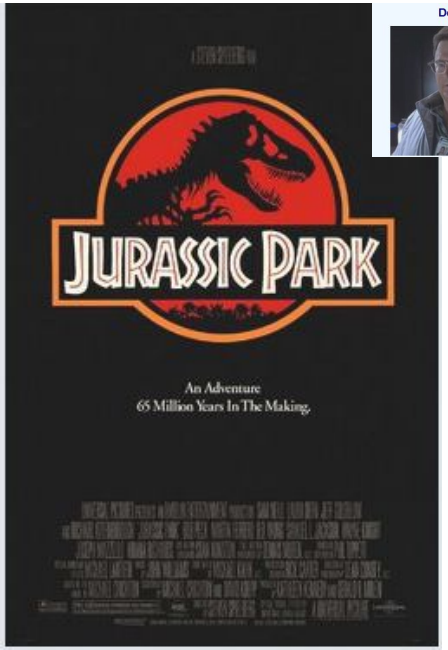
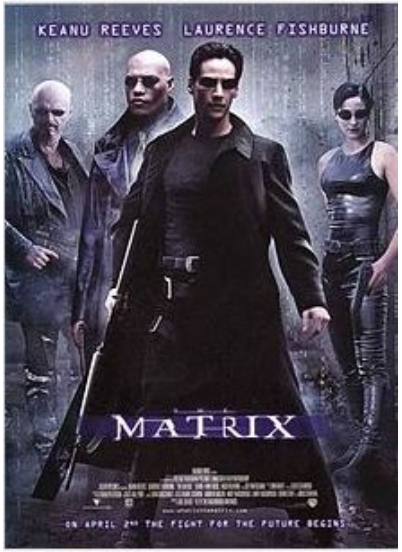
Overview of Cybersecurity

Part One

This research is supported by Award #1542465:
RET Site: Cyber Security Initiative for Nevada Teachers (CSINT)


JURASSIC PARK
An Adventure
65 Million Years In The Making.


Dennis Nedry


KEANU REEVES
LAURENCE FISHBURNE
MATRIX
ON APRIL 2ND THE FIGHT FOR THE FUTURE BEGINS


Office Space
Work sucks

What is Cybersecurity?

What does “cyber” mean?

- Popularized through 20th-century science fiction
  - “Cybermen” from Dr. Who (1966)
  - Martin Caidin’s novel *Cyborg* (1972)
  - “Cyberspace” from William Gibson’s novella *Burning Chrome* (1982) and novel *Neuromancer* (1984)

What is Cybersecurity?

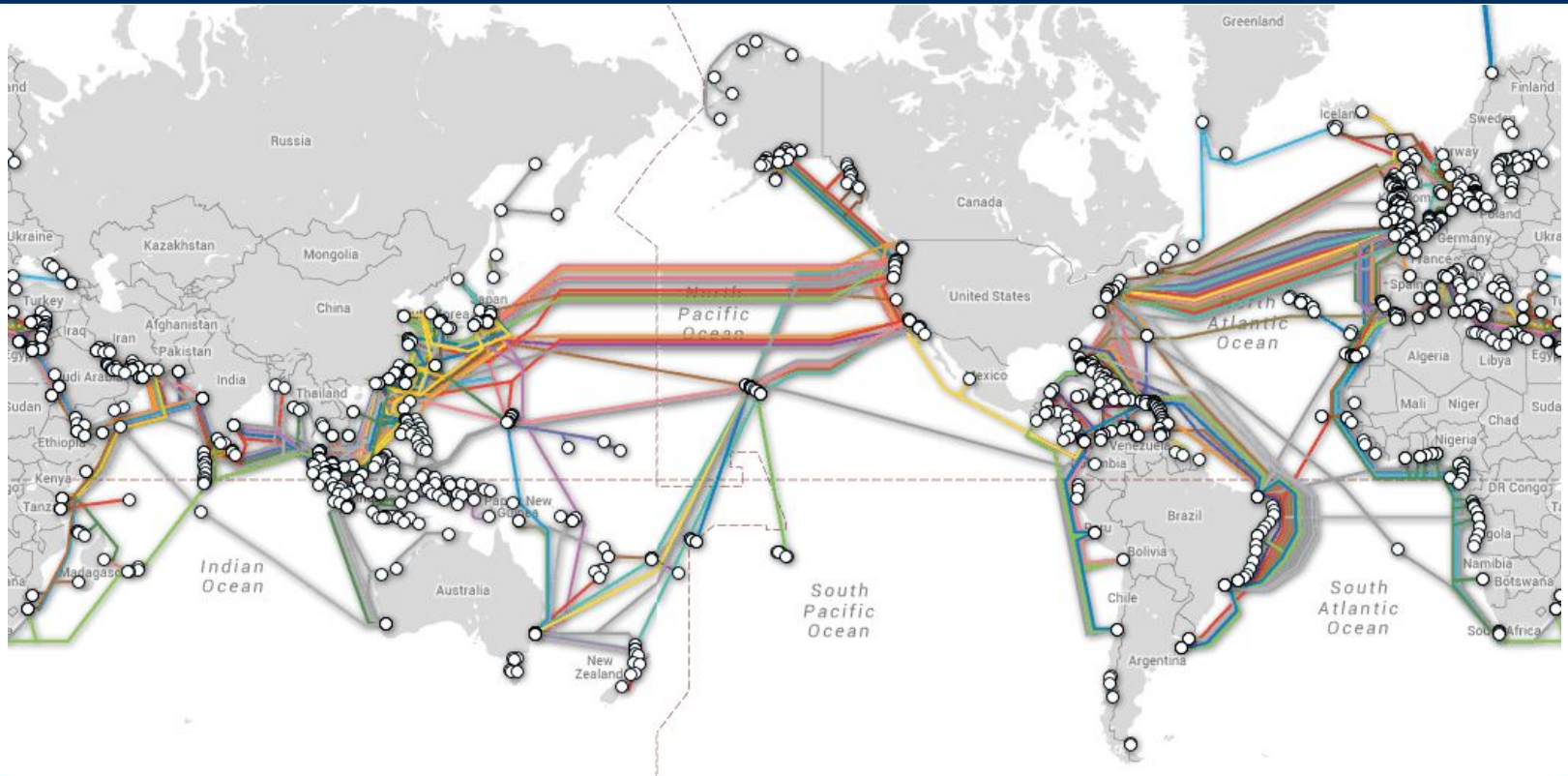
What does “cyber” mean?

- *“Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding”* - William Gibson (*Neuromancer*, 1984)
- Now, refers to “of, relating to, or involving computers or computer networks”

What is Cybersecurity?

- Cybersecurity is the security of computers and computer networks
- Basic questions:
  - What is security?
  - What is a computer? (not just PCs and phones)

Cyberspace / Geospace



Impact

Estimated cost of cybersecurity breaches: $600 billion (2018, CSIS/McAfee)

- This is 0.8% of global GDP
- An estimated 64% of Americans are victims of cybercrime

The same report discusses the growth of “Cybercrime-as-a-Service”

- Exploit kits, custom malware, botnet rentals, etc.

Impact

Some attacks target individuals, some target organizations, and some target nations

- Some simple security practices can go a long way in preventing the first of those three

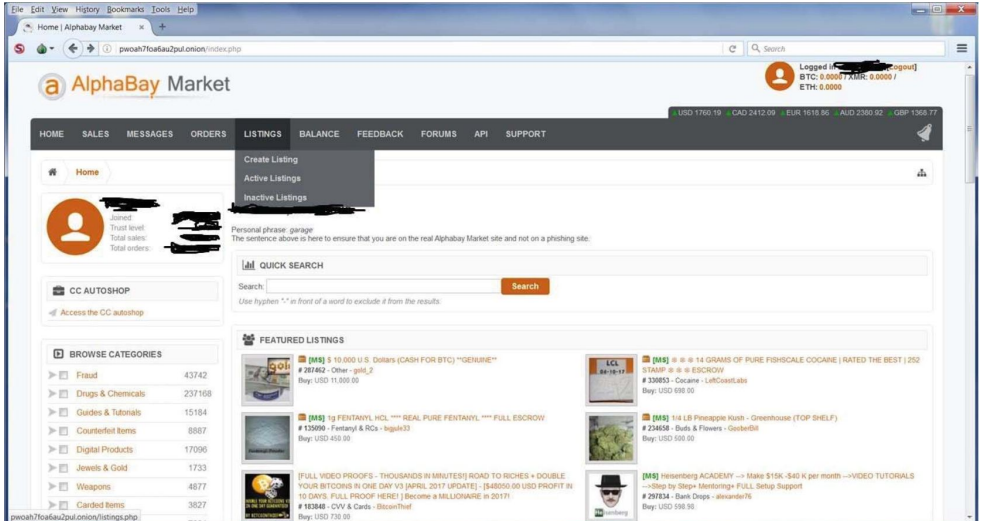
Cybercrime	Estimated Daily Activity
Malicious scans	80 billion
New malware	300,000
Phishing	33,000
Ransomware	4,000
Records lost to hacking	780,000

Table 1. Estimated daily cybercrime activity

Impact

A single darknet market, launched in late 2014, had over 400,000 users before being shut down in mid 2017

- Had laughably basic security failures such as the owner using his personal email for the site's welcome email



Four Levels of Security

Physical: Failures caused by the physical environment

Human: Failures caused by humans

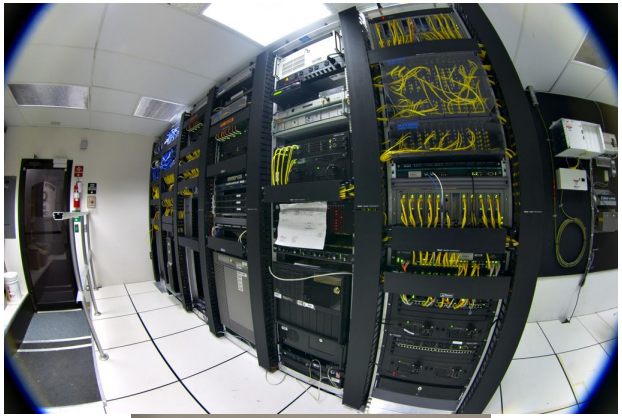
Operating System: Failures caused by or within an operating system

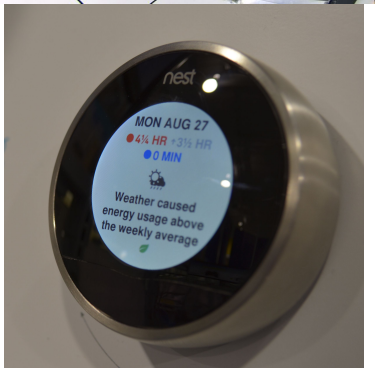
Network: Failures caused by the network

Four Levels of Security

Physical

- Physical security is concerned with the physical implementation of the system.
  - Back to the “what is a computer” question: are we concerned about a data center on private property, or a smart thermostat shipped to thousands of homes worldwide?
- What could go wrong with this implementation?





Four Levels of Security

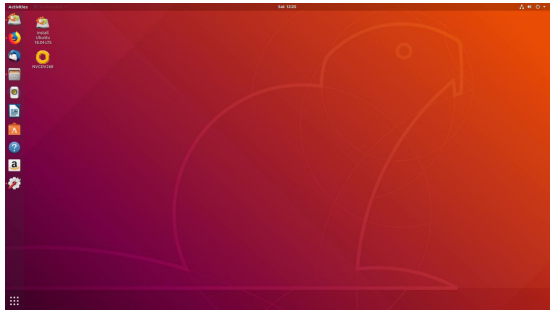
Human

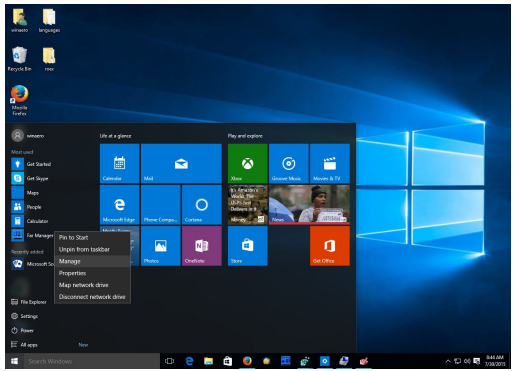
- At some point, humans are going to interact with the computers
- How easy is it for a human mistake to compromise the system?
- What protections are in place to prevent this?

Four Levels of Security

Operating System

- The operating system is a middleman between applications and hardware
- What operating system is the computer using?
  - Linux, Mac, Windows
- How does the service interact with the operating system?
  - What is the service able to do? What level of control does a user have over the service?





Four Levels of Security

Network

- The network connects systems, both internally and to the external world
- How is the network set up?
- Who has access to the network?

Four Levels of Security

Examples

- **Physical:**

- **Human:**

Four Levels of Security

Examples

- **Operating System:**

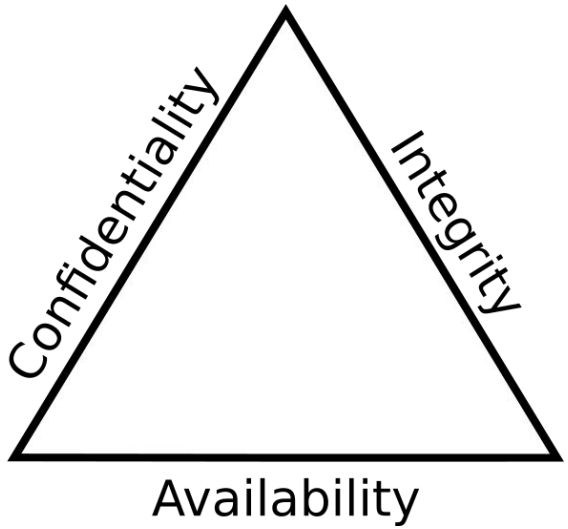
- **Network:**

CIA Triad

Confidentiality: Is secret data hidden from unauthorized parties?

Integrity: Does the system work as intended?

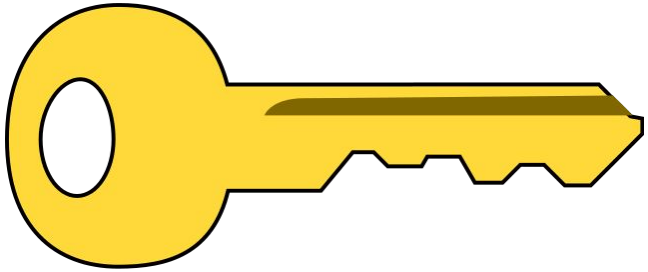
Availability: Can the system be accessed easily by authorized parties?



CIA Triad

Confidentiality

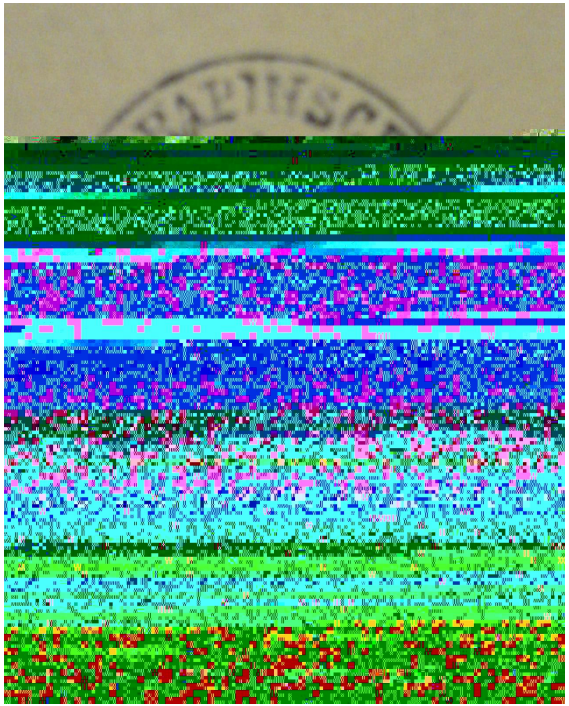
- What kinds of data do websites store?
- Who should be able to view that data?
- How much information about a system can be kept secret?



CIA Triad

Integrity

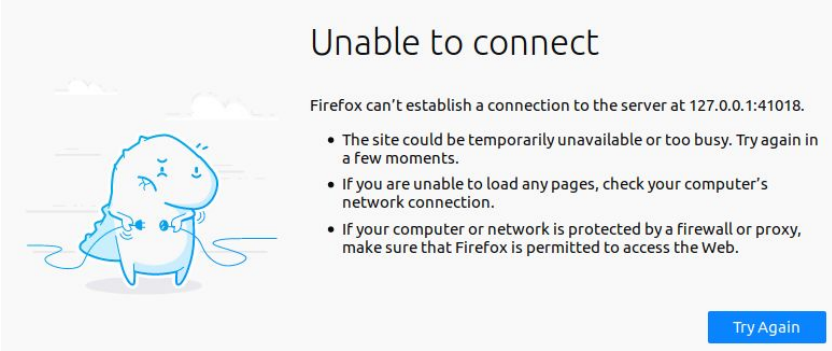
- An attacker can still attack something they can’t see
- How do we keep an attacker from modifying data?
- How do we keep data from being modified unintentionally?
- How can we check that a system works as intended?



CIA Triad

Availability

- The best security measure is to turn everything off
  - An attacker can't modify or view a system that isn't available!
- This obviously isn't a good solution
- How can we maintain confidentiality and integrity with as little inconvenience to a normal user as possible?



CIA Triad

More recently, the CIA triad has grown to include two additional concepts:

- **Non-repudiation:** can we ensure that only one person/group is the source of some given data?
- **Authentication:** can we ensure that a person is who they say they are?

Breaches

Confidentiality: An attacker has gained access to data they are not unauthorized to see

Integrity: The system does not work as intended; data is invalid

Availability: The system is not available to normal users

Breaches

Examples

- **Confidentiality:**
- **Integrity:**
- **Availability:**

Loss and Theft

What technologies might be stolen?

Examples:

Compromise

What services might be compromised?

Examples:

References

“Cyber” etymology

- https://www.merriam-webster.com/dictionary/cyber
- https://blog.oxforddictionaries.com/2015/03/05/cyborgs-cyberspace-csi-cyber/

Economic losses

- https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/economic-impact-cybercrime.pdf

AlphaBay Forfeiture Complaint

- https://www.justice.gov/opa/press-release/file/982821/download