Tech-Webinar

On 12th May 2020 organized jointly by IETE and SETS

During the launch of ***COE for*** **Cyber Security and Critical Infrastructure Security**

Cyber Security: Emerging Trends

Vulnerabilities, Attacks and Mitigation Strategy

Dr. N Sarat Chandra Babu

Executive Director

sarat@setsindia.net

SETS, Chennai

Outline

- Overview of Cyber Threats; Individual, Organisational and National perspective
- Impact of COVID 19 on Cyber Security
- Cyber Security – Evolution of Technology based Solutions
- Cyber Security Technology Trends
- Need of the Hour

Importance of Cyber Security

"The nation should ensure that the digital space does not become a playground of dark forces. Cyber attacks are significant threat to the global community. We need to ensure that the vulnerable section of the society does not fall prey to it"

Honourable Prime Minister Shri. Narendra Modi

Inaugural session of the fifth edition of the Global Conference on Cyber Space (GCCS) in Delhi (23rd Nov 2017)

Cyber Threats
(An individual, organizational and national perspective)

Individual level

- Ransom ware
- Malware
- Advanced Persistent Threats (APTs)
- Social Engineering
- Email hacking & misuse
- Identity theft & phishing
- Financial scams
- Abuse through emails
- Abuse through Social Networking sites
- Mobile device threats
- Laptop theft

Organizational level

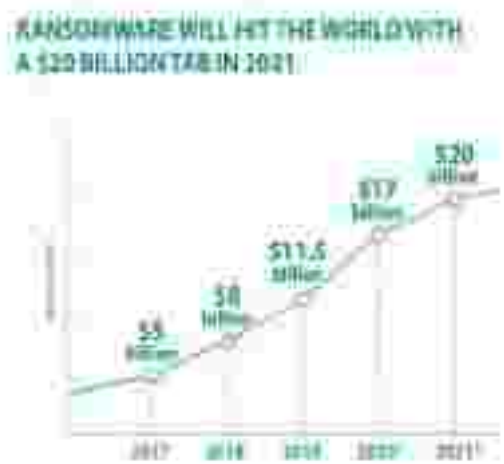
- Website intrusion/ defacement
- Domain stalking
- Malicious Code
- Scanning and probing
- Denial of Service & Distributed Denial of Service
- Targeted attacks
- Phishing
- Data theft
- Insider threats
- Financial frauds

National level

- Cyber Terrorism
- Attacks on Critical Infrastructure
- Web defacement
- Website intrusion and malware propagation
- Malicious Code
- Scanning and probing
- Denial of Service & Distributed Denial of Service
- Anonymous Applications

Attack Trends: From Stuxnet to Video Bombing

- **Stuxnet**:
  - A seminal point in ICS cybersecurity - Stuxnet (computer worm)
  - Attack at the Iranian uranium enrichment facility at Natanz, which damaged nearly 1,000 centrifuges.
  - It gave instructions rather than interfere with the PLC, faking rather than disrupting sensor output, and was accomplished without any internet connection, via a supply chain attack and a thumb drive.



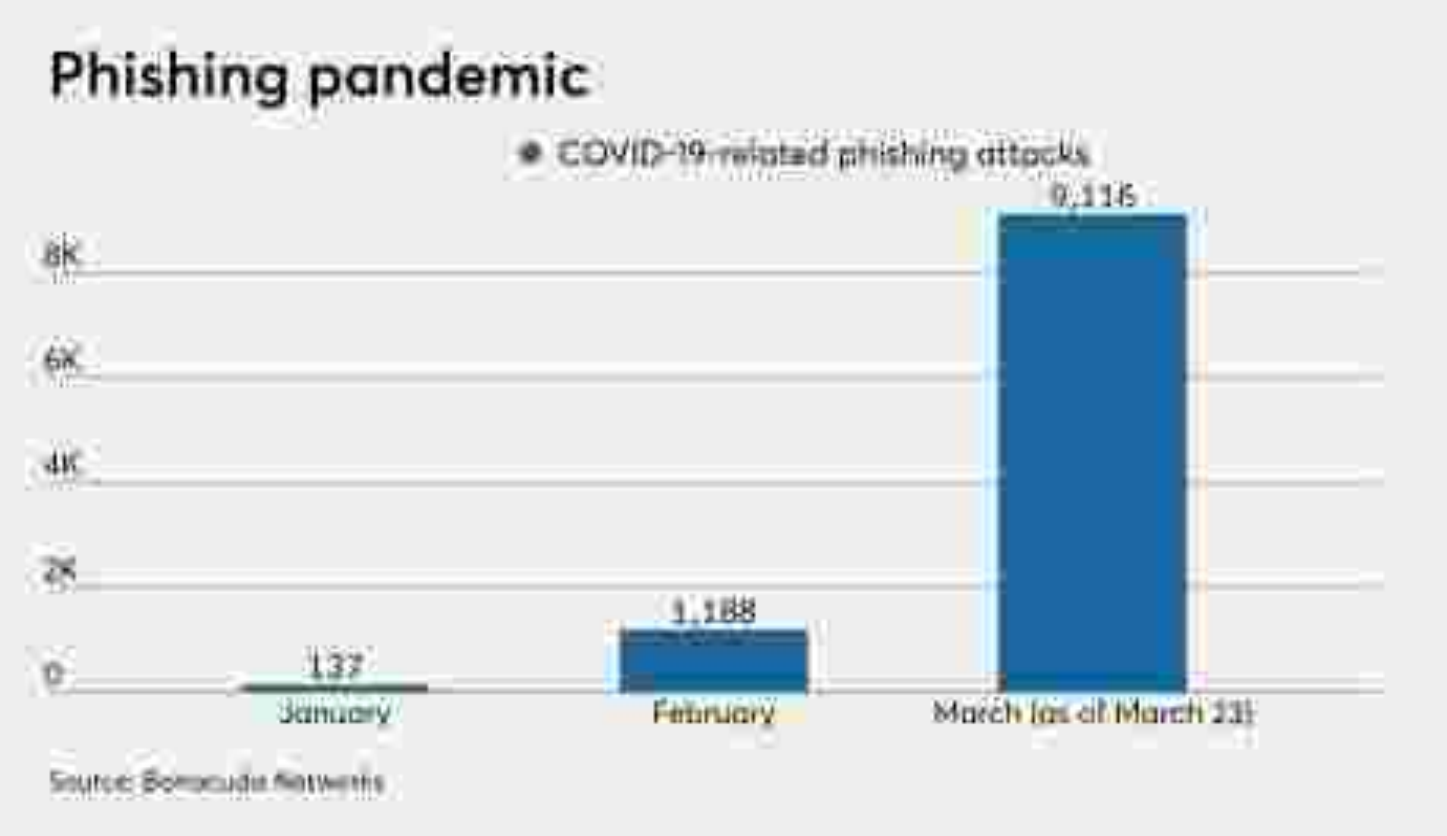
- **Mirai Attack**
  - Mirai took advantage of insecure IoT devices.
  - Scanned big blocks of the internet for open Telnet ports, then attempted to log in default passwords. In this way, it was able to a mass a botnet army.
  - On October 21, 2016 — Mirai botnet tested its capabilities by causing its millions of digital video recorders, routers, IP cameras, and other “smart” equipment to flood the DNS service provider
  - The DNS, as well as services that relied on it, became unavailable:
    - PayPal, Twitter, Netflix, Spotify, PlayStation online services
- **Ransomware Attack**
  - Locks user’s devices and prevents them from accessing data and software until a certain ransom is paid to its creator
  - Latest Ransomware also attacked power utilities
- **Video Bombing**
  - People unrelated to the user groups are found to be appearing/joining the calls as themselves or as famous celebrities in video conferencing

Impact of COVID 19 on Cyber Security

The COVID-19 outbreak has not only caused global disruption, it has also changed the cybersecurity threat landscape.

Different attack types became prominent

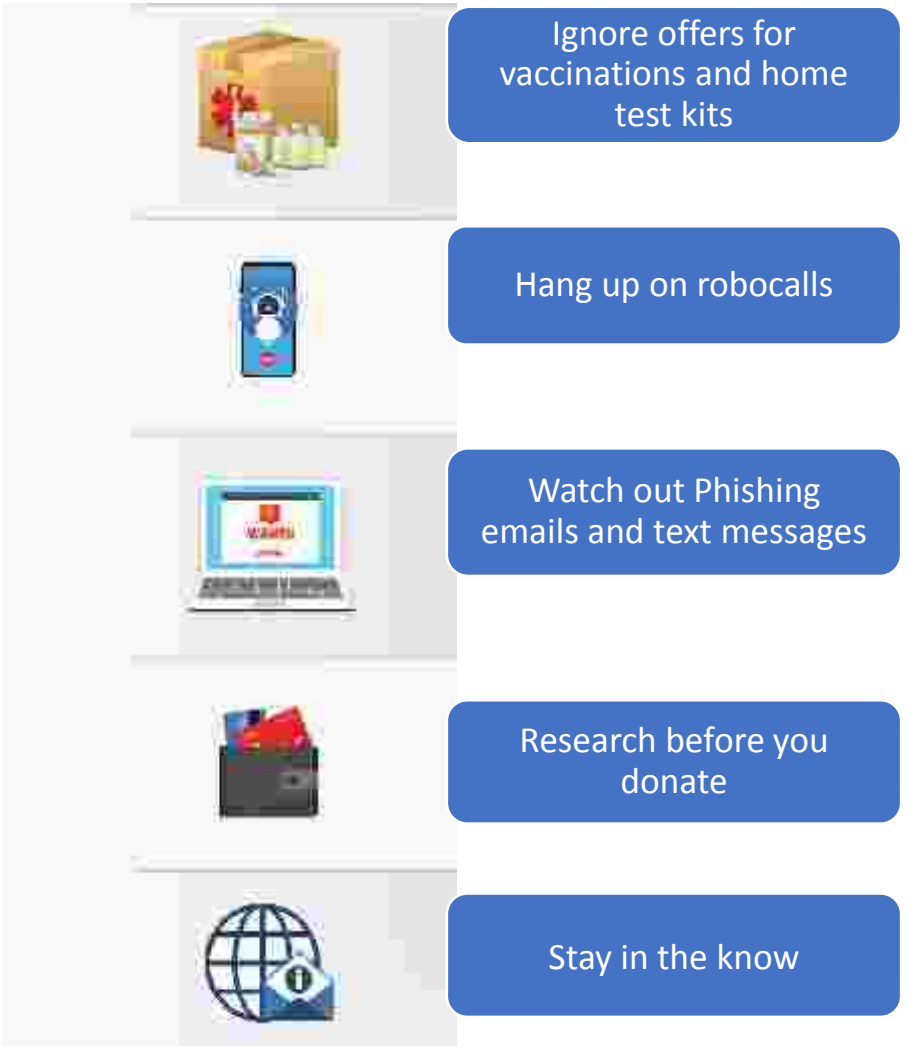
- Phishing Attacks
- Spear- Phishing Attacks
- Malware Attacks
- Ransomware Attacks
- Targeted Attacks
- Fake News
- Video-bombing
- DOS and DDOS Attacks
- Cross-site Scripting attacks
- Drive-by attacks



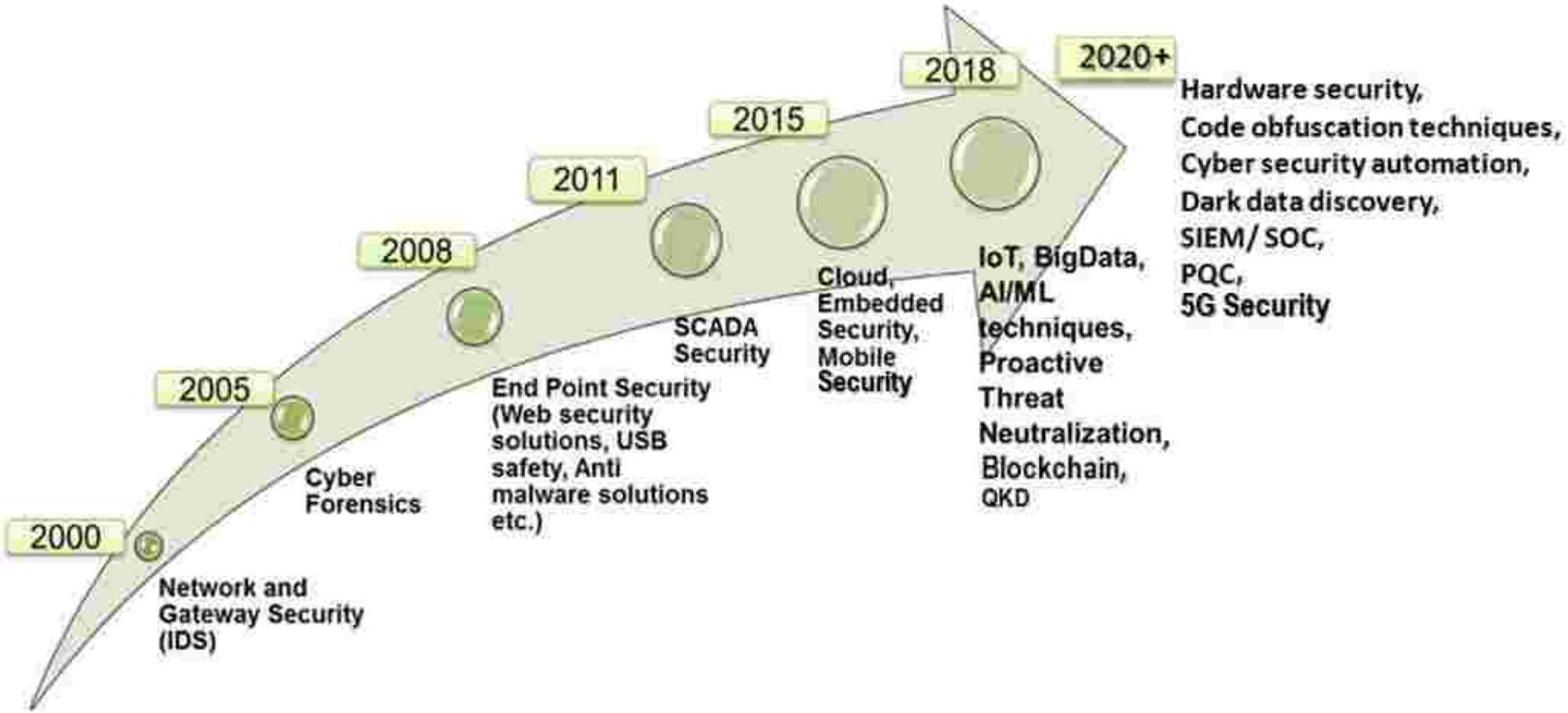
Beware of criminals during COVID 19 times: WHO's Inputs

- How to prevent phishing:
  - **Check their email address**
  - **Check the link before you click**
  - **Be careful when providing personal information**
  - **Do not rush or feel under pressure**
  - **If you gave sensitive information, don't panic**
  - **If you see a scam, report it**

- https://www.who.int/about/communications/cyber-security



Cyber Security – Evolution of Tech Based Solutions



Cyber Security Trends - 2020

Growing Attacks of Ransomware & Phishing

Integrating AI, & ML to Counter Security Threats

Expanding Cloud Security Threats

Mounting Mobile Apps Security Risks

Increasing Attacks on IoT Devices

Striking Cyber-Security Skills Gap

Increasing Investments in Cyber-Security

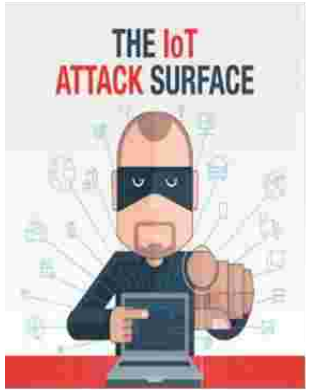
Mobile Security Attacks and Vulnerability Trends

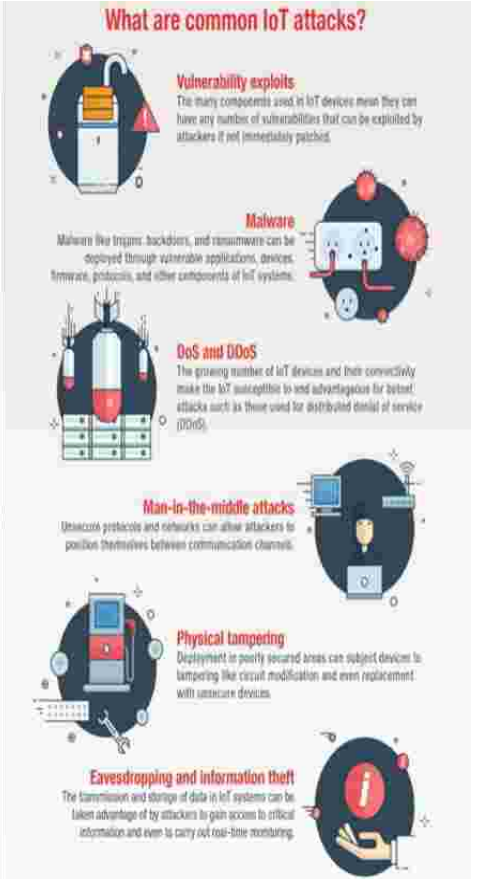
- Data leakage
- Social Engineering
- Wi-Fi interference
- Out of date devices
- Crypto-jacking Attacks
- Poor password hygiene
- Physical device breaches
- Mobile Ad fraud

IOT Security

IOT Security Issues

- Lack Of Compliance On The Part Of IoT Manufacturers
- Weak, guessable, or hard-coded passwords
- Hardware issues
- Lack of a secure update mechanism
- Old and unpatched embedded operating systems and software
- Insecure data transfer and storage
- High-jacking Your IoT Devices
- Rogue IoT Devices
- Industrial Espionage & Eavesdropping
- Crypto-mining With IoT Bots

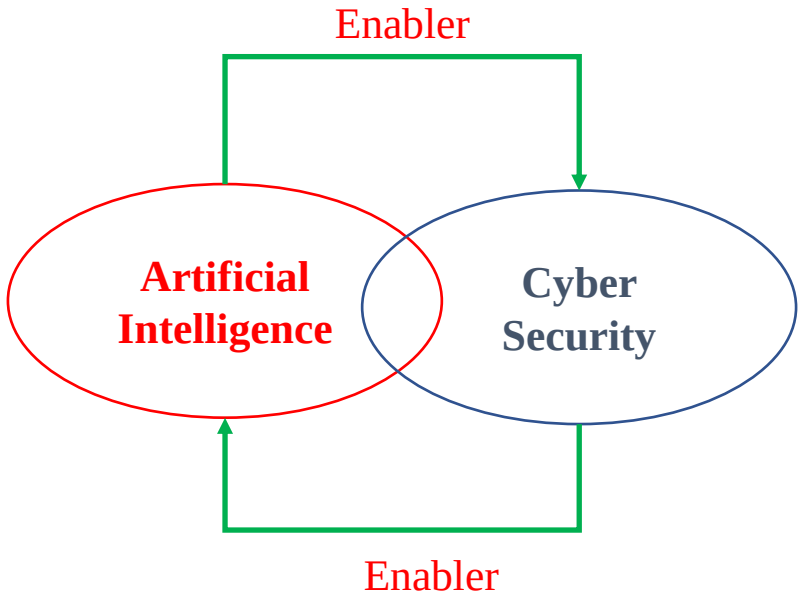




Need to Focus on

- Security by Design is the key requirement in securing the systems with IOT devices
- Evolving and complying to standards
- Light-weight Crypto due to constrained resources

AI & Cyber Security



- **AI and Cyber Security enables and complements each other to make system to work better and more safely and efficiently.**
- **AI enables new cyber security capabilities whereas cyber security enables a better AI and also prevents misuse of AI.**
- **Intersection of Figure shows how will Cyber (in)security impact the development of AI and how the rise of AI will alter the security landscape.**

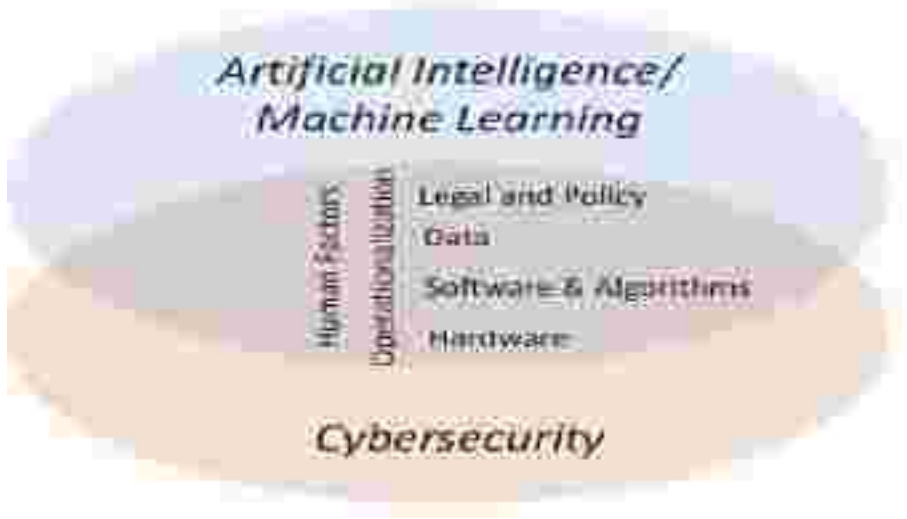
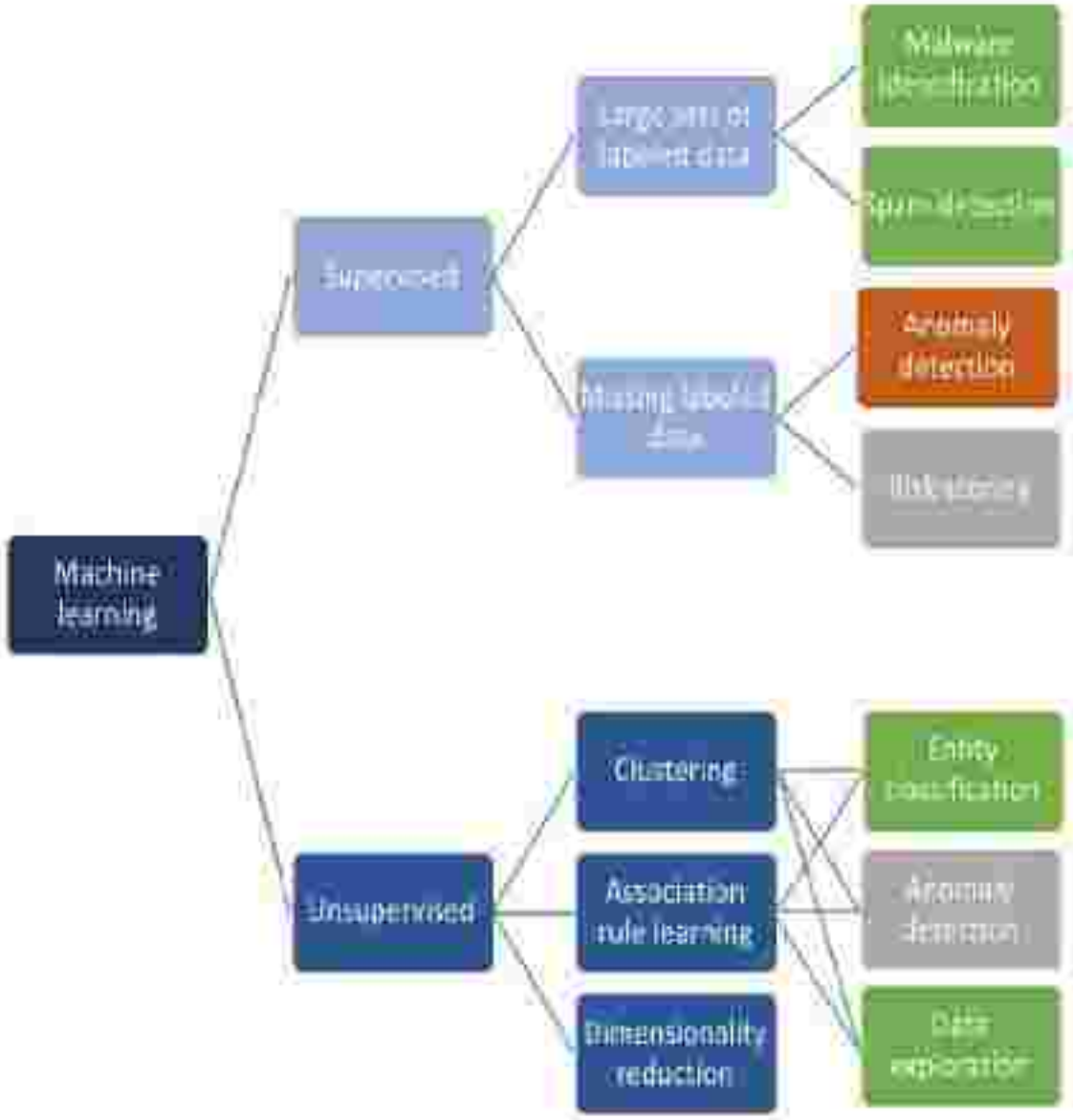


Figure shows the 6-dimensions of importance of AI-CS intersection (IEEE Confluence)

Use cases of AI/ ML in Cyber Security

- Network threat analysis
- Malware detection
- Security analyst augmentation
  - AI automates repetitive tasks
  - Raises the baseline of threat intelligence
    - to more rapidly analyse, curate, visualize and suggest potential actions
- AI-based threat mitigation
- Security for AI based Systems
  - Prevention from Data Poisoning
  - Verifiable Security from start to finish



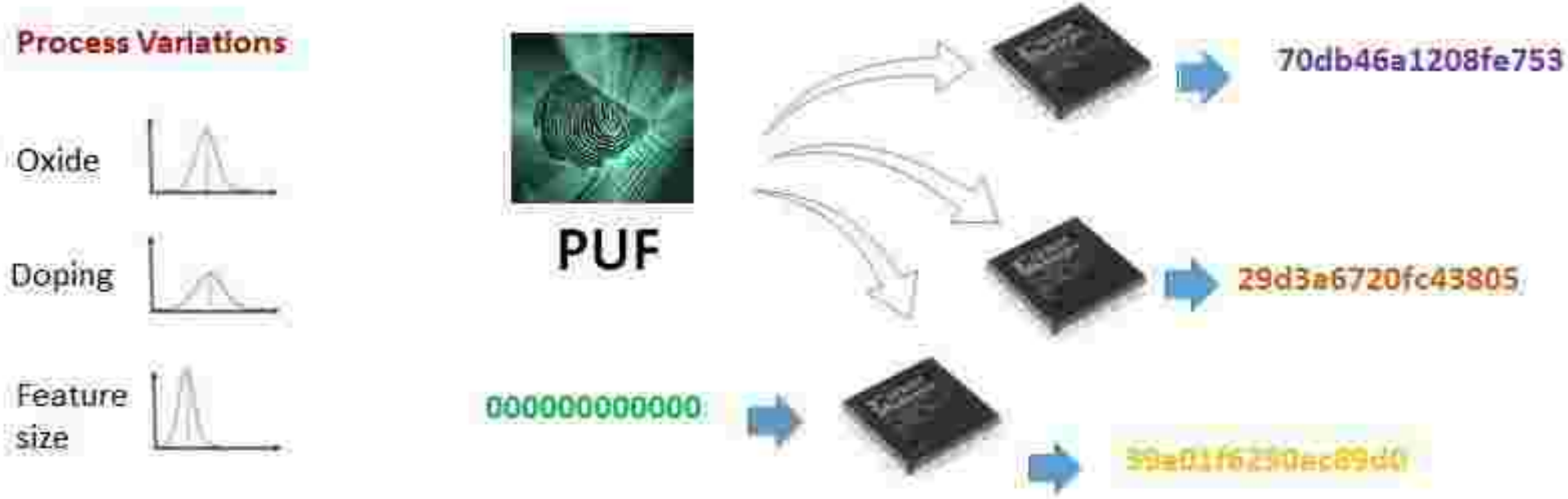
Hardware Trojan Detection

- Hardware Trojan (HT):
  Malicious modification of the original circuitry or designs
- What hardware Trojans can do:
  - Change the functionality
  - Leak valuable information or even destroy the chip
- Applications that are likely to be targets for attackers
  - Nuclear power plant, Space, Military etc.
- Hardware Trojan Detection techniques:
  - Intrusive
  - Non-Intrusive

Physical Unclonable Function (PUF)

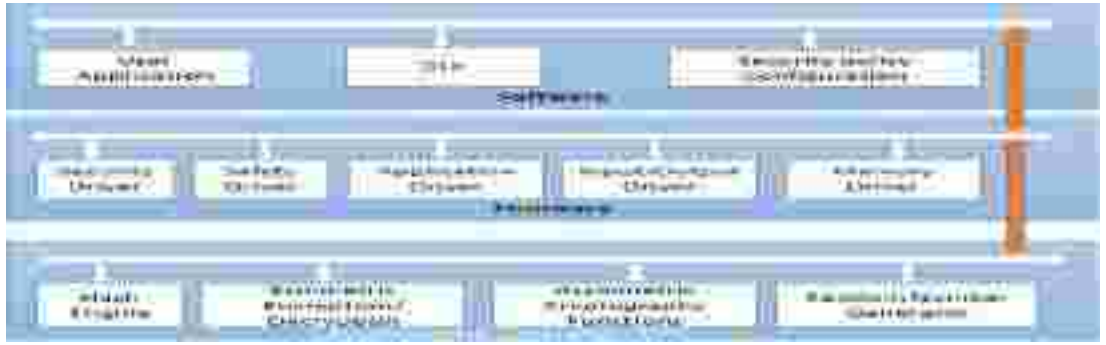
- A PUF (Physical Unclonable Function) is a digital circuit that uses manufacturing process variations to generate a unique digital fingerprint.

No two chips should give the same response when supplied with the same challenge.

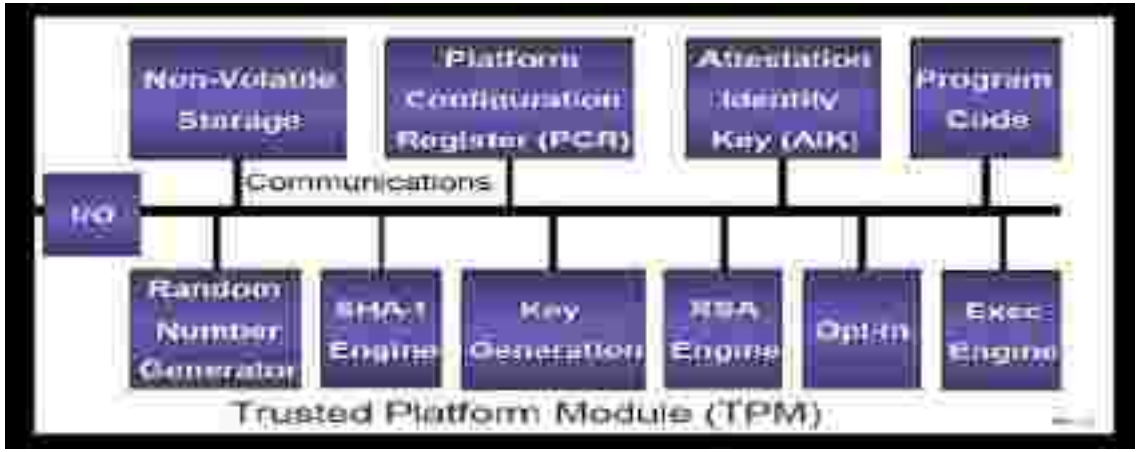


HSM & TPM

- A Hardware Security Module (HSM) is a security device you can add to a system to manage, generate, and securely store cryptographic keys.



- A Trusted Platform Module (TPM) is a hardware chip on the computer's motherboard that stores cryptographic keys, passwords, digital certificates.



Characteristics	TPM	HSM
Hardware	Chip in motherboard (included with many laptops)	Removable or external hardware device, (purchased separately)
Uses	Full disk encryption (for laptops and some servers)	High-end mission-critical servers (SSL accelerators, high availability clusters, certificate authorities)
Authentication	Performs platform authentication (verifies drive not moved)	Performs application authentication (only used by authorized applications)
Encryption Keys	RSA key burned into chip when created and can generate other keys	Stores RSA keys used in asymmetric encryption and can generate keys

Quantum Computing

- **Laws of Quantum Mechanics**
- **Bits are replaced with qubits**
- **Measurement gives the result**
- **Superposition of qubits gives speedup**

Are Quantum Computers Realizable?

- Michele Mosca estimates 1/7 chance of factorization of 2048 bit RSA modulus by 2026 and 1/2 by 2031
- Google demonstrates a 72 qubit system
- Intel begins testing a silicon-based spin-qubit processor
- D-Wave sells a 2000 qubit system

HISTORY

- 1982-Feynman proposed the idea of creating machines based on the laws of quantum mechanics instead of the laws of classical physics.
- 1985-David Deutsch developed the quantum Turing machine,showing that quantum circuits are universal.
- 1994-Peter Shor came up with a quantum algorithm to factor very large numbers in polynomial time.
- 1997-Lov Grover develops a quantum search algorithm with $O(\sqrt{N})$complexity.

Cyber Security in Quantum Era

- Quantum computers can solve factoring and discrete log problems in poly time: **Shor**
- Impact also symmetric key cryptography due to Grower & Simon Quantum Search Algorithms
- Two options for key problem:
  - a. use quantum key distribution
  - b. use quantum secure protocols (PQC)

Cyber Security - need of the hour

- Indigenous Technology and capability building
- Collaboration amongst R&D, academia and Industry
- Standards Compliance
- Creation of Cyber Security Test Labs
- Training and Awareness

References

- https://www.who.int/about/communications/cyber-security
- https://www.gartner.com/en/conferences/apac/security-risk-management-australia/gartner-insights/security-risk-trends
- https://www.ciodive.com/news/5-cybersecurity-trends-for-2020infographic-cyber-security-trends-to-know-in-2020.jpg.webp
- https://www.csoonline.com/article/3241727/8-mobile-security-threats-you-should-take-seriously-in-2020.html?
- http://www.darpa.mil/MTO/solicitations/baa07-24/index.html
- https://www.intellectsoft.net/blog/biggest-iot-security-issues/
- Source: Srinath Srinivasan, 19th August, 2019 - Cyber Security: Are IoT deployments in India safe from hackers?
  - Ref: https://www.financialexpress.com/industry/technology/cyber-security-are-iot-deployments-in-india-safe-from-hackers/1679046/

If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.

— Bruce Schneier —

Thank you!