भारत इलेक्ट्रॉनिक्स
BHARAT ELECTRONICS

Era of Digital Trust & Need of Indigenous Hardware Security

M Hemavathy
Bharat Electronics Ltd

Era of Digital Trust

- Web 3.0 is the next evolution of the internet, which promises to usher in a new era of connectivity and digital trust
  - open, decentralized web that gives users more control over their data and privacy.
  - Block chain technology enables secure and tamper-proof transactions and data storage
  - Zero trust Architecture
  - Adoption of Public Key Infrastructure (PKI) & AI Technologies

- Organizations has both a physical and a digital supply chain:
  - In internal IT environments, we can decide what controls are in place and what security is positioned in the environment
  - Digital supply chain, relies upon the third party making the right choices
- Increased proliferation & Adoption of AI & cloud technologies
- Challenges of Quantum Computing
- Key areas to Address:
  - Cyber security and privacy
  - digital governance and risk management
  - digital supply chain
  - Ethics and governance of AI

Need for Indigenous Hardware Security

Need of Indigenous Hardware Security

- Hardware Security refers to the protection of systems or physical devices from various global cyber threats which can compromise their security.

- Indigenous hardware security ensures the national security by preventing the backdoors and foreign surveillance that could be exploited by other nations.

- It is also essential for protecting national interests, reducing dependency on foreign entities and ensuring control over critical technologies.

- Major global cyber threats are
  - **Supply Chain Attacks**
  - **Hardware Trojans**
  - **Tampering**
  - **Side-channel Attacks**
  - **Electromagnetic Interference and Fault Injection**
  - **Eavesdropping and snooping**
  - **Firmware Attacks**

Protective measures of Hardware Security

- **Secure boot :** Ensures only trusted and digitally signed firmware and software are loaded during boot process

- **Trusted Platform Modules (TPM)** : Hardware module that is used for secure boot, device authentication and sensitive data storage

- **Trusted Execution Environments (TEEs)** : These are isolated areas within a processor where sensitive data and operations can be securely executed without interference from the rest of the system

- **Hardware Security Modules (HSM)** : Its a dedicated device for cryptographic operations and sensitive parameters storage such as keys, passwords and certificates

- **Physically Unclonable Functions (PUFs)** : It’s a security primitive used to uniquely identify and authenticate hardware devices based on their intrinsic physical characteristics.

- **Tamper resistant circuit and package** : Detect and prevent unauthorized access or physical attack on hardware

Hardware Imports: Global Scenario

- 89.8 billion USD of electronics, telecom and electrical products as per Global Trade Research Initiative (GTRI) report for the year 2023-24.
- Most of the electronics hardware imports from China and Hong Kong
- Nearly all ICs for electronic products are procured from outside country
- Pager attack is one example of supply chain hardware security vulnerabilities

Import Disadvantages:-

- Most of the products and technologies are imported from border countries and socio economical policy(i.e., sovereignty, strategic autonomy) restrictions imposed by countries
- Continuous surveillance: Products (CC cameras, network products)/Servers (App data storage)
- Difficult to control emergency situations like war or resource scarcity
- Restrictions:-Materials/Tools/Components/Design/Expertise/ToT/Sub-modules/Products import/ Market/Financial restrictions

Indigenization: Govt & Industry Perspective

Advantages from Government Perspective

- Self reliance/ Strategic importance for the country/Atmanirbhar Bharat
- Independent employment opportunities
- Improved Economy
- Foreign exchange savings and earnings
- Accountability of the chip or product manufacturer

Advantages from Industry Perspective

- Product Obsolescence can be minimized with enhanced life cycle management
- Customization to meet country specific needs/ Innovation can be carried out from small to large scale
- Cost saving and profit improvement in mass scale production
- Knowledge in design, development, testing and validation, standardisation
- IP Protection

Indigenization Challenges/Approaches

Challenges:

- Market Potential for continuous revenue generation
- Huge fund requirement/Lack of Investments(Investments orientation towards ROI)
- Expertise/ Government Policies
- Technological Gap with established foreign players
- Rapid technological growth in terms of policy, process adaptability, miniaturization,cost, time to market

Approaches:

- Promoting commercial market towards indigenous solutions ex. Make In India Policy
- Establishment of indigenous IC fabrication and design industries
- Long term Sustainability plan
- Introducing Standardisations (Design and testing) and Certifications for hardware security
- Technical documentation of design and development details for its usage
- Moderating IP restrictions(patents, copy rights etc.) for indigenization

Indigenization Challenges/Approaches

Challenges:

- Market Potential for continuous revenue generation
- Huge fund requirement/Lack of Investments(Investments orientation towards ROI)
- Expertise/ Government Policies
- Technological Gap with established foreign players
- Rapid technological growth in terms of policy, process adaptability, miniaturization,cost, time to market

Approaches:

- Promoting commercial market towards indigenous solutions ex. Make In India Policy
- Establishment of indigenous IC fabrication and design industries
- Long term Sustainability plan
- Introducing Standardisations (Design and testing) and Certifications for hardware security
- Technical documentation of design and development details for its usage
- Moderating IP restrictions(patents, copy rights etc.) for indigenization

BEL Cyber Security & PKI Capabilities/Roadmap

- ✓ Indigenous PKI Token & Hardware Security Module (HSM)
- ✓ Indigenous Registration Authority & Certification Authority
- ✓ Block chain framework
- ✓ Quantum Safe RA&CA
- ✓ Post Quantum Crypto based HW Encryptor
- ✓ Quantum Key Distribution
- ✓ E-Sign Framework(Code signing)
- ✓ EAL4 Data diode for air gap
- ✓ Security solutions: NGFW, AAA, EDR, WAF, SIEM, SOAR, ZTNA

Thank you

Cyber Threats - Hardware

- Hardware Security : Protection of physical devices from cyber threats which can compromise their security

- Cyber threats:
    - Supply Chain Attacks : Introduction of malicious components during manufacturing or distribution process of hardware components
    - Hardware Trojans: Introduction of malicious circuitry or firmware modification to hardware components to leak sensitive information or disrupt system operation
    - Side-channel Attacks: Attacks exploits unintentional information leakage from hardware components such as power consumption, electro magnetic leaks and timing information to extract the sensitive data.
    - Tampering : Physical access to hardware components which enables adversaries to extract data, modify firmware or install malicious hardware components and posing a risk to sensitive system
    - Electromagnetic Interference and Fault Injection : EMI is a disturbance caused with electro magnetic field to interfere the normal operations of electronic devices which affects the performance, stability or security of a system. Fault injection refers to the deliberate induction of errors or faults into a system to observe the behavior and discover weaknesses.