
Common Vulnerabilities and Exposures

- TOTAL CVE Records: 192510
  - As of January 9th, 2023

Format	Unix compressed (.Z)	Gzipped (.gz)	Raw	Other
CSV	allitems.csv.Z	allitems.csv.gz	allitems.csv	NOTE: suitable for import into spreadsheet programs
HTML	allitems.html.Z	allitems.html.gz	allitems.html	
Text	allitems.txt.Z	allitems.txt.gz	allitems.txt	
XML	allitems.xml.Z	allitems.xml.gz	allitems.xml	cve_1.0.xsd

CVRF	All CVE Records	By Year
(Learn more about CVE and CVRF)	All records - Raw (cvrf.xml)	CVE-2022-xxxxxx records CVE-2021-xxxxxx records CVE-2020-xxxxxx records CVE-2019-xxxxxx records CVE-2018-xxxxxx records CVE-2017-xxxxxx records CVE-2016-xxxxxx records CVE-2015-xxxxxx records CVE-2014-xxxx records CVE-2013-xxxx records CVE-2012-xxxx records CVE-2011-xxxx records CVE-2010-xxxx records CVE-2009-xxxx records CVE-2008-xxxx records CVE-2007-xxxx records CVE-2006-xxxx records CVE-2005-xxxx records CVE-2004-xxxx records CVE-2003-xxxx records CVE-2002-xxxx records CVE-2001-xxxx records CVE-2000-xxxx records CVE-1999-xxxx records

Common Vulnerabilities and Exposures



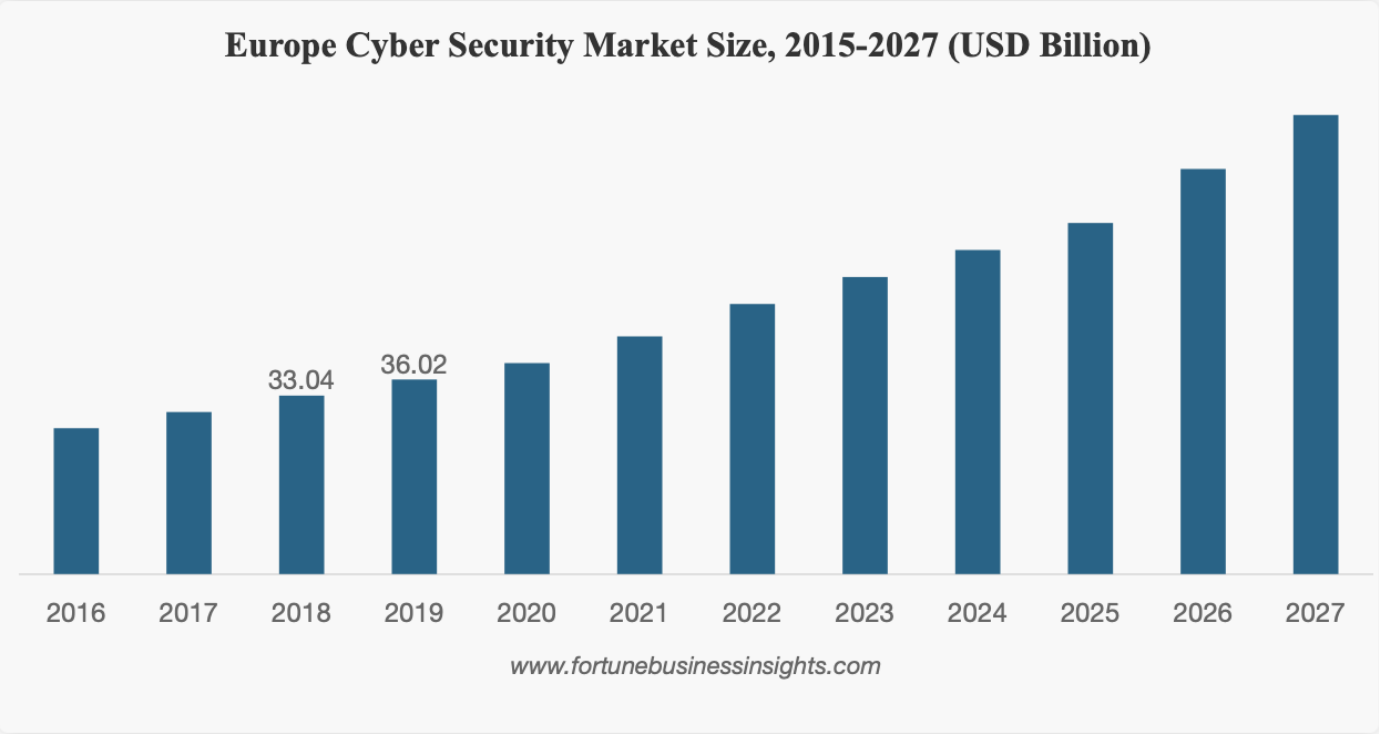
"Zero Days, Thousands of Nights"

There is an ongoing policy debate over whether the U.S. government—or any government—should retain so-called zero-day software vulnerabilities or disclose them so they can be patched.[1] Those who have knowledge of a zero-day vulnerability may create "exploits"—code that takes advantage of the vulnerability—to access other parts of a system, execute their own code, act as an administrator, or perform some other action, but many worry that keeping these vulnerabilities secret can expose people who use the vulnerable software to malware attacks and other attempts to collect their private information. Furthermore, cybersecurity and the liability that might result from attacks, hacks, and data breaches using zero-day vulnerabilities have substantial implications for U.S. consumers, companies, and insurers, and for the civil justice system broadly.

The debate of whether to retain or disclose these vulnerabilities is often fueled by how much overlap there might be between the zero-day vulnerabilities or exploits the U.S. government keeps and those its adversaries are stockpiling. If both sides have the same stockpiles, then some argue that there is little point to keeping them private—whereas a smaller overlap might justify retention. But without information on the overlap, or concrete metrics based on actual data, it is challenging to make a well-informed

Cyber Security as an Industry

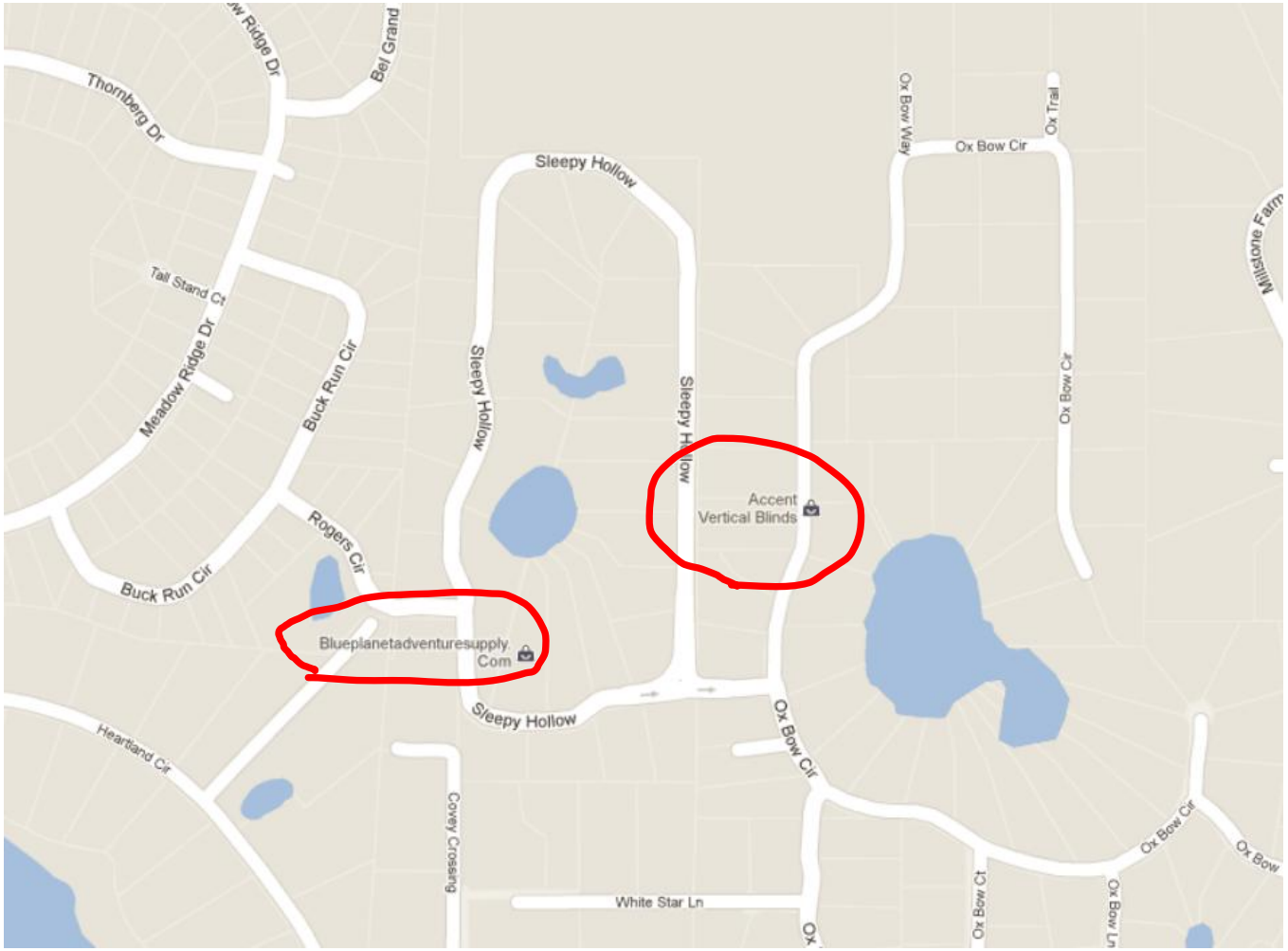
- It is a multi-billion industry that is expected to grow steadily
  - In addition, security has become a top priority of software development companies



http://www.marketresearchmedia.com/2009/05/25/us-federal-cybersecurity-market-forecast-2010-2015/

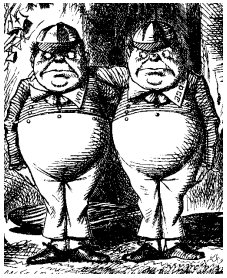
Creating an Online Store

- Due to the availability of Internet connections, one trend is to establish an online store to sell specialized products



The Cast of Characters

- Alice and Bob are the good guys



- Trudy is the bad guy
- Trudy is our generic “intruder”
- Note that they do not have to be real people

Securing Multi-User Systems

- Cyber security issues are practical
  - For example, how we can secure a multi-user system like linprog.cs.fsu.edu?
    - As a simple example, how to manage passwords of users securely and efficiently?

```
liux:x:1001:1001:Xiuwen Liu,,,:/home/liux:/bin/bash
fwupd-refresh:x:128:134:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
luwei:x:1002:1002:luwei,,,:/home/luwei:/bin/bash
mendelso:x:1003:1003:mendelso,,,:/home/mendelso:/bin/bash
```

Securing Multi-User Systems

- Cyber security issues are practical
  - For example, how we can secure a multi-user system like linprog.cs.fsu.edu?
    - As a simple example, how to manage passwords of users securely and efficiently?

```
liux:x:1001:1001:Xiuwen Liu,,,:/home/liux:/bin/bash
fwupd-refresh:x:128:134:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
luwei:x:1002:1002:luwei,,,:/home/luwei:/bin/bash
mendelso:x:1003:1003:mendelso,,,:/home/mendelso:/bin/bash

messi:$6$H7z$oG3h02shEWubDF8U1tgbB0xPJ/RrrQKcFq4qL8ZyJXSUtsbF3vczr5QlHfnuxAoanvvya/9rjD3AN
sshd:*:19186:0:99999:7:::
liux:$6$6mQ65TuIxbVuq5eC$HZjJF/7jTsWMBNS8YMgMz1UdB3RbI/o7hpaHuToiN/dfSeAavgADQFQdYZRXHgpOS
fwupd-refresh:*:19325:0:99999:7:::
luwei:$6$RZo8Xn9HbDOs.Oel$VvWuG8Qc9jqDKp1p0J4rYvRqrTViIznJ1T8ELdBrO1HYUSF5a8PwKkAXtWaCooS4
mendelso:$6$4C89/4lnMWeXWHQ.$z2xgEVGKoBO57MYOkHACfl.oK5wVN8SzyNtuAauyF6CyufggKOq88RhSAl/Ei
```

Need for Privileged Programs

- Password Dilemma
  - Permissions of /etc/shadow File:

```
-rw-r----- 1 root shadow 1443 May 23 12:33 /etc/shadow
```

Only writable to the owner

  - How would normal users change their password?

```
root:$6$012BPz.K$fbPkT6H6Db4/B8cLWbQI1cFjn0R25yqtqrSrFeWfCgybQWWnwR4ks/.rjqyM7Xw
h/pDyc5U1BWOzkWh7T9ZGu.:15933:0:99999:7:::
daemon:*:15749:0:99999:7:::
bin:*:15749:0:99999:7:::
sys:*:15749:0:99999:7:::
sync:*:15749:0:99999:7:::
games:*:15749:0:99999:7:::
man:*:15749:0:99999:7:::
lp:*:15749:0:99999:7:::
```

Authentication Methods

- A process to verify a user's identity
- Typical authentication methods
  - Based on something the **user knows**: password
  - Based on something the **user has**: ID card
  - Based on something the **user is or does**: fingerprint
- Multi-factor authentication

The Password File

- Each entry contains a user account information
- Password is not stored here (used to be)

```
root:x:0:0:root:/root:/bin/bash
seed:x:1000:1000:SEED,,,:/home/seed:/bin/bash
bob:x:1001:1001:Bob,,,:/home/bob:/bin/bash
alice:x:1002:1003:Alice,,,:/home/alice:/bin/bash
```

First Command After Login

- The last field of each entry

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
gdm:x:125:130:Gnome Display Manager:/var/lib/gdm3:/bin/false
seed:x:1000:1000:SEED,,,:/home/seed:/bin/bash
bob:x:1001:1001:Bob,,,:/home/bob:/bin/bash
alice:x:1002:1003:Alice,,,:/home/alice:/bin/bash
```

```
$ sudo su bin
This account is currently not available.
```

The Shadow File

- Store password, why not use /etc/password anymore?
- Structure for each entry

The Purpose of Salt

- Defeat brute-force attacks
  - dictionary attack, rainbow table attack
- These 3 accounts have the same password

```
seed:$6$n8DimvsbIgU0OxbD$YZ0h1EA...(omitted)...wFd0:18590:0:
alice:$6$.1CMCeSFZd8/8QZl$QhfhId...(omitted)...Sga.:18664:0:
bob:$6$NOLhqomO3yNwyFsZ$K.Ql/KnP...(omitted)...b8v.:18664:0:
```

Locking Account

- Putting an invalid value in the password field
- The root account is locked

```
root:!:18590:0:99999:7:::
```

Security Issues of mysecureonlinestore.com (MSOS)

- Suppose that you are the new owner of the MSOS store,
  - What are your security concerns?
  - How about your customers?
  - How about hackers?

Security Issues of mysecureonlinestore.com (MSOS)

- What are your security concerns?
  - How about your customers?
  - How about hackers?
- How can you define your security precisely?
  - Then how can you prove that the system you have satisfy your security requirements?
    - Note that your security depends on your computer systems as well as many other components (Internet and computers your customers use).

CIA

- Confidentiality, Integrity, and Availability
- You must prevent Trudy from learning Bob's account information
- **Confidentiality:** prevent unauthorized reading of information
  - More generally, prevent revealing information to unauthorized parties

CIA – cont.

- Note that confidentiality potentially involves many aspects

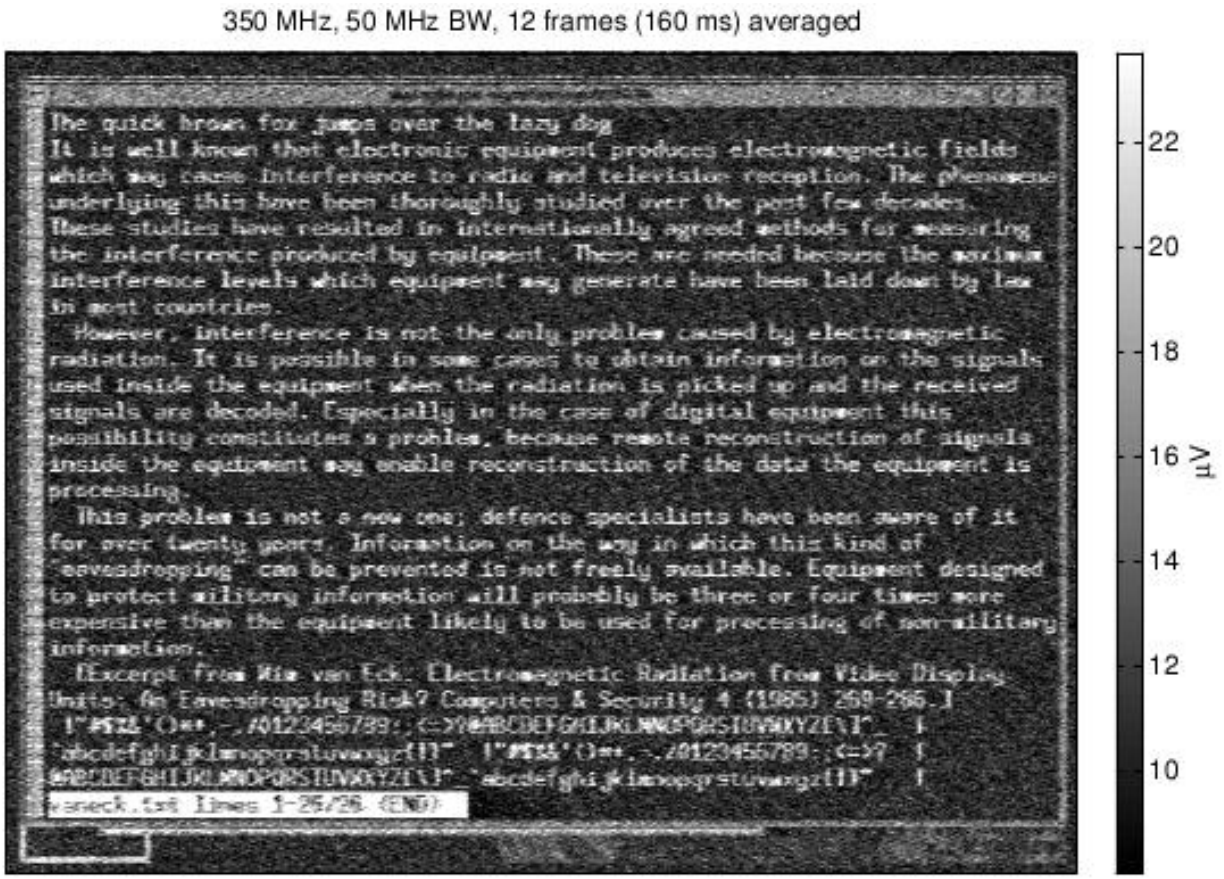


Figure 4.3: Text signal received from a 440CDX laptop at 10 m distance through two intermediate offices (3 plasterboard walls).

CIA – cont.

- Trudy must not be able to change Bob's order information
  - Bob must not be able to improperly change his own account balance
- **Integrity:** prevent unauthorized writing of information

CIA – cont.

- Your store information must be available when needed
- Alice must be able to make transactions
  - If not, she'll take her business elsewhere
- **Availability:** Data is available in a timely manner when needed
  - Availability is a "new" security concern
    - In response to denial of service (DoS)
  - We will discuss some methods to mitigate DoS attacks (for example, by using distributed servers)

Beyond CIA

- How does Bob's computer know that "Bob" is really Bob and not Trudy?
- Bob's password must be verified
  - This requires some clever **cryptography**
- What are security concerns of passwords?
- Are there alternatives to passwords?

Beyond CIA

- When Bob logs into MSOS, how does MSOS know that "Bob" is really Bob?
  - As before, Bob's password is verified
- Unlike standalone computer case, network security issues arise
  - What are network security concerns?
  - **Protocols** are critically important
- Crypto is also important in protocols

Beyond CIA – cont.

- Once Bob is *authenticated* by MSOS, then MSOS must restrict actions of Bob
  - Bob can't view Charlie's account info
  - Bob can't install new software, etc.
- Enforcing these restrictions is known as *authorization*
- **Access control** includes both authentication and authorization

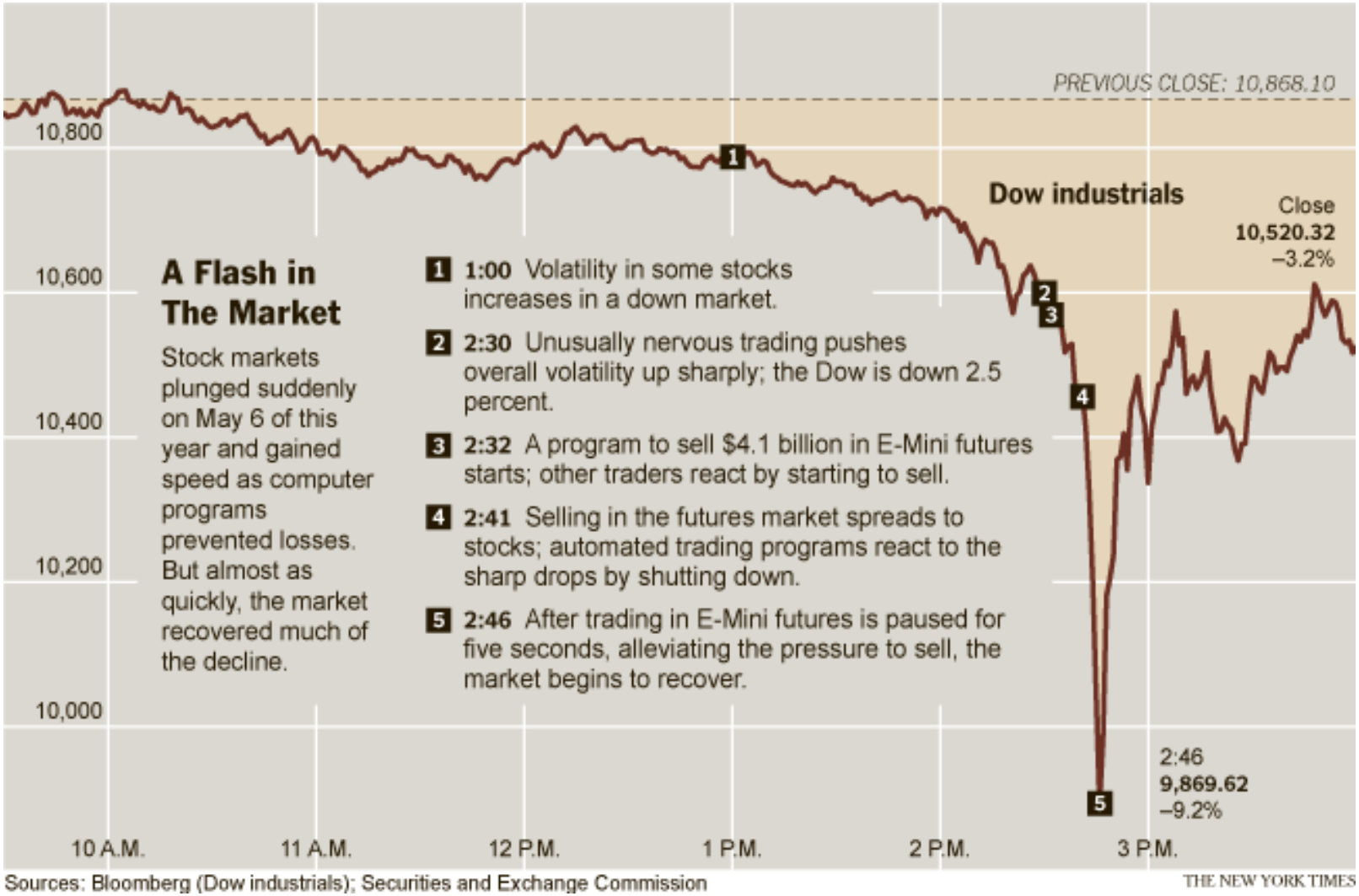
Beyond CIA – cont.

- For military applications, one of the worst authorization problems is "insider" threat
  - A current or former employee, contractor, or business partner who
    - has or had authorized access to an organization's network, system, or data and
    - intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems
  - How to prevent insider threat is an active research topic

Beyond CIA – cont.

- Cryptography, protocols, and access control are implemented in software
- What are security issues of software?
  - Most software is complex and buggy
  - Software flaws lead to security flaws
  - How to reduce flaws in software development?

Site Note: Flash Crash 2010



Beyond CIA – cont.

- Some software is intentionally evil
  - Malware: computer viruses, worms, etc.
- What can Alice and Bob do to protect themselves from malware?
- What can Trudy do to make malware more "effective"?

Beyond CIA – cont.

- Operating systems enforce security
  - For example, authorization
- OS: large and complex software
  - Win XP has 40,000,000 lines of code!
  - Subject to bugs and flaws like any other software
  - Many security issues specific to operating systems
    - Because kernel functions have many privileges that user programs do not have
  - Can you trust an OS?

Beyond CIA – cont.

- Suppose that you are in charge of a top-secret government program, your group needs to purchase security products
  - How can you make sure the products satisfy your security requirements?
    - How do you even approach the problem?
  - How do you make sure that the systems are configured correctly and always remain secure?

Beyond CIA – cont.

- Note that security related jobs are often considered as “unnecessary” overheads
  - Unless bad things happen to the systems
  - Security can be expensive
  - Security in practice depends heavily on the risk management of users and managers and the society
    - Such as laws to punish cyber crimes

Cyber Threats

- Adversaries and targets
- Motivations and techniques
- Types of cyber attacks

Information Assurance Fundamentals

- Threats and adversaries
- Vulnerabilities and risks
- Basic risk assessment
- Security life cycle
- Data security
- Access control models (MAC, DAC, and RBAC)
- Security mechanisms (identification/authentication, auditing)

Cyber Defense Principles and Practices

- Malicious activity detection
  - Forms of attack identification
  - Appropriate countermeasures
- Trust relationships
- Patching
  - OS and application updates
  - Vulnerability windows

Secure System Administration

- Security policy development
  - Password requirements
  - Password resetting mechanisms

This Class and The Textbook

- The textbook consists of four parts
  - They are organized around hands-on labs
  - We will cover selected chapters; however, we do not follow the book closely
    - As the book does not provide broader contexts in most cases and we will supplement the chapters with handouts and papers

Think Like Trudy

- In the past, no respectable sources talked about “hacking” in detail
- It was argued that such info would help hackers
- Very recently, this has changed
  - Books on network hacking, how to write evil software, how to hack software, etc.

Think Like Trudy

- Good guys must think like bad guys!
- A police detective
  - Must study and understand criminals
- In computer security
  - We want to understand Trudy's motives
  - We must know Trudy's methods
  - We'll often pretend to be Trudy

Think Like Trudy

- We must try to think like Trudy
- We must study Trudy's methods
- We can admire Trudy's cleverness
- Often, we can't help but laugh at Alice and Bob's naivety
- But, we **cannot** act like Trudy
  - We will cover ways to break systems that are being used; if you try them on others' systems, you will be liable for all the consequences
  - If you do **not** have **permission**, do not do it

Related Areas

- Computer Science
  - Network security
  - Secure programming
  - Artificial intelligence
  - Pattern recognition
  - Operating systems
- Mathematics
  - Number theory
  - Elliptic curve cryptography
  - Proofs of security theories

Related Areas – cont.

- Electric engineering
  - Physical security and emanations security
- Statistics
  - Risk management
  - Statistical analysis
- Psychology
  - Human factors and social engineering
- Politics and economics

Summary

- Computer security is ubiquitous
  - As computers are highly connected, computer security becomes relevant to every computer user and system
  - Additionally, as many government and essential services also rely on the Internet, computer security is vital for critical infrastructure protection

Next Time

- Information Security Principles and Authorization