PESU ISFCR

PESU Center for
Information Security,
Forensics and
Cyber Resilience

PES UNIVERSITY

Welcome to

PES University

Ring Road Campus, Bengaluru

10 June 2020

APPLIED CRYPTOGRAPHY

Lecture 2

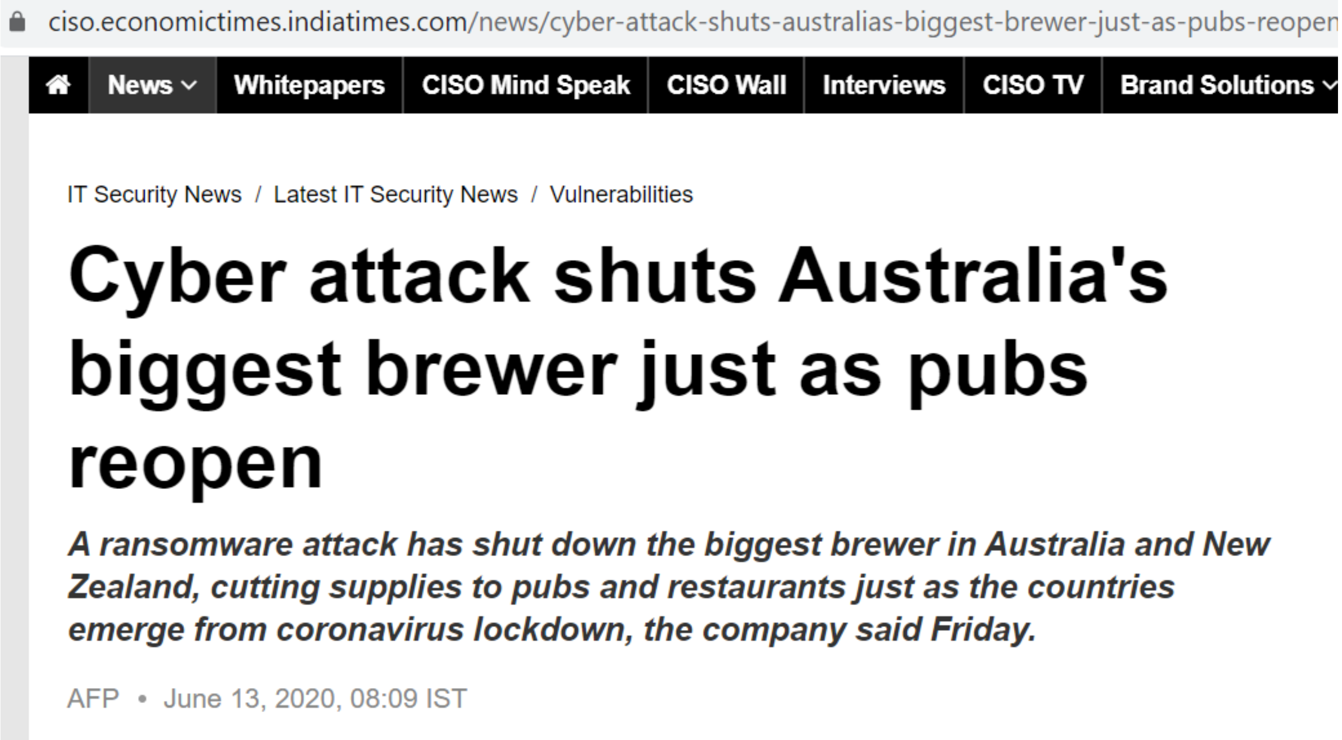
Legal, Ethical and Professional aspects

One must be aware of ……..

Cryptographic laws

- Deals with legislation ensuring that information is secure and transmitted confidentially, as well as policies designed to keep secure encryption schemes out of the hands of unauthorized individuals and foreign powers

Ransomware



ciso.economictimes.indiatimes.com/news/cyber-attack-shuts-australias-biggest-brewer-just-as-pubs-reopen

IT Security News / Latest IT Security News / Vulnerabilities

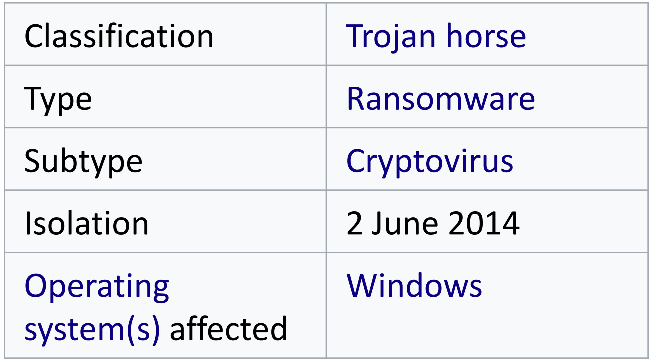
Cyber attack shuts Australia's biggest brewer just as pubs reopen

A ransomware attack has shut down the biggest brewer in Australia and New Zealand, cutting supplies to pubs and restaurants just as the countries emerge from coronavirus lockdown, the company said Friday.

AFP • June 13, 2020, 08:09 IST

Case Study: Cryptolocker Ransomware Attack

- occurred from 5 September 2013 to late May 2014
- It is type of malware encrypted certain types of files stored on local and mounted network drives using RSA public-key cryptography



Classification	Trojan horse
Type	Ransomware
Subtype	Cryptovirus
Isolation	2 June 2014
Operating system(s) affected	Windows

- In order to prevent the incidents like the above-mentioned, laws are required

Objectives of Information Security

- Confidentiality (secrecy): Only the sender and intended receiver should be able to understand the contents of the transmitted message
- Authentication: Both the sender and receiver need to confirm the identity of other party involved in the communication
- Data integrity: The content of their communication is

not altered, either maliciously or by accident,

in transmission.

- Availability: Timely accessibility of data to

authorized entities.

Laws with Cryptography

- Export Control law
- Import Control law
- Patent Related law
- Search and seizure

Source: https://ifca.ai/pub/fc97/r4.pdf

Export Control law

- Export control laws restrict the export of cryptography methods within a country to other countries or commercial entities.
- These laws often relate to matters of national security, but can also relate to private or commercial matters, as well.
- To protect cryptography for military use, there are international export control agreements such as the Wassenaar Arrangement which requires disclosures by member nations of any military technology exported to other countries, including cryptography technology.

Import Control Laws

- Import control laws pertaining to cryptography restrict the use of certain types of cryptography within a country.
- These laws are designed to go hand-in-hand with international agreements to discourage the importation of cryptography from other nations.
- It also helps to protect international business interests by allowing governments to prohibit the importation of private sector encryption technologies that could jeopardize legitimate business interests and allow for unfair competition.

Patent Issues

- Some cryptography law deals with the use of cryptography tools that are patented.
- These laws pertain to protecting intellectual property that allows for different forms of encryption, such as technologies for securing electronic financial transactions, keeping E-mail communications private, or authenticating web sites.
- These often go hand-in-hand with import laws

designed to protect intellectual property from

illegal import and use in another country

without the permission of the inventor.

Search and Seizure

- A final area of interest to cryptography laws are issues related to search and seizure.
- These are often criminal constitutional issues regarding under what circumstances a person can be compelled to decrypt data files or reveal an encryption key to allow investigators to compile a case against that individual.
- This is a contested area of encryption law given the competing interests in protecting the public and national security versus the constitutional protections against self-incrimination and for due process.

In INDIA

- General right to encryption: No known legislation or policies.
- Mandatory minimum or maximum encryption strength:
- Section 84A of the Information Technology Act 2000 allows the government to set nationally permitted “modes or methods” for encryption, however no such modes or methods have been prescribed.
- Separately, the Department of Telecommunications Guidelines and General Information for Grant of License for Operating Internet Services provides that internet service providers may not deploy “bulk encryption” on their networks and prohibits users from using encryption with greater 40-bit key length without prior permission. Anyone using stronger encryption is required to provide the government with a copy of the encryption keys.

Data Protection Law Articles

- Bureau of Industry and Security
- e-Government Act
- Federal Information Security Management Act (FISMA)
- PKCS 1 - RSA Cryptography Standard

https://www.hg.org/encryption-law.html

Bureau of Industry and Security (BIS)

- Encryption and Export Administration Regulations (EAR)
- Encryption items fall under Category 5, Part 2 for Information Security.
  - https://www.bis.doc.gov/index.php/encryption-and-export-administration-regulations-ear

e-Government Act

- The E-Government Act was passed by Congress in 2002 and supplements many of the privacy rights guaranteed by the Privacy Act of 1974.
- To employ external access safeguards to identify and prevent unauthorized tries of outsiders to hack into, or cause harm to, the information in our systems.
- Proposes section Federal Information Security Management Act (FISMA)

  - https://www.transportation.gov/individuals/privacy/e-government-act

Federal Information Security Management Act (FISMA)

- Requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other sources.

Organizations Related to Encryption Law

- Central Intelligence Agency (CIA)
- Department of Homeland Security
- National Security Agency
- NIST Computer Security Division - Cryptographic Technology

Central Intelligence Agency (CIA)

- Created in 1947 by by President Harry S. Truman
- Roles:
    - provision of analysis in areas relevant to national security
    - Give early warning of impending crises, serve national and international crisis management by helping to discern the intentions of current or potential opponents
    - Inform national defense planning and military operations
    - Protect sensitive information secrets, both of their own sources and activities, and those of other state agencies.

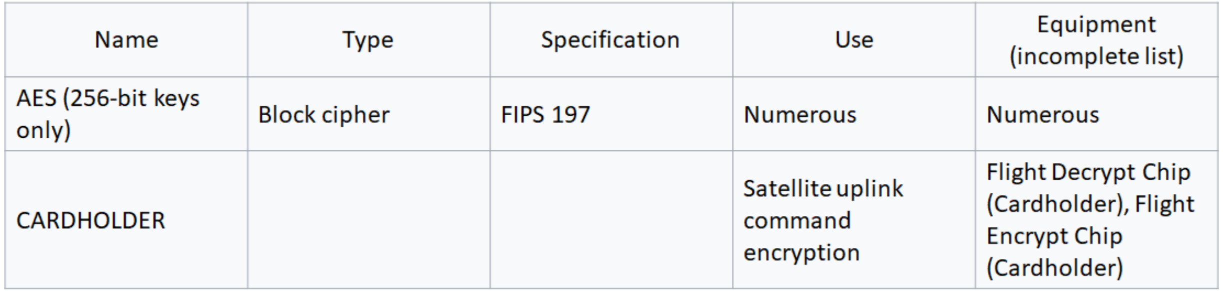
https://www.cia.gov/index.html

Department of Homeland Security (DHS)

- DHS established SAVER (System Assessment and Validation for Emergency Responders)
  - SAVER provides information on equipment that falls within the categories listed in the DHS Authorized Equipment List (AEL)

National Security Agency (NSA)

- The NSA has categorized encryption items into four product types
  - A Type 1 Product refers to an NSA endorsed classified or controlled cryptographic item for classified or sensitive U.S. government information, including cryptographic equipment, assembly or component classified or certified by NSA for encrypting and decrypting classified and sensitive national security information when appropriately keyed.



Name	Type	Specification	Use	Equipment (incomplete list)
AES (256-bit keys only)	Block cipher	FIPS 197	Numerous	Numerous
CARDHOLDER			Satellite uplink command encryption	Flight Decrypt Chip (Cardholder), Flight Encrypt Chip (Cardholder)

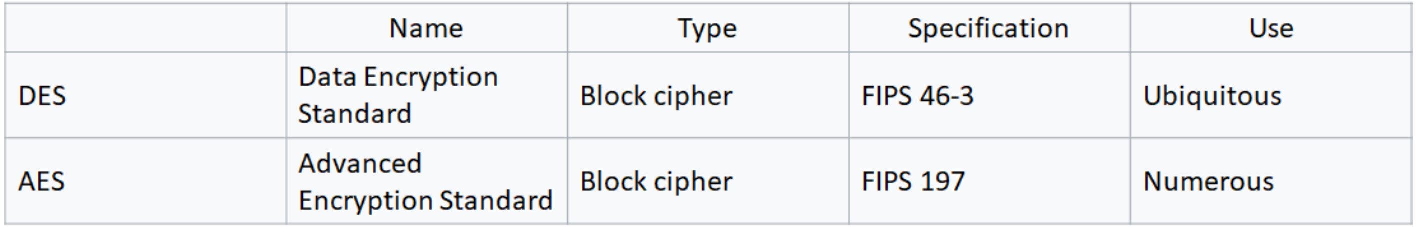
https://www.nsa.gov/

NSA Type 2 product

- A Type 2 Product refers to an NSA endorsed unclassified cryptographic equipment, assemblies or components for sensitive but unclassified U.S. government information.

NSA Type 3 product

- A Type 3 Algorithm refers to NIST endorsed algorithms, registered and FIPS published, for sensitive but unclassified U.S. government and commercial information.



	Name	Type	Specification	Use
DES	Data Encryption Standard	Block cipher	FIPS 46-3	Ubiquitous
AES	Advanced Encryption Standard	Block cipher	FIPS 197	Numerous

NSA Type 4 product

- A Type 4 Algorithm refers to algorithms that are registered by the NIST but are not FIPS published. Unevaluated commercial cryptographic equipment, assemblies, or components that are neither NSA nor NIST certified for any Government usage.

NIST Computer Security Division - Cryptographic Technology

- Research, develop, engineer, and produce guidelines, recommendations and best practices for cryptographic algorithms, methods, and protocols.
  - NIST recommended 15 elliptic curves of varying security levels for US federal government use.

Next Class

- ☞ Mandatory reading for the next class

  https://en.wikipedia.org/wiki/Cryptographic_primitive

S Rajashree

Computer Science and Engineering

PES University, Bengaluru

PESU ISFCR

PESU Center for Information Security, Forensics and Cyber Resilience

PESU IoT

PESU Center for **Internet** of **Things**