Security of the Internet of Things (IoT), Hardware Security: Part 3

Gaurav S. Kasbekar
Dept. of Electrical Engineering
IIT Bombay

References

- W. Stallings, "*Cryptography and Network Security*", 8th edition, Pearson Education, 2023
- P. Lea, "*IoT and Edge Computing for Architects",* Packt Publishing Ltd., 2020
- D. Hanes, G. Salgueiro, P. Grossetete, R. Barton, and J. Henry, "*IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things",* Cisco Press, 2017

Tamper Resistance and Detection

- IoT ecosystem involves a large number of devices deployed in edge network
- These are from numerous manufacturers and deployed in areas where physical security is difficult
- Two essential security measures in such an environment are tamper resistance and tamper detection
- Tampering:
  - ❑ Unauthorized modification that alters intended functioning of a system or device in a way that degrades the security it provides
- Tamper Resistant:
  - ❑ A characteristic of a system component that provides passive protection against an attack
- Tamper Detection:
  - ❑ Techniques to ensure that the overall system is made aware of unwanted physical access

Tamper Resistance

- A common approach to tamper resistance is to use specialized physical construction materials to make tampering with a fog node difficult
- Examples include hardened steel enclosures, locks, and security screws
- Tightly packing components and circuit boards within an enclosure increases the difficulty of using fiber optics to probe inside the node without opening the enclosure
- A second category of tamper resistance is deterrence of tampering by ensuring that tampering leaves visible evidence behind:
  - ❑e.g., special seals and tapes that make it obvious when there has been physical tampering

Tamper Detection

- Mechanisms for tamper detection include the following
- Switches:
  - ❑Variety of switches, such as mercury switches, magnetic switches, and pressure contacts can detect the opening of a device, the breach of a physical security boundary, or the movement of a device
- Sensors:
  - ❑Temperature and radiation sensors can detect environmental changes
  - ❑Voltage and power sensors can detect electrical attacks
- Circuitry:
  - ❑Possible to wrap components with flexible circuitry, resistance wire, or fiber optics so as to detect a puncture or break

Lightweight Cryptography

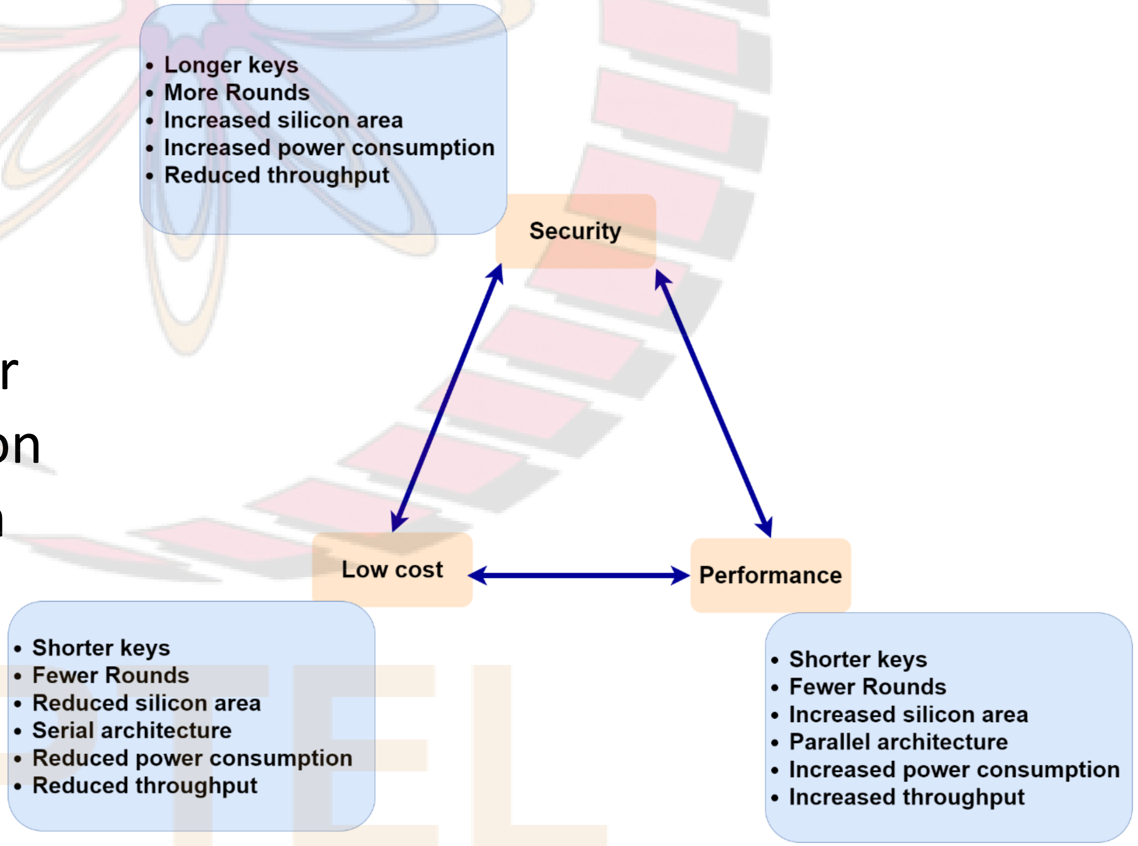
- Focused on developing algorithms that, while secure, minimize execution time, memory usage, and power consumption
- Such algorithms are suitable for resource-constrained devices and small embedded systems such as those in wide use in the IoT
- Work on lightweight cryptography is devoted to symmetric key algorithms and cryptographic hash functions
- Lightweight cryptography includes attempts:
  - ❑ to develop efficient implementations of conventional cryptographic algorithms, and
  - ❑ to design new lightweight algorithms

Constrained Devices

- Constrained device is one with:
  - ❑ limited volatile and non-volatile memory,
  - ❑ limited processing power, and
  - ❑ a low data-rate transceiver
- Many devices in the IoT, particularly the smaller, more numerous devices, are resource constrained
- Typical constrained devices are equipped with 8 or 16 bit microcontrollers that possess very little RAM and storage capacities
- Resource-constrained devices are often equipped with an IEEE 802.15.4 radio, which enables low-power low-data-rate wireless personal area networks (WPANs) with data rates of $20 - 250$ kbps and frame sizes of up to 127 bytes

Design Trade-offs

- Fig. illustrates trade-offs between security, cost, and performance in designing lightweight cryptographic algorithms
- In general, longer the key and the more rounds, the greater the security
- This implies a reduced throughput, in terms of the amount of plaintext processed per time unit, as well as increased power consumption
- Similarly, the more complex an algorithm or its implementation, the more security it can provide, but this generally requires increased silicon area, either for hardware implementation or software implementation
- Thus, achieving greater security can degrade either cost or performance objectives or both



Lightweight Cryptographic Algorithms

- To meet the requirements of lightweight cryptography, a number of new algorithms have been proposed
- Typical characteristics include:
  - ❑ Many iterations of simple rounds
  - ❑ Simple operations like XORs, rotation, 4×4 S-boxes, and bit permutations
  - ❑ Smaller block sizes (e.g., 64 or 80 bits)
  - ❑ Smaller key sizes (e.g., 96 or 112 bits)
  - ❑ Small security margins by design
    - o *security margin of a cipher*: difference between number of rounds in the complete implementation of the cipher and maximum number of rounds that are known to be breakable using best-known real-world attack
- These design choices yield smaller security margins compared to established algorithms such as AES and SHA-2

Lightweight Block Ciphers and Cryptographic Hash Functions

- An example of a lightweight cryptographic block cipher is the Scalable Encryption Algorithm (SEA)
- Two ways in which lightweight hash functions differ from more traditional ones are:
  - ❑Smaller internal state and output sizes
  - ❑Smaller message (input) size
- An example of a lightweight cryptographic hash function is PHOTON