463.1 Introduction (Cont.)

Computer Security II
CS463/ECE424
University of Illinois

MP1: Overview

- **Inference in Location-Based Social Networks**
- To be released today

- You are given:
  - Real anonymized datasets
  - Users may or may not share their home location
- Your task:
  - Infer private home locations using friendship information
- Due: 11:59 PM on September 8th (2 weeks)

MP1: Overview

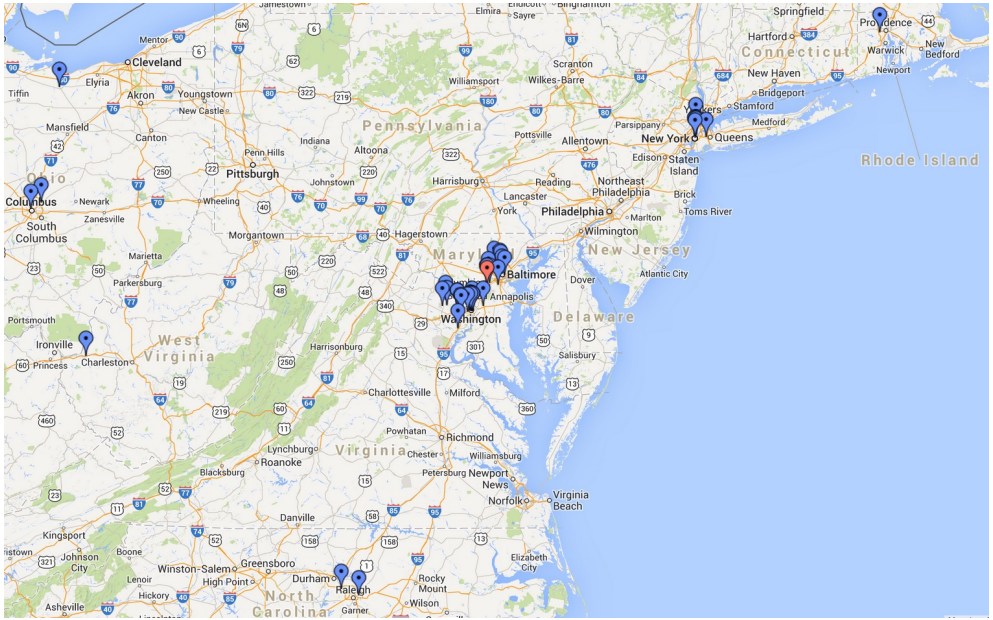
- Code skeleton is provided
- Checkpoint 1 (*start now*)
  - Get familiar with Java
  - Read and parse the dataset
- Checkpoint 2 (*you may wait for next lecture*)
  - Implement simple inference algorithm
  - Implement your own inference algorithm
- Report: one-page, two questions
- Ranking

MP1: Datasets

- Dataset 1:
  - Friendship information
  - Home locations for all users
- Dataset 2:
  - Same format as dataset 1
  - No ground truth

MP1: Visualization

- Visualization class ‘Visualizer.java’ is provided



MP1: Keep in mind

- Individual effort only
- Implementation in Java
- Submission:
  - Your code must compile and run on EWS
  - You can modify ‘compile.sh’ and ‘run.sh’
- Automated tests

Security News of the Day

https://www.zdnet.com/article/apple-microsoft-and-amazon-chiefs-to-meet-biden-over-critical-infrastructure-cyber-attacks/
https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity

Apple, Microsoft and Amazon chiefs to meet Biden over critical infrastructure cyber attacks

US President invites CEOs of US tech giants to discuss how critical infrastructure can be protected from foreign cyber attackers.

By Liam Tung | August 24, 2021 -- 10:16 GMT (03:16 PDT) | Topic: Security

The Biden administration issued a long-awaited cybersecurity executive order Wednesday that, among other things, requires federal agencies to develop an implementation plan for a zero-trust architecture for security.

May 2021

government agencies and critical infrastructure providers have faced numerous ransomware and espionage attacks during the pandemic, including the SolarWinds software supply chain espionage attack, and ransomware attacks against Colonial Pipeline, Kaseya, and meat packer JBS.

Security News of the Day

https://www.zdnet.com/article/
https://www.whitehouse.gov/br

Apple, Micro
Biden over c

US President invites CEOs of U
attackers.

By Liam Tung | Augu

inside and outside traditional network boundaries. The Zero Trust security model eliminates implicit trust in any one element, node, or service and instead requires continuous verification of the operational picture via real-time information from multiple sources to determine access and other system responses. In essence, a Zero Trust Architecture allows users full access but only to the bare minimum they need to perform their jobs. If a device is compromised, zero trust can ensure that the damage is contained. The Zero Trust Architecture security model assumes that a breach is inevitable or has likely already occurred, so it constantly limits access to only what is needed and looks for anomalous or malicious activity. Zero Trust Architecture

The Biden administration issued a long-awaited cybersecurity executive order Wednesday that, among other things, requires federal agencies to develop an implementation plan for a zero-trust architecture for security.

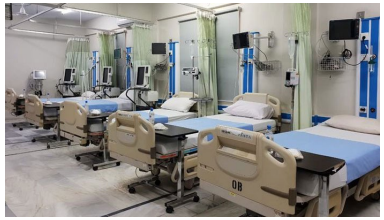
May 2021

government agencies and critical infrastructure providers have faced numerous ransomware and espionage attacks during the pandemic, including the SolarWinds software supply chain espionage attack, and ransomware attacks against Colonial Pipeline, Kaseya, and meat packer JBS.

463.1.2
Critical Infrastructure Protection

Examples of Systems

- Transportation
- Financial
- Energy
- Human health
- Agriculture and food
- Water
- Communication
- Cities and fixed infrastructure


Presidential Decision Directive 63
Critical Infrastructure Protection

- Bill Clinton, May 22, 1998

- Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private.

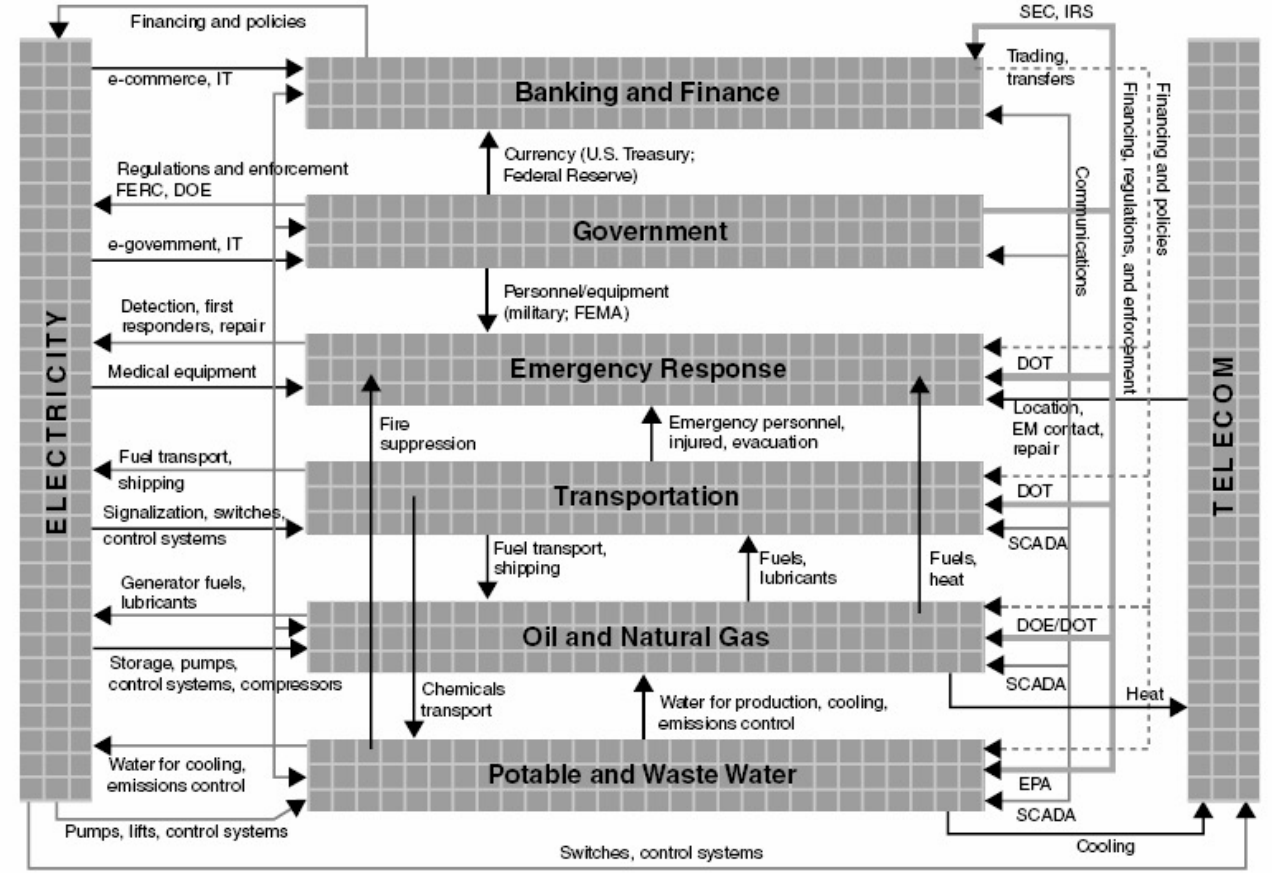
- Many of the nation's critical infrastructures have historically been physically and logically separate systems that had little interdependence. *As a result of advances in information technology* and the necessity of improved efficiency, however, *these infrastructures have become increasingly automated and interlinked.*

- *These same advances have created new vulnerabilities* to equipment failure, human error, weather and other natural causes, and physical and cyber attacks. Addressing these vulnerabilities will necessarily require flexible, evolutionary approaches that span both the public and private sectors, and protect both domestic and international security.

Documented Security Incidents for Industrial Control Systems

- Salt River Project (1994): breach of a water and electricity provider's computers by modem
- Worchester Air Traffic Communications (1997): teenager disables public switching network for an airport
  - Knock out the phone service of the control tower
  - Shut down radio transmitter of the control tower and runway lights
- Maroochy Shire Sewage Spill (2000): disgruntled former employee accesses system releasing 264,000 gallons of raw sewage

Interdependency of Systems

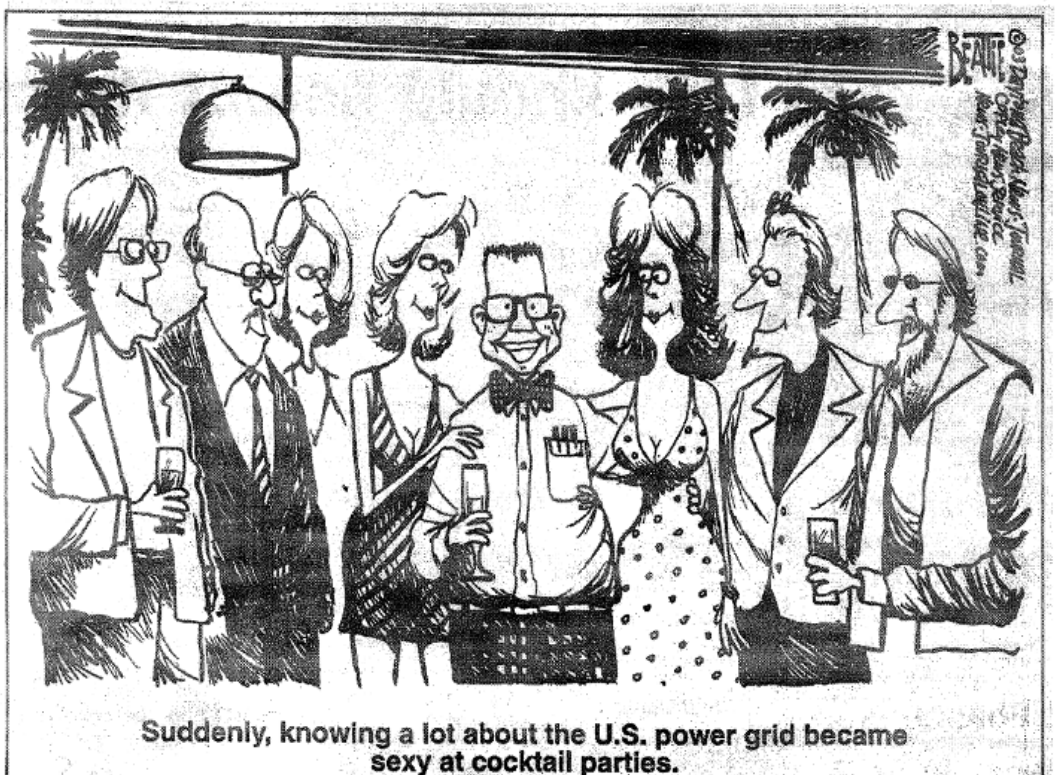


Case Study: 2003 Blackout

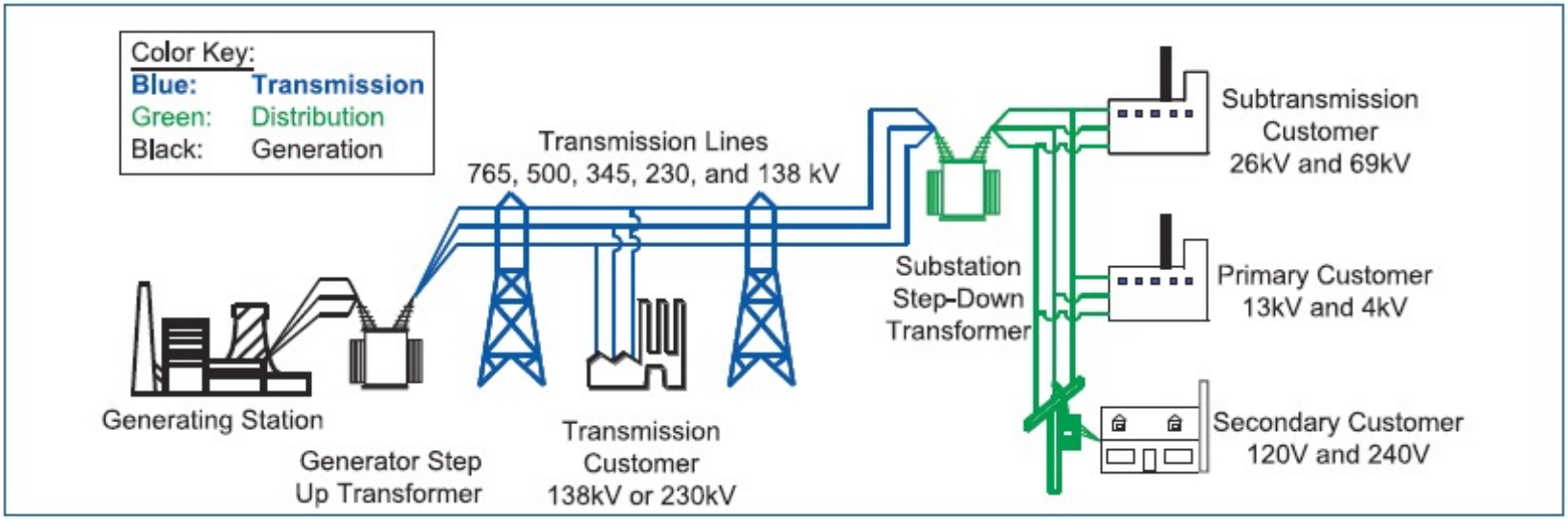
- Provides an excellent example of failure of a critical infrastructure system involving computer control

- Not caused by a malicious attack but influential in advancing concerns about cyber security for critical infrastructure

Power Engineering is Cool Again



Basic Structure of the Electric Grid



Objectives of an Energy Management System (EMS)

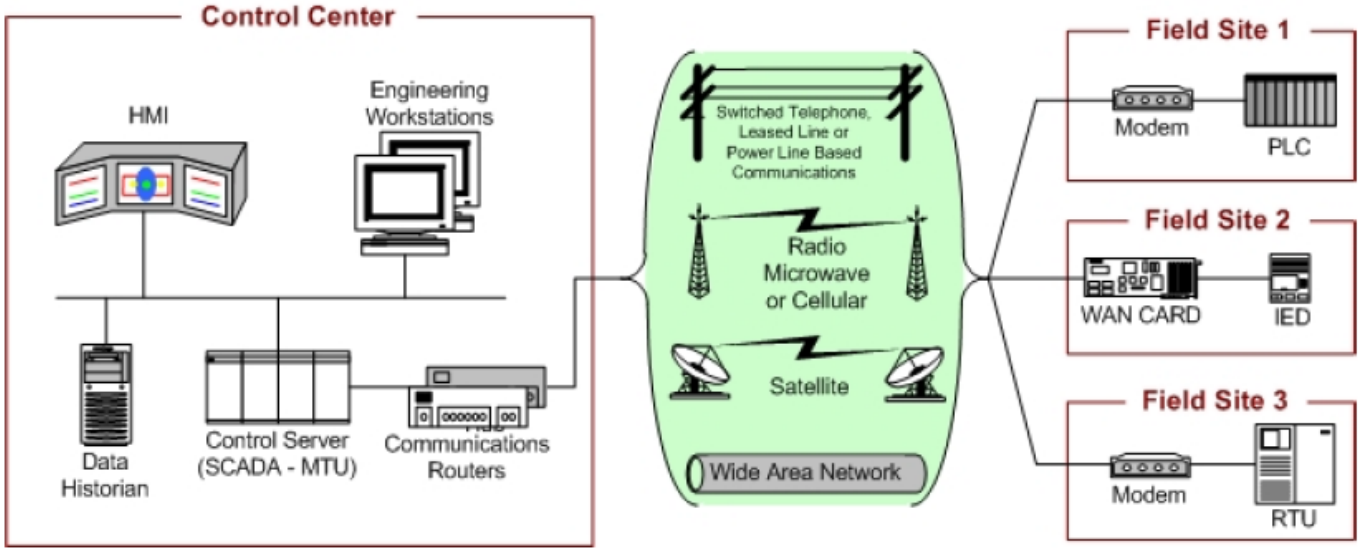
- Balance generation and demand
- Maintain scheduled voltages
- Ensure that thermal limits are not exceeded
- Plan, design, and maintain the system to operate reliably
- Keep the system in a stable condition
- Prepare for emergencies
  - Maintain the “N-1 criterion”
  - Can withstand failures at a single system component and recover

SCADA for EMS

- EMSs are increasingly exploiting computers and data networking

- Supervisory Control and Data-Acquisition (SCADA):
  - Data acquisition: collection, processing, monitoring
  - Supervisory control: manual overrides, alarm inhibit/enable
  - Alarm display and control

SCADA System General Layout



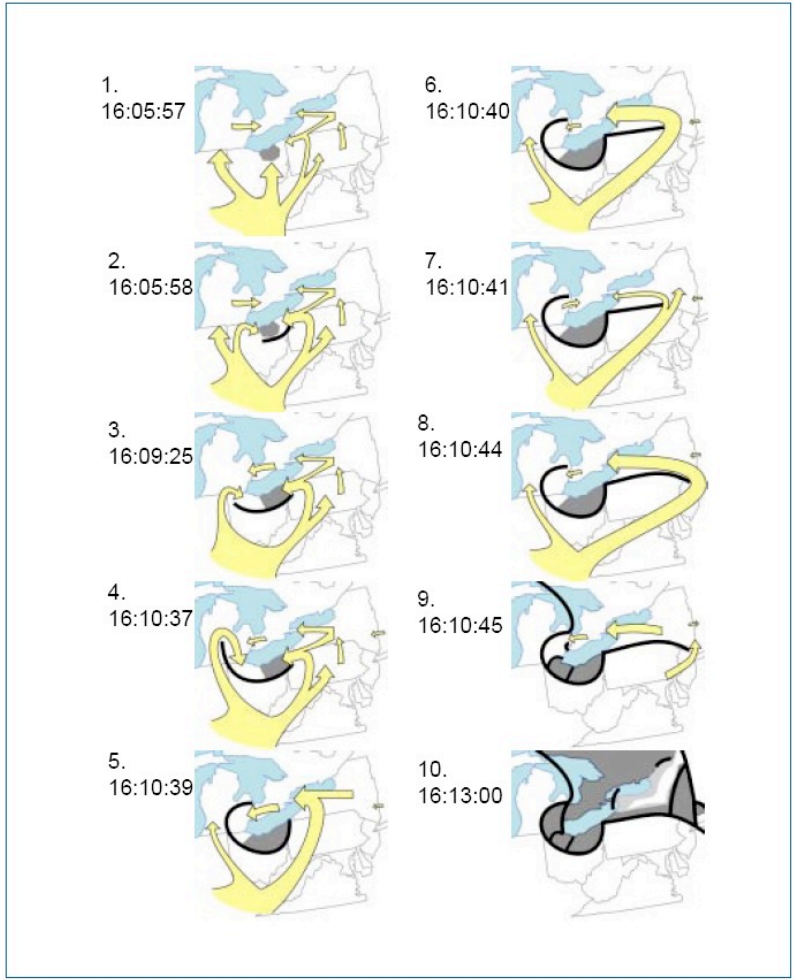
The 2003 Blackout

- Started August 14 around 4pm
- Lasted about 4 days.
- 50 million people were affected.
- Total costs were estimated at more than 5 billion US dollars.

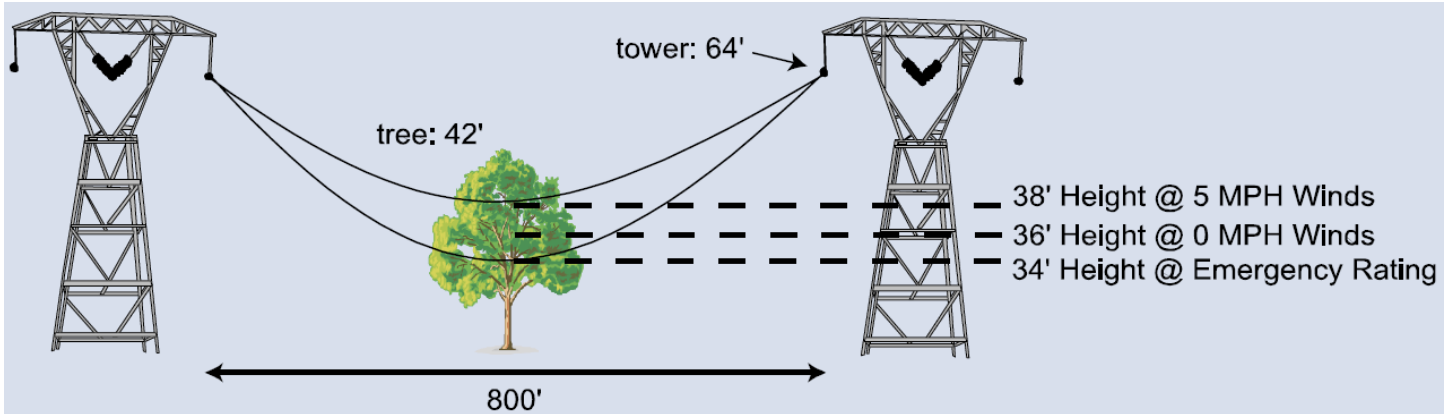
Cascading Failure

- Started from one power line going down
- The neighboring area got over stressed
- The neighboring areas of the neighboring area got over-stressed
- Cascading …

- **Phase 5**: Unplanned shifts of power across region
- **Phase 6**: Full cascade
- **Phase 7**: Formation of islands
- Why the blackout stopped where it did
  - Cascade stops at areas with less integration



The Tree that Did $5,000,000,000 in Damage



What Caused the Blackout?

- Limited electricity reserves
- Un-trimmed trees in the Cleveland control area

- Insufficient understanding of system state through networked computer control
  - Multiple failed systems: delays from MISO state estimator and missed alarms at First Energy
- System integration that enabled the blackout to spread broadly without supporting adequate information exchange

Effects on Other Infrastructure

- Water supply
  - Example: Cleveland lost water pressure and issued a boil advisory
- Transportation
  - Example: Amtrack NE Corridor down above Philadelphia
  - Example: 7-hour wait for trucks because of loss of electronic border checks at the Canada/US border
- Communication
  - Wired telephones continued but cellar service was disrupted
- Industry
  - Many factory closings in affected area
- Fixed infrastructure
  - Looting in Ottowa and Brooklyn (but limited compared to the 1977 NY blackout)

Cyber-Security Dimension

- The 2003 Blackout was influential for cyber-security.
- Why? The report asserts that there is no evidence that a cyber-attack contributed to the blackout.
- Yet, the computer control difficulties **did** contribute.
- Increasing interdependency of the system and increased reliance on computer monitoring and control open the path to **deliberately-caused** failures like the 2003 blackout based on cyber-attacks.

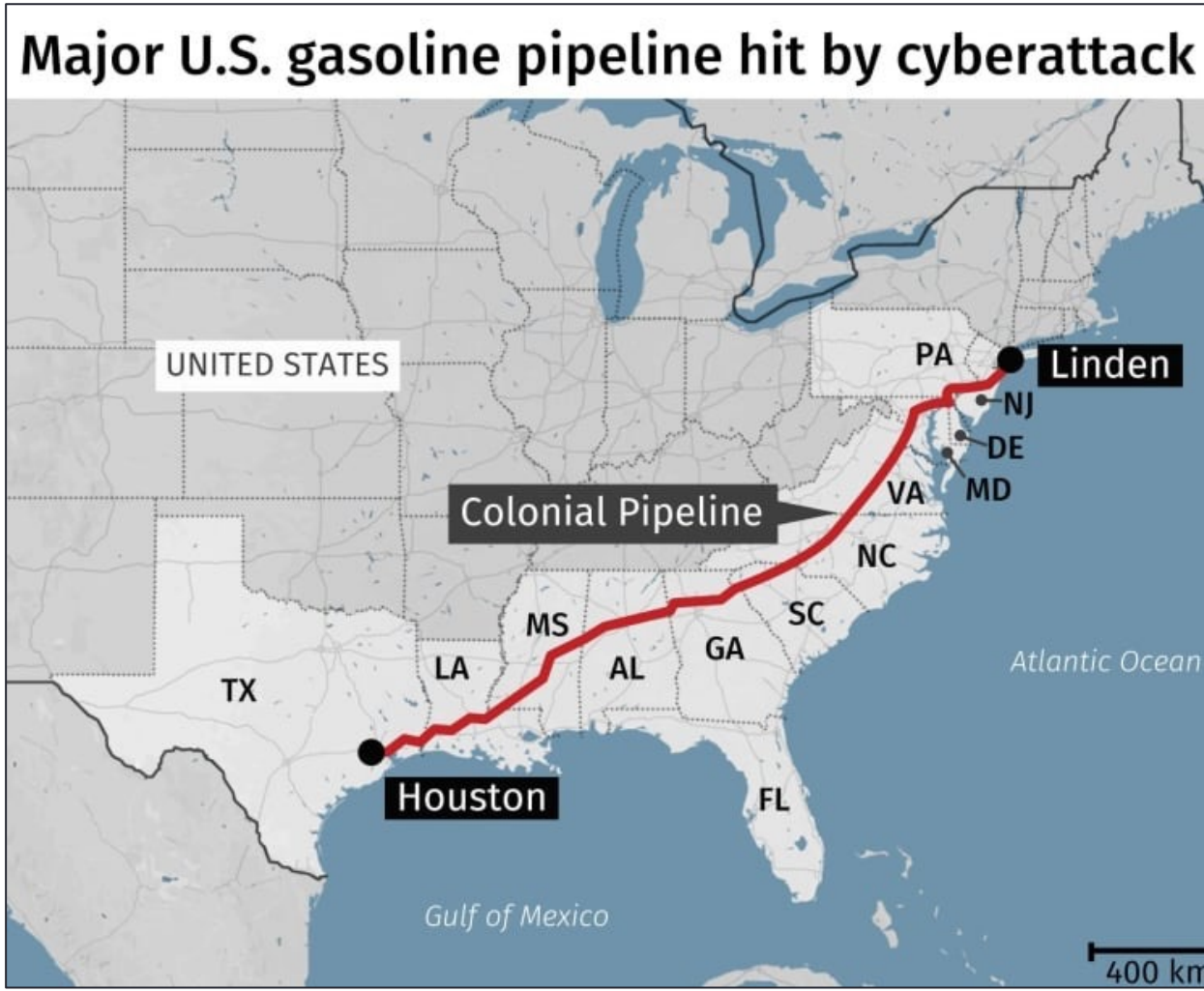
Now This →

On May 7, 2021, Colonial Pipeline, an American oil pipeline system, suffered a ransomware attack.

Colonial carries fuel/ gasoline for airports, military bases and gas stations southeastern of the US

The company halted all pipeline operations to contain the attack

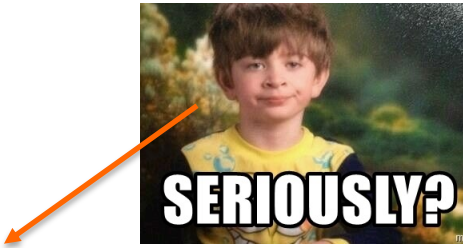
Colonial Pipeline paid $4.4 million in bitcoins several hours after the attack



Impacts (6 days of pipeline shutdown)

- Fuel shortages at filling stations
- Panic buying after the 4th day of pipeline shutdown
- Average fuel prices rose
- The restart of pipeline operations began on May 12, 2021

Investigation and Aftermath



- DarkSide hacking group is behind this attack
  - *Claim: "our goal is to make money, and not creating problems for society"*
  - A hacking group that develops its own ransomware and runs attacks
  - Also offers "ransomware-as-a-service"; grants its affiliate subscribers to use its ransomware and gets a portion of ransom payments in return

- On June 7, 2021, the Department of Justice recovered $2.3 million ransom payments (63.7 bitcoins)
  - FBI seized the private key of the ransom account

DOJ seizes millions in ransom paid by Colonial Pipeline

The Justice Department recovered some of the ransom paid to DarkSide actors.

Root Causes

https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password?sref=Wg6QzS2e

- According to a report from **Bloomberg** and **FireEye**, the company was likely breached through a leaked password to an old account that had access to the VPN used to remotely access the company's servers.
- The account reportedly didn't have multifactor authentication
- Colonial employee may have used the same password on another account that was previously hacked

Reading

- [HennessyPL03] Information Technology for Counterterrorism Immediate Actions and Future Possibilities, John L. Hennessy, David A. Patterson, and Herbert Lin, Editors. Computer Science and Telecommunications Board, National Research Council, 2003. http://www.nap.edu/openbook.php?isbn=0309087368
- [StoufferFS08] Guide to Industrial Control Systems (ICS) Security, Keith Stouffer, Joe Falco, and Karen Scarfone. NIST Special Publications 800-82, Final Public Draft 2008.
- [Blackout04] Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations, U.S.-Canada Power System Outage Task Force. 2004.

- https://www.nytimes.com/2021/05/13/us/politics/biden-colonial-pipeline-ransomware.html

Discussion Questions

1. Are smartphones more secure than hosts? Why?

2. Are voting systems a critical infrastructure? What are their cyber threats and risks?

Be sure to do the Quiz ☺