CS302 Information Security and Cryptography – Lectures 1&2

B Tech III Div. A and B

(Jan 2023 - 1st and 2nd week)

Dr Dhiren Patel

NIT Surat, India

Key information about course

- Course name: Information Security and Cryptography
- Course code: CS302
- Course scheme: 3-1-2
- Credits: 5
- Class: B Tech III CSE Semester 6
- Period: Jan - Apr 2023
- Physical classroom: CSE new building
- Google classroom code: uwvjhs2
- Meet link: https://meet.google.com/byz-pkhh-fmr
- Instructors: Dhiren Patel, Suhani Chauhan

Course outcome (COs)

At the end of the course, the students will be able to	
CO1	Understand the concepts related to Information Security and Cryptography.
CO2	Apply the concept of security services and mechanisms from the application developers and network administrator's perspective.
CO3	Analyse the security schemes for their use in different application scenarios.
CO4	Evaluate and asses the computer and network systems for associated risks.
CO5	Design the security schemes depending on the organisation's requirements.

Curriculum – p1

INTRODUCTION	(04 Hours)
Security Attacks, Services and Mechanisms, CIA Traid, Security Design Principles, Attack Surface and Attack Trees, Model for Network Security, Introduction to Number Theory, Shannon's Theory	
SYMMETRIC KEY CIPHERS	**(10 Hours)**
Substitution Techniques, Transposition Techniques, Digital Watermarking and Steganography, Data Encryption Standard (DES), Advanced Encryption Standard (AES), Block Cipher Modes of Operation, Random Bit Generation and Stream Ciphers	

Curriculum – p2

ASYMMETRIC KEY CIPHERS	(08 Hours)
Principles of Public-Key Cryptosystems, RSA, Diffie-Hellman Key Exchange, Elgamal Cryptosystem, Elliptic Curve Cryptography.	
CRYPTOGRAPHIC HASH FUNCTIONS	(04 Hours)
Hash Functions and Data Integrity, Security of Hash Functions- The Random Oracle Model, Iterated Hash Functions- Merkel Damgard Construction, Secure Hash Algorithm (SHA).	
MESSAGE AUTHENTICATION	(06 Hours)
Message authentication requirements, message authentication codes (MAC) based on hash functions-HMAC and block ciphers-DAA and CMAC, Authenticated Encryption-CCM and GCM	

Curriculum – p3

DIGITAL SIGNATURES	**(06 Hours)**
Security requirements, RSA Digital Signatures, NIST Digital Signature Algorithm (DSA), Elliptic Curve Digital Signature Algorithm (ECDSA), RSA-PSS Digital Signature Algorithm	
IDENTIFICATION SCHEMES AND ENTITY AUTHENTICATION	**(02 Hours)**
Challenge Response Protocols, Password Based Authentication, Zero Knowledge Schemes.	
ADVANCED TOPICS	**(02 Hours)**

Ref books:

- William Stallings, Cryptography and Network Security – Principles and Practice, Pearson
- William Stallings, Network Security Essentials: Applications and Standards, Pearson
- Dhiren Patel,Information Security: Theory and Practice, PHI
- Web
- Papers (IEEE, ACM)
- Journals and Magazines

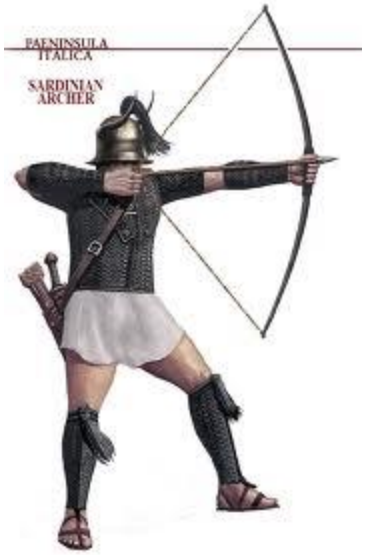
Scope and terminologies

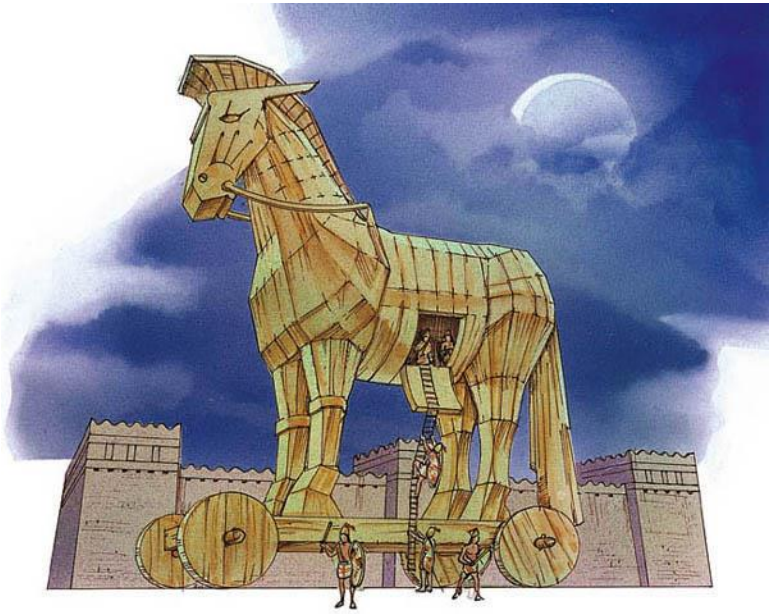
- Cryptography, Information Security, Cyber Security, Network Security, Web Security,
- Data Confidentiality (Encryption Algorithms),
- Data hiding (Steganography),
- Data Integrity (Hash functions),
- Authentication (Identity and Access Management),
- Non-repudiation (Digital signature),
- Security Policy, Vulnerability Assessment and Penetration Testing ….

Example: Technology works, System fails

- Class room attendance (IIT)
- Big class – 1st year
- Roll call time - (eats up valuable time)
- Gate open through access control
- Biometric – (error and peer pressure inducing delay (false negative))
- RFID (cards in class not students)
- Technology worked, system failed

Ancient attackers…

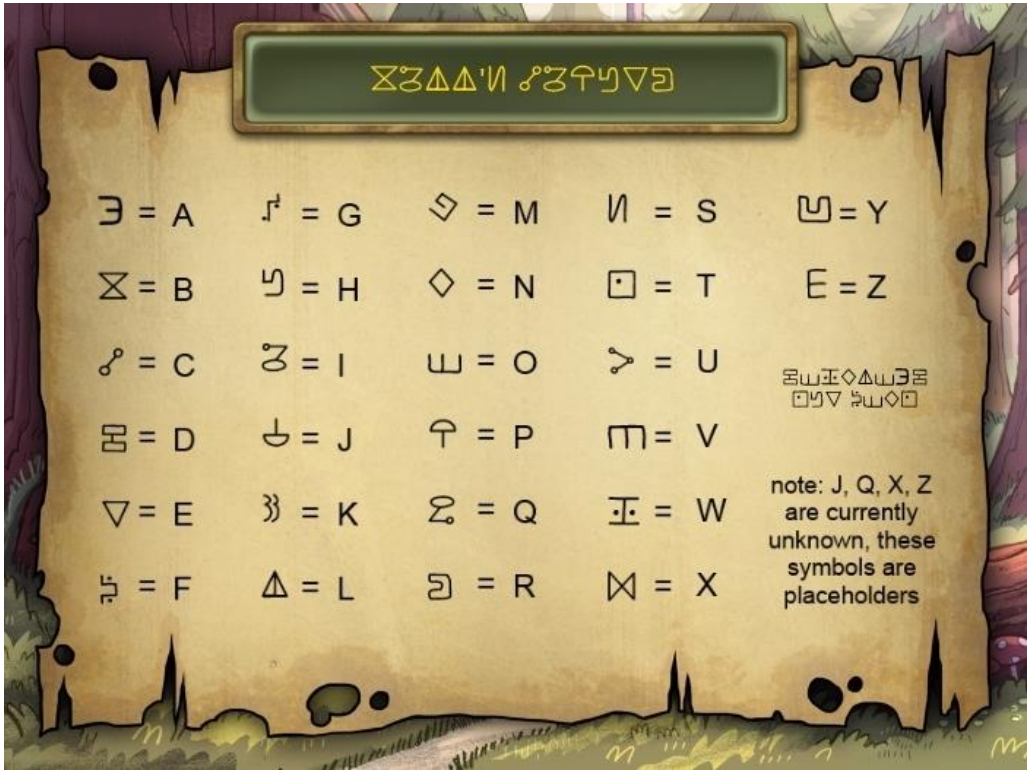




Ancient Secret Keeping/Msgs

- Signals
- Signs
- Colors
- Messenger – msg on head
- Shadow Events

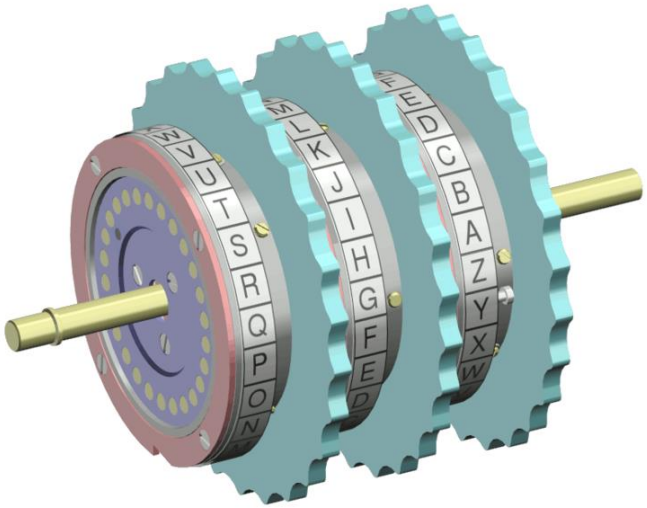
BC – Caesar Cipher



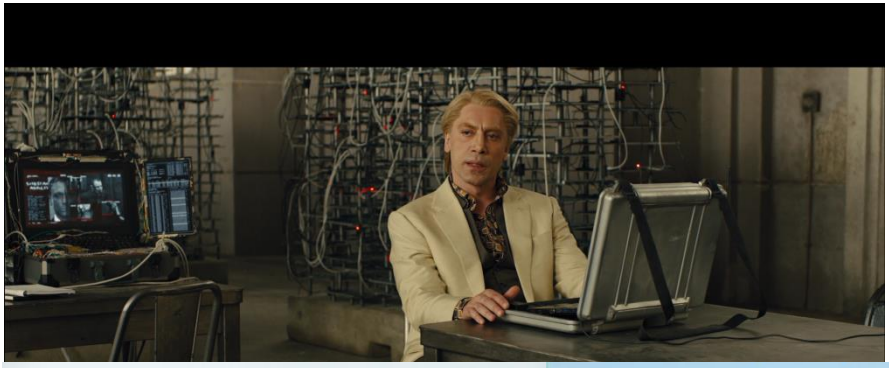
1854 Playfair Cipher

C	O	D	E	S
A	B	F	G	H
I/J	K	L	M	N
P	Q	R	T	U
V	W	X	Y	Z

Second world war – Rotor machines (Imitation Game – Alan Turing)



(Modern) attackers….



Die Hard 4 (2007)

- Attack on Critical infrastructure
- Power (Energy Generation & Distribution)
- Telecom hijacking – emergency services (control over telecom infrastructure)
- Computing - Transferring money (control over Financial infrastructure)
- Access codes, Authorization codes of warfare (control over utility services and military)

Natanz fuel enrichment plant, Central Iran – Stuxnet (2009-10)

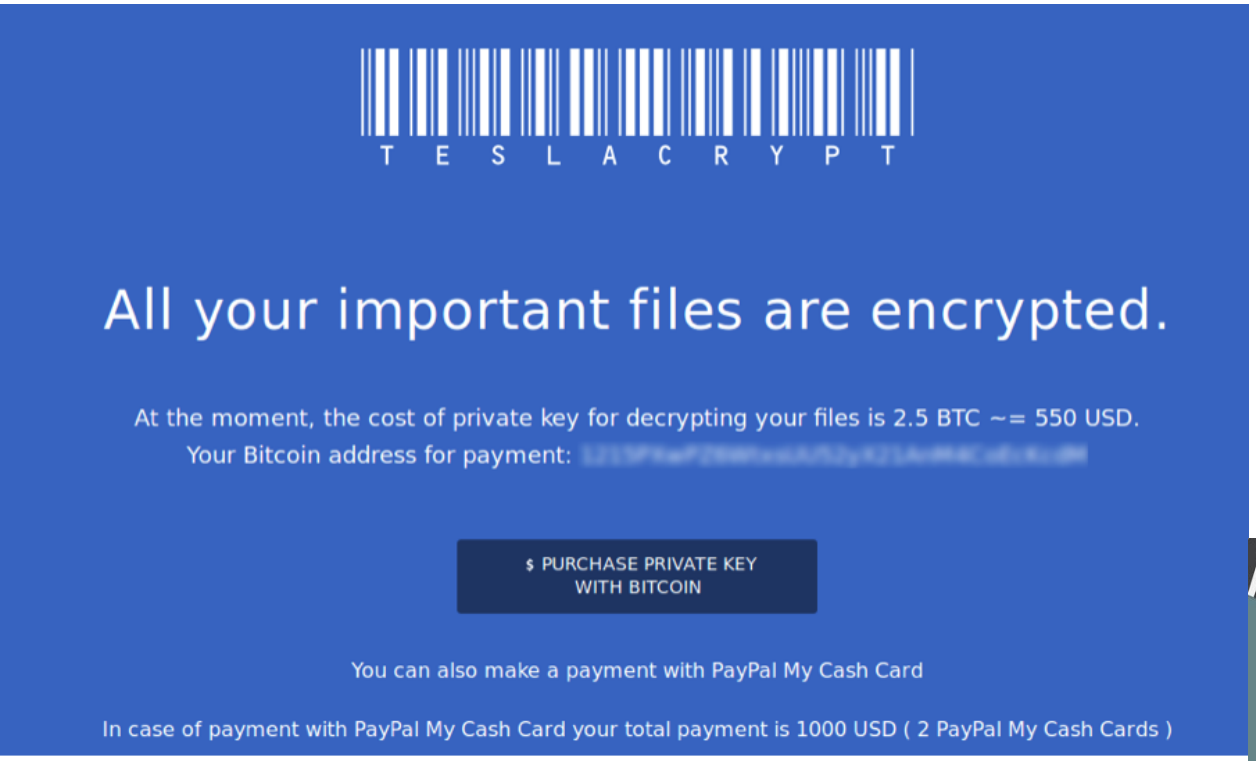
Stuxnet attack

- **Stuxnet** - a malicious computer worm first uncovered in 2010.
- It was tailored as a platform for attacking modern SCADA and PLC systems. (SCADA - supervisory control and data acquisition (SCADA), programmable logic controllers (PLC))
- Stuxnet is believed to be responsible for causing substantial damage to the nuclear program of Iran.
- Stuxnet specifically targets programmable logic controllers (PLCs), which allow the automation of electromechanical processes such as those used to control machinery and industrial processes including gas centrifuges for separating nuclear material.
- Stuxnet functions by targeting machines using the Microsoft Windows operating system and networks, then seeking out Siemens Step7 software.
- Stuxnet reportedly compromised Iranian PLCs, collecting information on industrial systems and causing the fast-spinning centrifuges to tear themselves apart

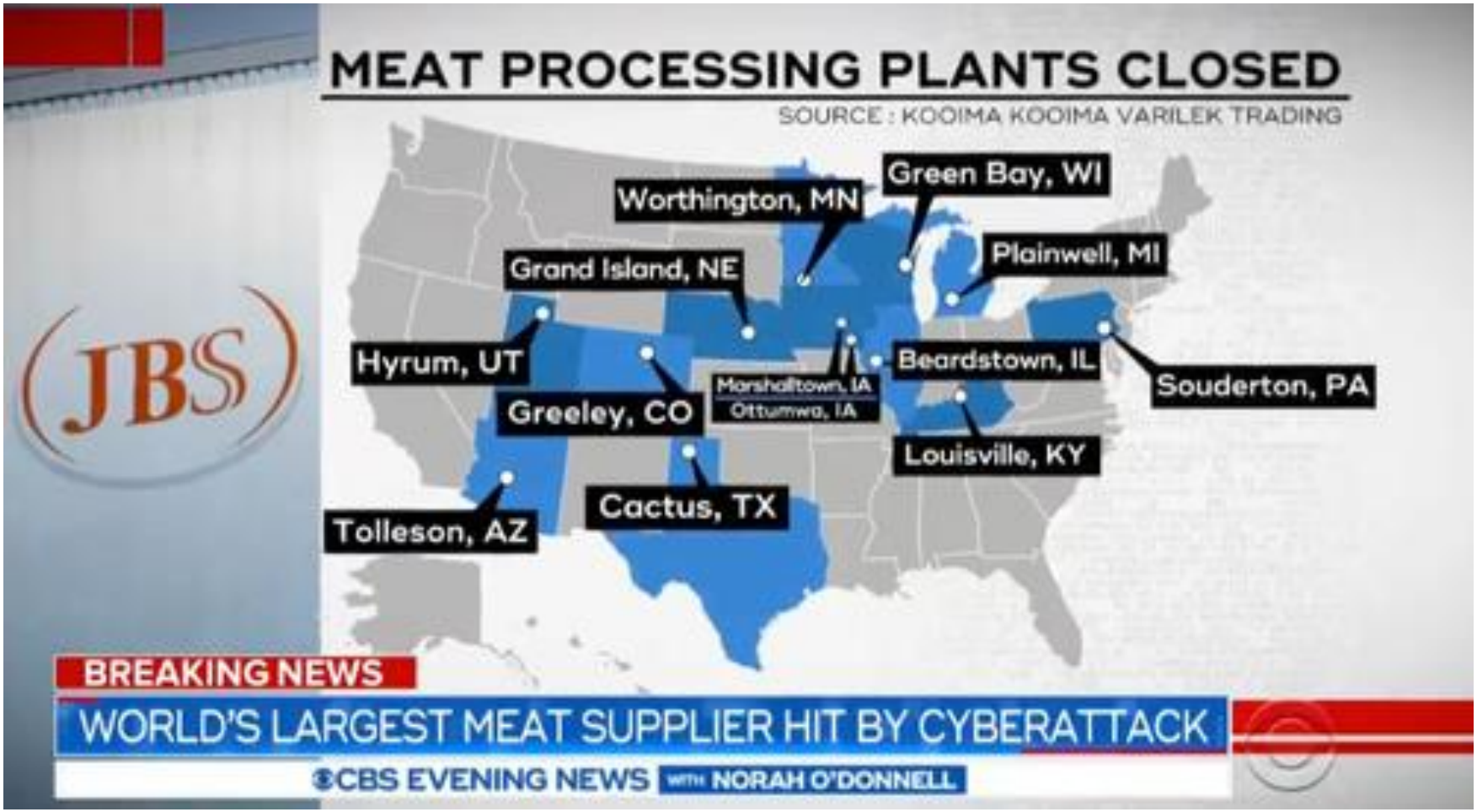
Regin (2014)

Persistent, long-term mass surveillance operations; targets specific users of Microsoft Windows-based computers and has been linked to the intelligence gathering agency NSA and GCHQ.

Ransom ware (2014-15)



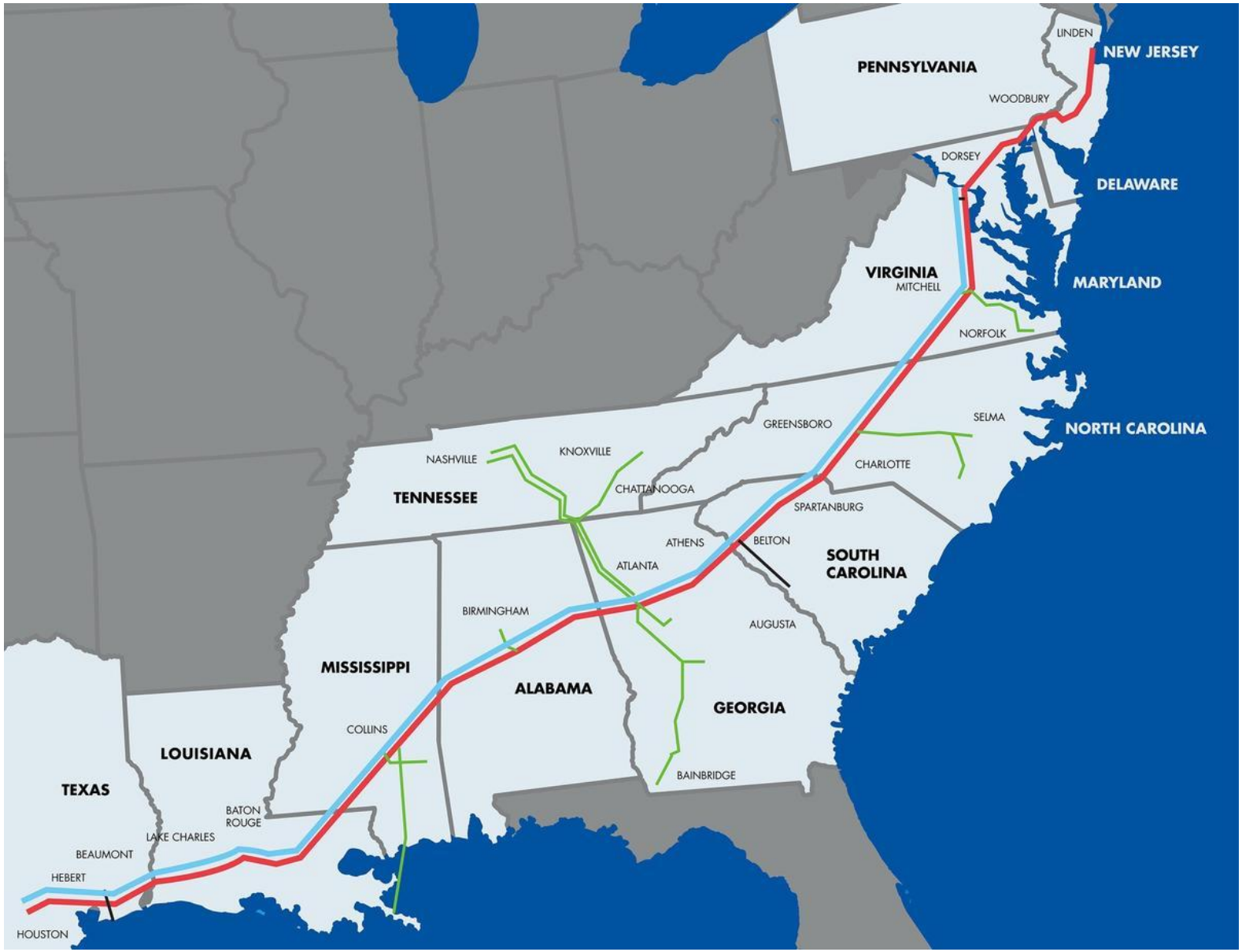
JBS attack (May-June, 2021)



JBS

- On May 30, 2021, JBS S.A., a Brazil-based meat processing company, suffered a cyberattack, disabling its beef and pork slaughterhouses. The attack impacted facilities in the United States, Canada, and Australia.
- JBS paid the hackers an $11 million ransom (in Bitcoin).

Colonial Pipeline Attack (May 2021)



CP

- On May 7, 2021, Colonial Pipeline, an American oil pipeline system that originates in Houston, Texas, and carries gasoline and jet fuel mainly to the Southeastern United States, suffered a ransomware cyberattack that impacted computerized equipment managing the pipeline.
- The Colonial Pipeline Company halted all pipeline operations to contain the attack. The primary target of the attack was the billing infrastructure of the company.
- the company paid the amount that was asked by the hacker group (75 bitcoin or $4.4 million) within several hours.

CP

- The restart of pipeline operations began at 5 p.m. on May 12, ending a six-day shutdown
- On June 7, the US Department of Justice announced that it had recovered 63.7 of the bitcoins from the ransom payment
- Through possession of the private key of the ransom account, the FBI was able to retrieve the Bitcoin, though it did not disclose how it obtained the private key.
- Bitcoin nose dived with a fear that FBI has broken ECC – recovered next day.

Personalized Attack (Sept 2020)

- A**ttack targeting a German hospital** prevented emergency service personnel from communicating with the hospital, forcing the re-routing of an individual who required emergency services.

AIIMS and NIC (Dec 1st week, 2022)

- **5 AIIMS Servers Hacked, 1.3 TB Data Encrypted in Recent Cyberattack, Govt Tells RS**
- Media reports citing investigators had earlier revealed that records of nearly 3-4 crore patients, including high-profile politicians, were compromised.
- AIIMS Delhi server attack was by the Chinese, FIR details that the attack had originated from China. Of 100 servers (40 physical and 60 virtual), five physical servers were successfully infiltrated by the hackers.

USA (Oct 10, 2022)

- The distributed denial of service (DDoS) attacks hit the airport websites of several major US cities including Atlanta, Chicago, Los Angeles, New York, Phoenix and St Louis.
- A DDoS attack involves knocking a website offline by flooding it with traffic. (made it inaccessible to the public).
- pro-Russian hacking group known as "KillNet" published a list of sites and encouraged its followers to attack them

Iran (Oct 9, 2022)

- the group Edalat-e Ali (Ali's Justice) – Iran
- "Woman, Life, Freedom"
- the biggest wave of social unrest
- new tactics to spread their message of resistance in public spaces
- (e.g. altering the wording of a government billboard, footage from the Ghezel Hesar prison was released to the public, Several water features in the Iranian capital were said to have been coloured blood-red)

Web - Universal Client (browser, apps)

Any thing…. Any where….. Convergence

amazon.com
and you're done.™

Windows Azure

Microsoft®
Office 365

flexiant™
utility computing on demand

salesforce.com
SOFTWARE
Success On Demand.™

Attacks on ICT: Motivation

- Theft of sensitive info.
- Disruption of service
- Illegal access to resources

Attacks – on confidentiality, integrity, masquerading, non-repudiation, replay,

<example: going to Cinema - India>

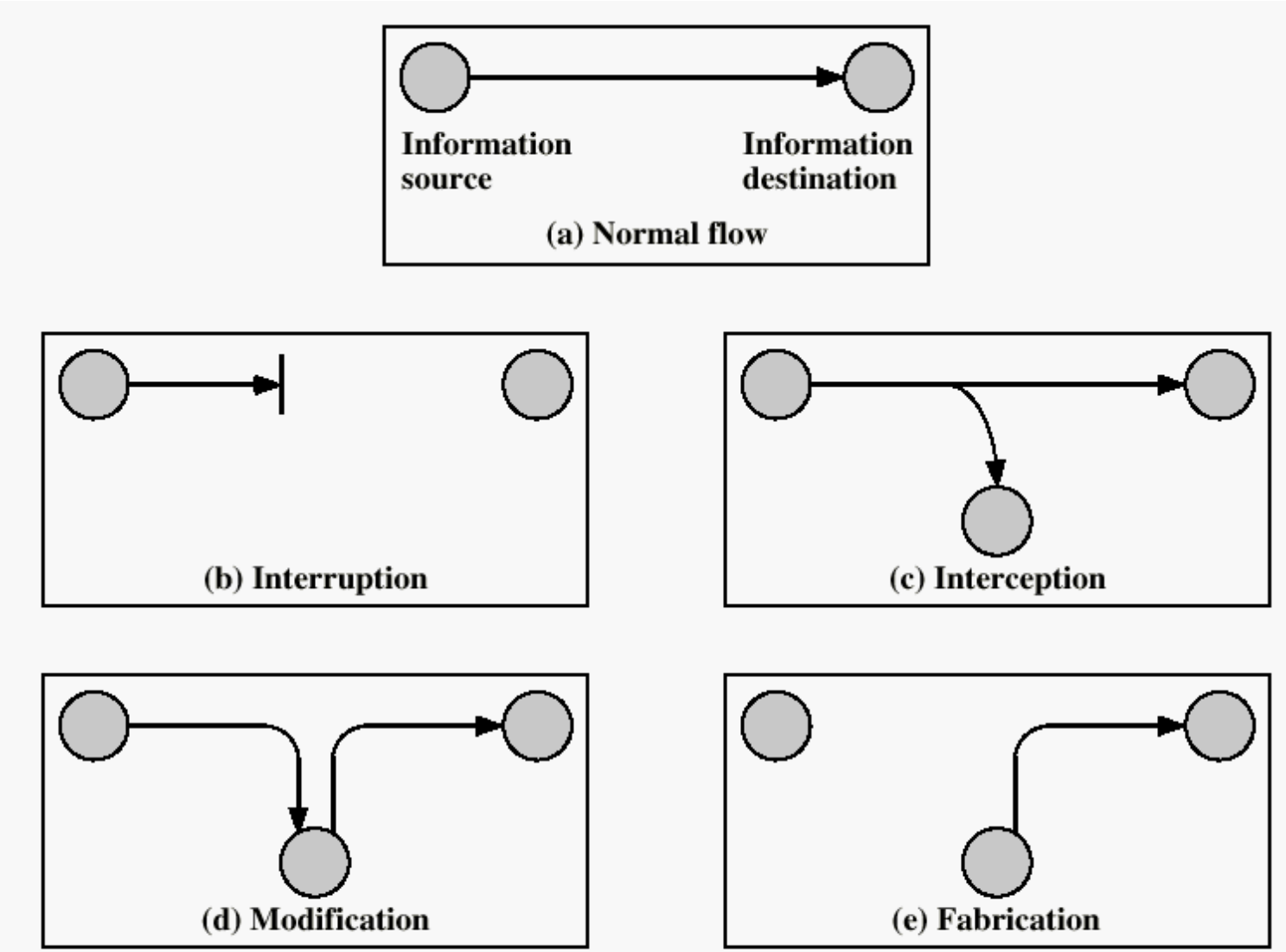


Figure 1.1 Security Threats

Usable Apps – attack targets
(when launched! – Now Secure??)

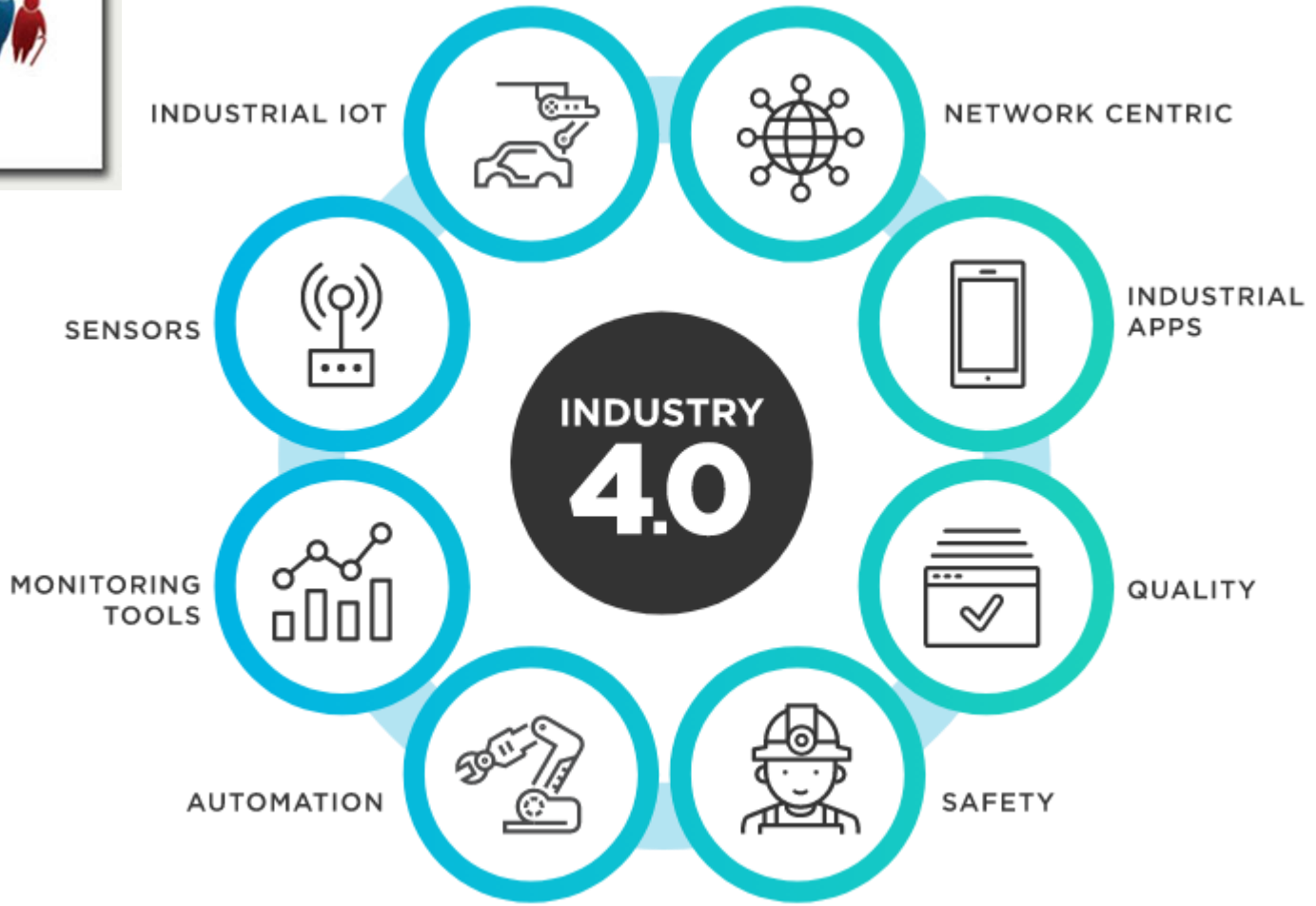
Meta

BitTorrent™

Universal client

Changing landscape (and Security scope)


INTERNET


INDUSTRIAL IOT
NETWORK CENTRIC
SENSORS
INDUSTRIAL APPS
INDUSTRY 4.0
MONITORING TOOLS
QUALITY
AUTOMATION
SAFETY

IIoT

- Digital transformation of industries toward a demand service model
- IIoT is used across a range of industries from manufacturing, logistics, oil and gas, transportation, mining, aviation, energy, and more.
- Its focus is to optimize operations--particularly the automation of processes and maintenance.
- Trans disciplinary (Inter disciplinary) systems engineering

Remote Monitoring and Diagnostics (maintenance and health audit of …..)

Data Security, Privacy, Access Control

Security Primitives and Solutions

- Steganography
- Encryption – Symmetric, Asymmetric
- Hash functions
- Key exchange
- Key life time
- Biometric
- CAPTCHA
- Embedded Security
- Security Associations
- Authentication, Identity Management and Access control
- Multi-factor
- Blockchain (???)

Summary

- Security Technology, Secure System, Trust??
- Don’t miss the lectures….
- It provides you broad insights and awareness of security landscape, examples, use cases, scope, challenges and opportunities!!
- Welcome aboard…..