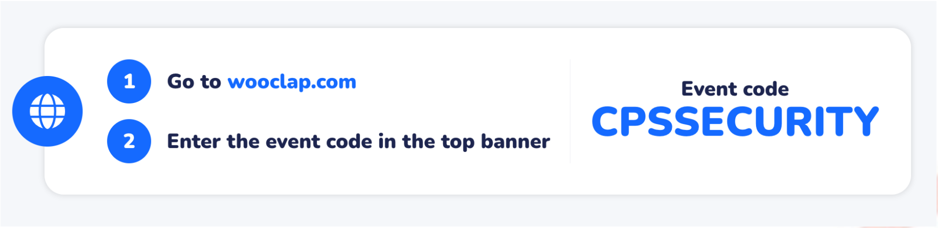
CE/CZ4055 Cyber Physical System Security

Key Management

Anupam Chattopadhyay
CCDS, NTU



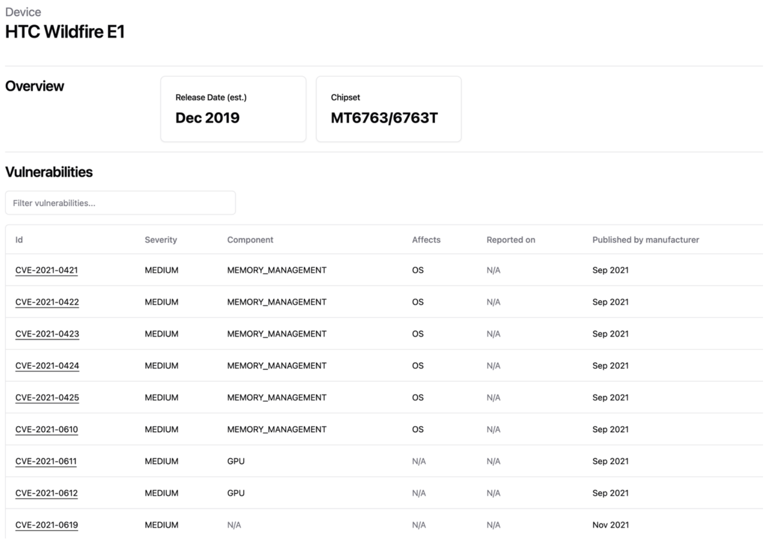
1 Go to wooclap.com

2 Enter the event code in the top banner

Event code
CPSSECURITY

Microprocessor Vulnerability

Academic community maintaining vulnerabilities across devices and chipsets.



Device

HTC Wildfire E1

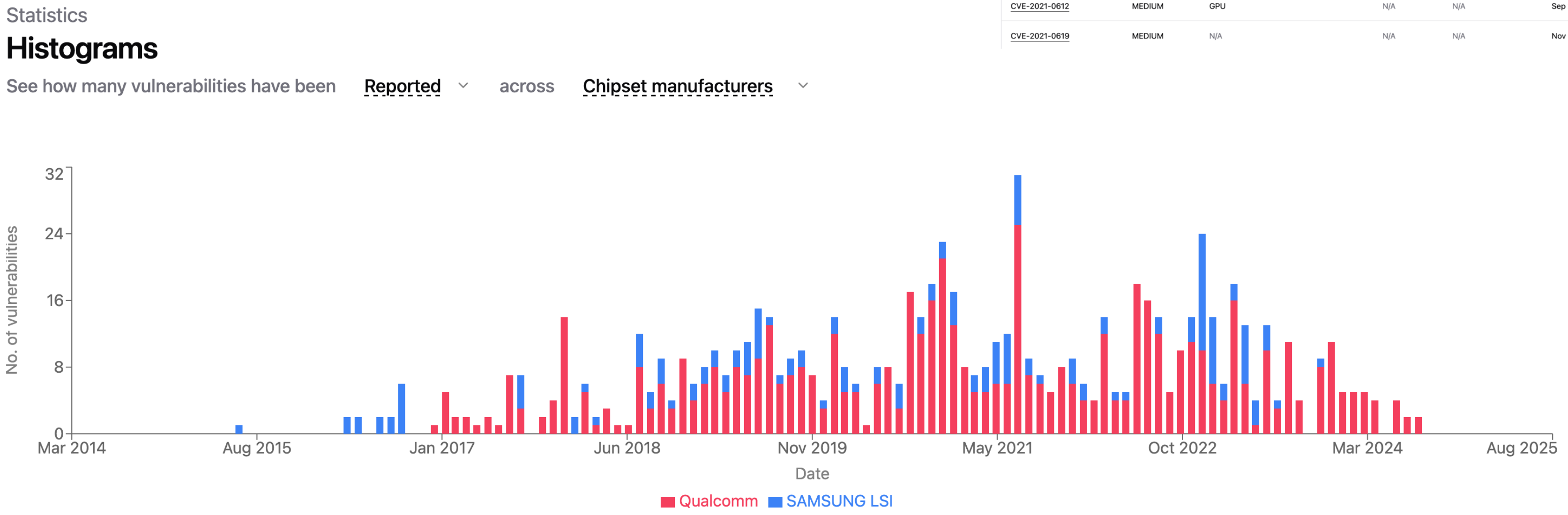
Overview

Release Date (est.)	Chipset
Dec 2019	MT6763/6763T

Vulnerabilities

Filter vulnerabilities...

Id	Severity	Component	Affects	Reported on	Published by manufacturer
CVE-2021-0421	MEDIUM	MEMORY_MANAGEMENT	OS	N/A	Sep 2021
CVE-2021-0422	MEDIUM	MEMORY_MANAGEMENT	OS	N/A	Sep 2021
CVE-2021-0423	MEDIUM	MEMORY_MANAGEMENT	OS	N/A	Sep 2021
CVE-2021-0424	MEDIUM	MEMORY_MANAGEMENT	OS	N/A	Sep 2021
CVE-2021-0425	MEDIUM	MEMORY_MANAGEMENT	OS	N/A	Sep 2021
CVE-2021-0610	MEDIUM	MEMORY_MANAGEMENT	OS	N/A	Sep 2021
CVE-2021-0611	MEDIUM	GPU	N/A	N/A	Sep 2021
CVE-2021-0612	MEDIUM	GPU	N/A	N/A	Sep 2021
CVE-2021-0619	MEDIUM	N/A	N/A	N/A	Nov 2021



Statistics

Histograms

See how many vulnerabilities have been Reported across Chipset manufacturers

https://www.chipsets.org/

D. Klischies et al, "Vulnerability, Where Art Thou? An Investigation of Vulnerability Management in Android Smartphone", NDSS 2025

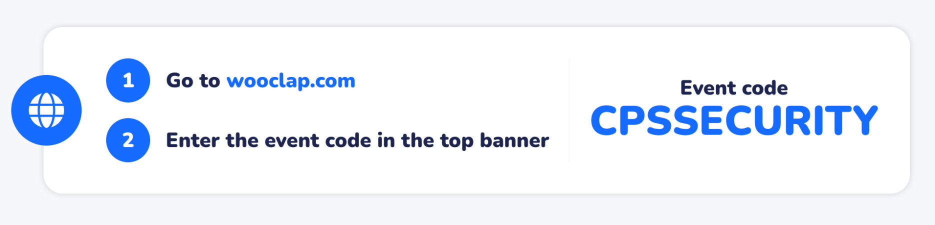
Kerckhoffs' Principle

A cryptosystem should be secure even if everything about the system, *except the key*, is public knowledge

No *security through obscurity*

Contents

- *Key Management Systems*
- Key Management for Wireless Sensor Networks
- Discussion



1 Go to wooclap.com

2 Enter the event code in the top banner

Event code

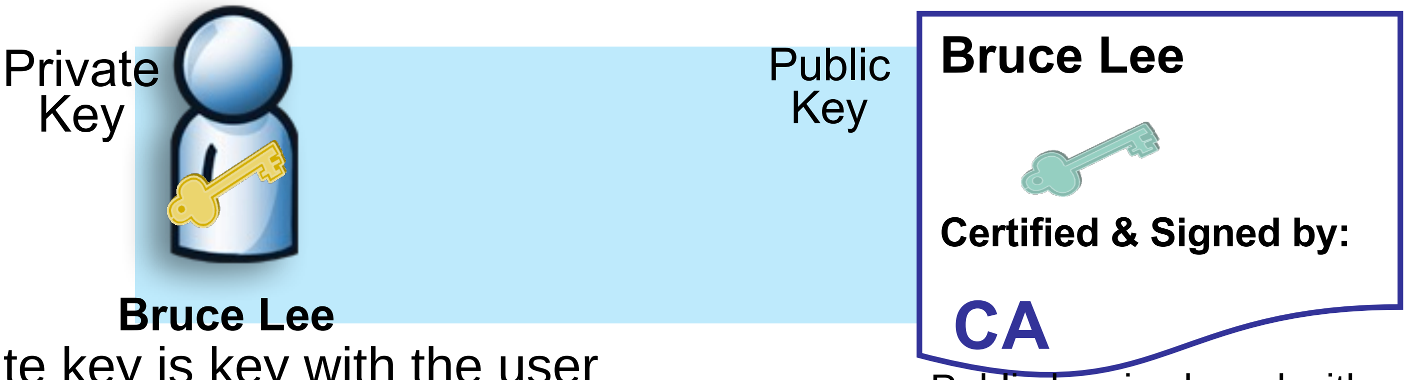
CPSSECURITY

NANYANG TECHNOLOGICAL UNIVERSITY

Every user has a private key and public key

What is a Digital Identity?

- **An asymmetric key pair assigned to a particular individual**
  - Implemented using a digital certificate
  - Contains information about you…name etc. plus your public key
  - Certificate is digitally signed by a trusted source



Private Key

Bruce Lee

Public Key

Bruce Lee

Certified & Signed by:

CA

Private key is key with the user

Public key is shared with everyone.
It is a Digital Certificate issued by a PKI

- **How do you use your digital identity?**
  - Use your private key digitally sign documents
  - Others verify your signature with the public key on your certificate

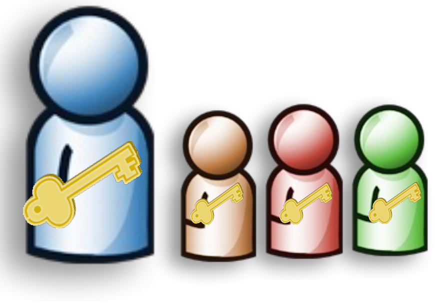
Other ppl can use my public key to encrypt the messages and ONLY I can decrypt it
Because I am the only one with the private key

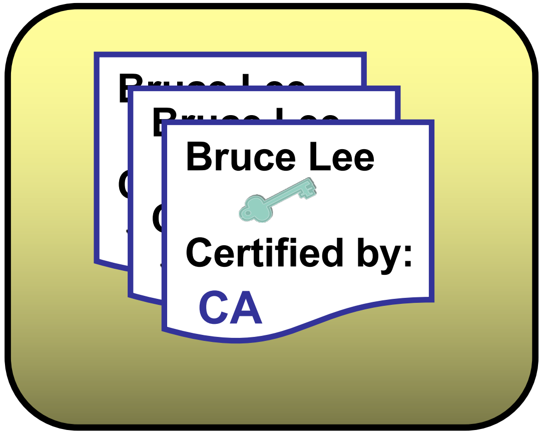
What is a PKI?

- A Public Key Infrastructure (PKI) is a system to deploy and manage digital identities

PKI CAN -->

- **Issue** digital identities
- **Revoke** digital identities
- **Publish** public keys via directories



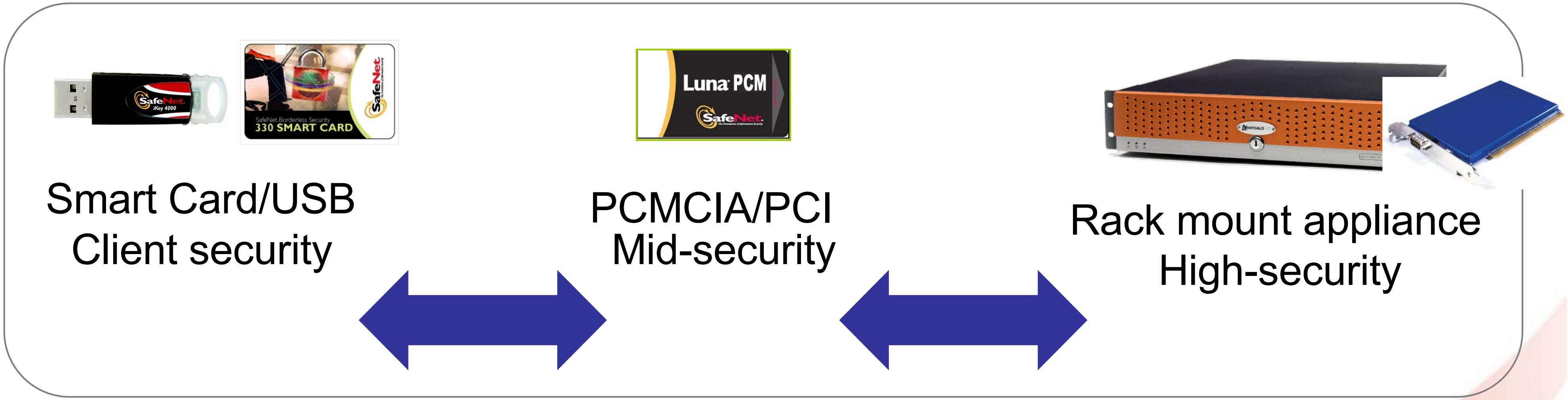


What is a Hardware Security Module (HSM)?

Basically like mom's company USB to access the laptop

- Security: A device to keep private keys secure
- Performance: Accelerate encryption operations to eliminate bottlenecks
- Audit: Provides a clear audit trail

Wide range of Security, Performance, Scalability & Price



Smart Card/USB
Client security

PCMCIA/PCI
Mid-security

Rack mount appliance
High-security

Types of HSMs

- HSM **USB**

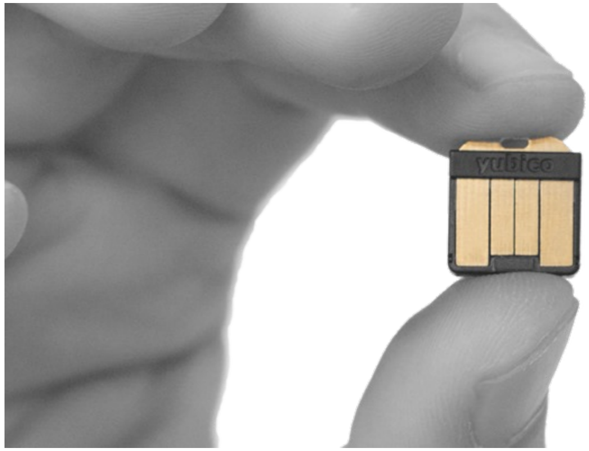
- HSM embedded in **Desktop**

- HSM in **Cloud**

NANYANG TECHNOLOGICAL UNIVERSITY

Portable HSM

- Small Form Factor
  - USB
  - Smartcard



Smartcard HSM

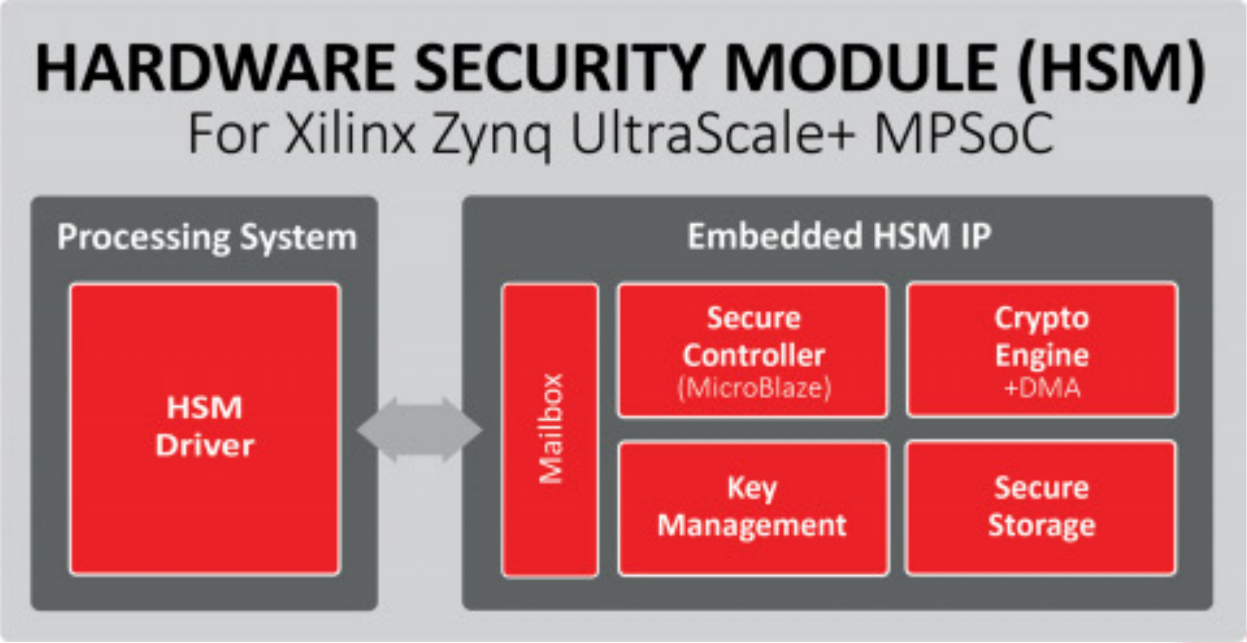
- Smartcard HSM hosts a built-in key-pair, which can be authenticated by a certificate issuer, or card service provider

- Interface: contact/contactless with standard readers that support ISO-7816 or ISO14443

- Personalization for an user, easy to deploy and maintain for strict access controls

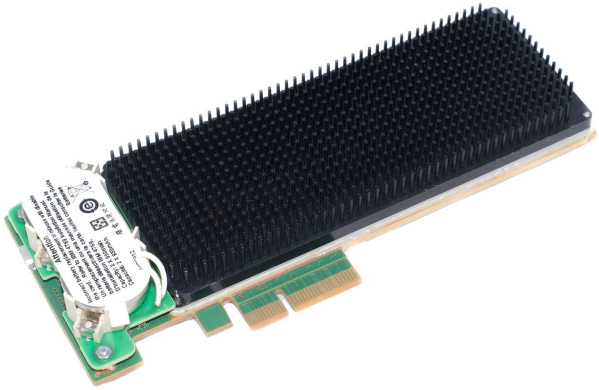
USB HSM, HSM as IP

- OTP access
- 2-factor authentication
- Secure (encrypted) password storage
- Encrypted mass storage



Embedded HSM

- Interface
  - PCI-Express X4, PCI CEM 1.0a
- Cheaper, lower performance than cloud-based HSM



Network-attached HSM

- Benefits
  - Load sharing, Easily upgradable
  - Supporting multiple users (over cloud, multiple partitions)
- Tamper resistance through built-in chassis
- Mode of deployment
  - Private/Public cloud

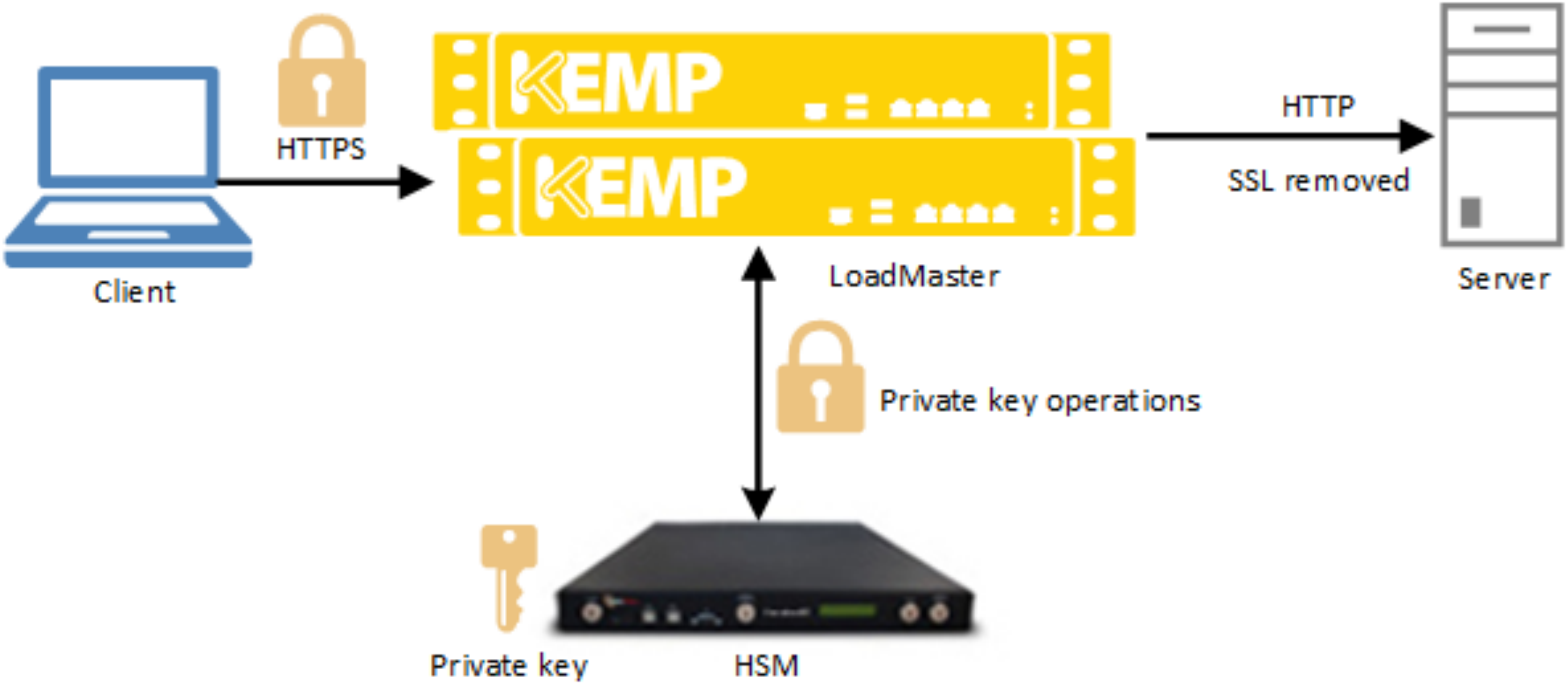
- *Example: Thales Luna Network HSM*
  - 2 options: 4 Gigabit ethernet ports with Port Bonding
  - 2 x 10G fibre network connectivity and 2 x 1G with Port Bonding
    - IPv4 and IPv6

Network-attached HSM: Example

- **Thales Luna Network HSM**

- Supported Operating Systems
  - Windows, Linux, Solaris, AIX
  - Virtual: VMware, Hyper-V, Xen, KVM
- API Support
  - PKCS#11, Java (JCA/JCE), Microsoft CAPI and CNG, OpenSSL
  - REST API for administration
- Cryptography
  - Asymmetric: RSA, DSA, Diffie-Hellman, Elliptic Curve Cryptography (ECDSA, ECDH, Ed25519, ECIES)
  - Symmetric: AES, AES-GCM, Triple DES, DES, ARIA, SEED, RC2, RC4, RC5, CAST
  - Hash/Message Digest/HMAC: SHA-1, SHA-2, SHA-3, SM2, SM3, SM4

Network-attached HSM: Sample Configuration



Load Balancing through Kemp LoadMaster

Key Management using HSM

- **Challenges**
  - **Key Generation, Replacement and Retiring**
  - **Key Distribution** *(partly addressed by PKI)*

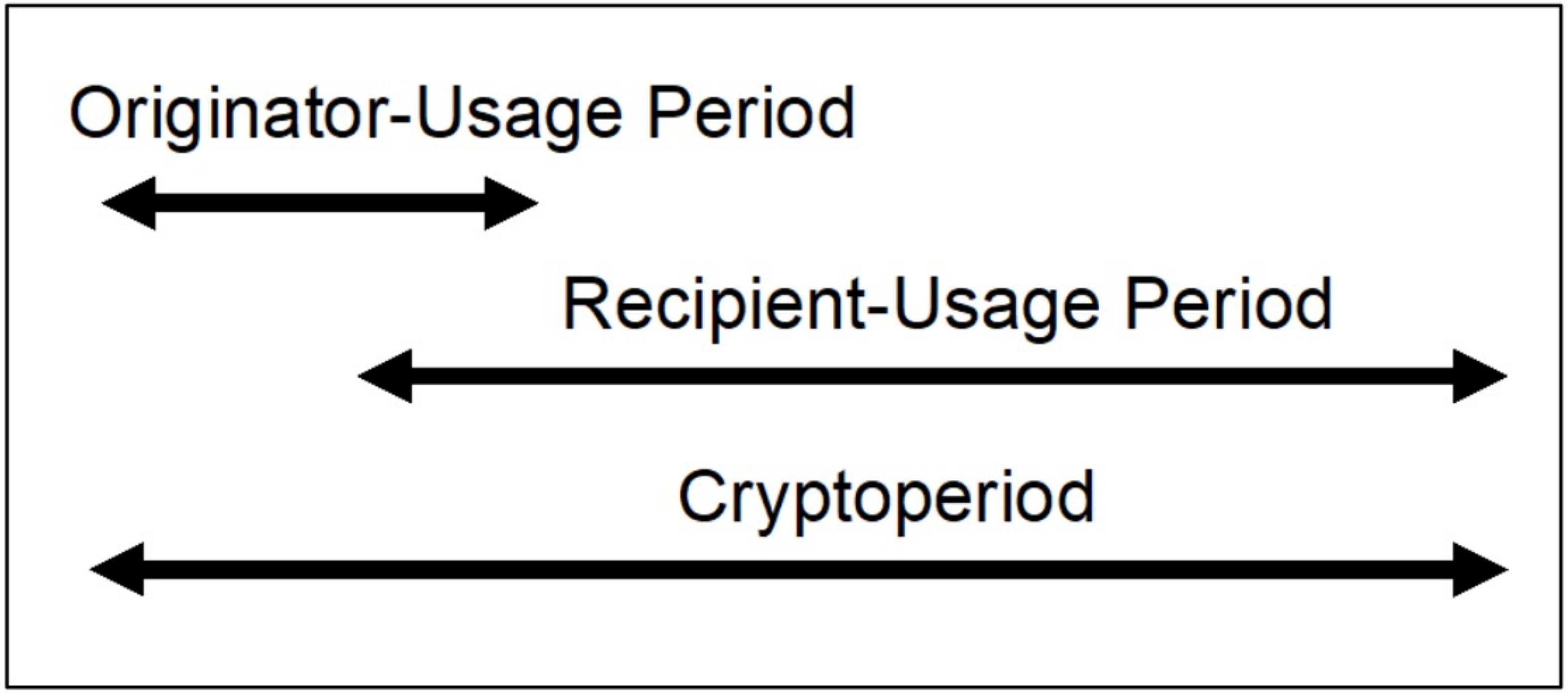
- **NIST Recommendation (**NIST Special Publication 800-57 Part 1**)**
  - *"The proper management of cryptographic keys is essential to the effective use of cryptography for security. Keys are analogous to the combination of a safe…Ultimately, the security of information protected by cryptography directly depends on the strength of the keys, the effectiveness of mechanisms and protocols associated with the keys, and the protection afforded to the keys."*

Key Management using HSM *(contd.)*

A cryptoperiod is the time span during which a specific key is authorized for use by legitimate entities or the keys for a given system will remain in effect. A suitably defined cryptoperiod:

- Limits the amount of information that is available for cryptanalysis to reveal the key (e.g. the number of plaintext and ciphertext pairs encrypted with the key);
- Limits the amount of exposure if a single key is compromised;
- Limits the use of a particular algorithm;
- Limits the time available for computationally intensive cryptanalysis.

Key Management using HSM *(contd.)*

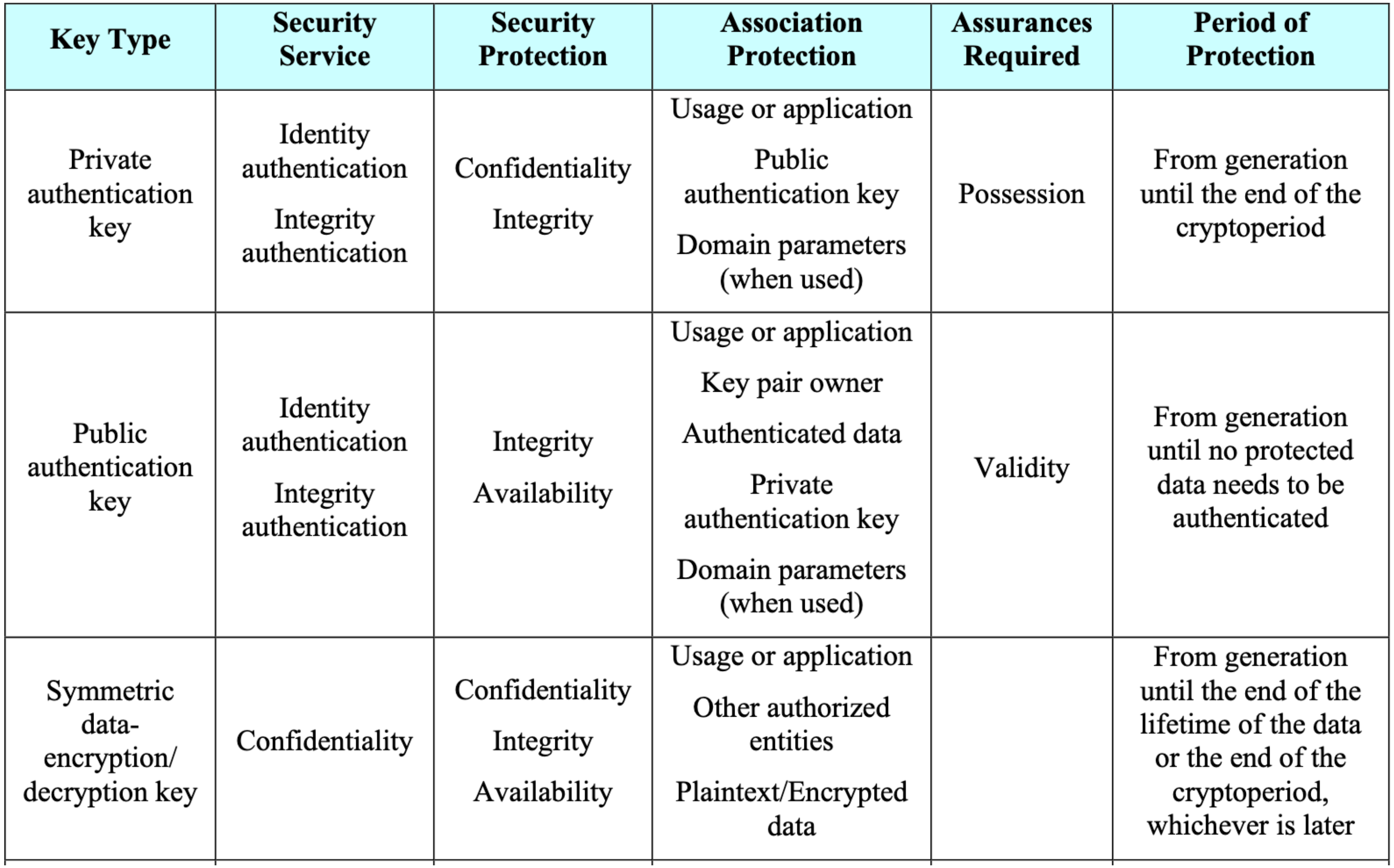


Originator-Usage Period

Recipient-Usage Period

Cryptoperiod

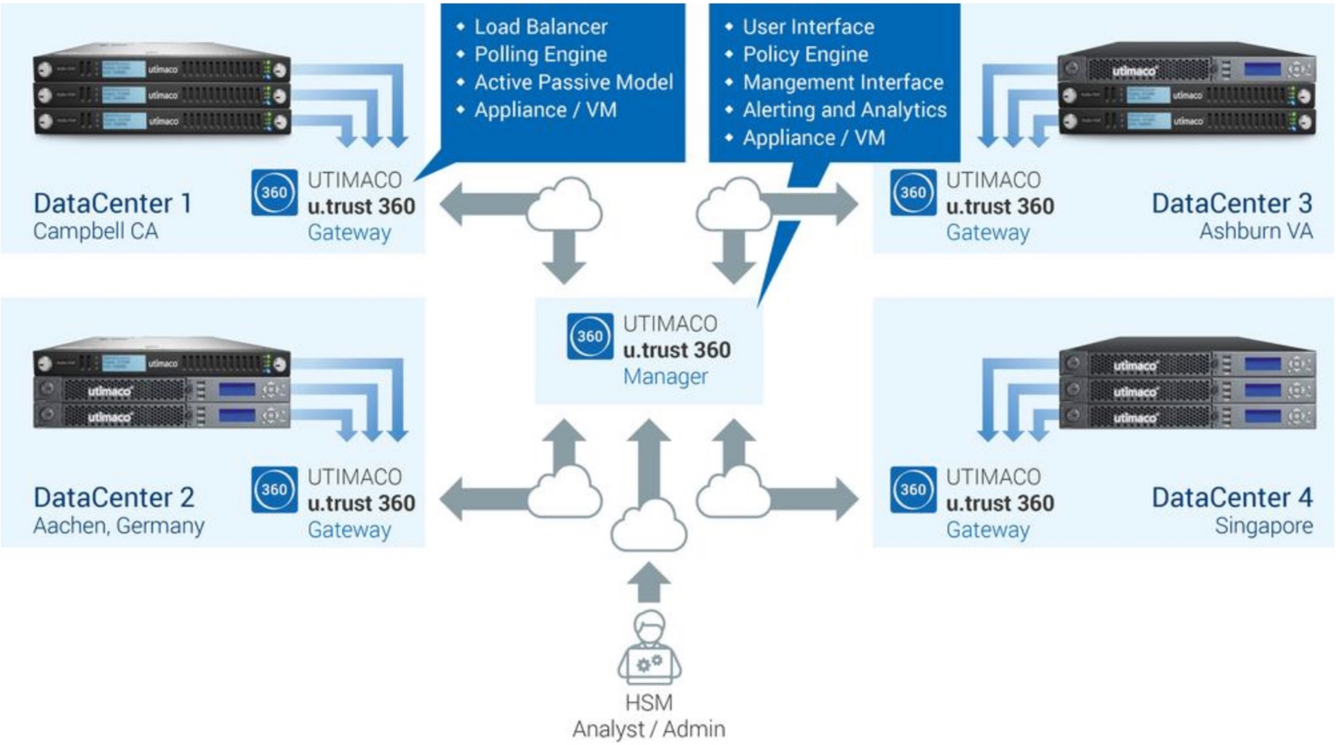
Key Management using HSM *(contd.)*



Key Type	Security Service	Security Protection	Association Protection	Assurances Required	Period of Protection
Private authentication key	Identity authentication Integrity authentication	Confidentiality Integrity	Usage or application Public authentication key Domain parameters (when used)	Possession	From generation until the end of the cryptoperiod
Public authentication key	Identity authentication Integrity authentication	Integrity Availability	Usage or application Key pair owner Authenticated data Private authentication key Domain parameters (when used)	Validity	From generation until no protected data needs to be authenticated
Symmetric data-encryption/ decryption key	Confidentiality	Confidentiality Integrity Availability	Usage or application Other authorized entities Plaintext/Encrypted data		From generation until the end of the lifetime of the data or the end of the cryptoperiod, whichever is later

Types of keys

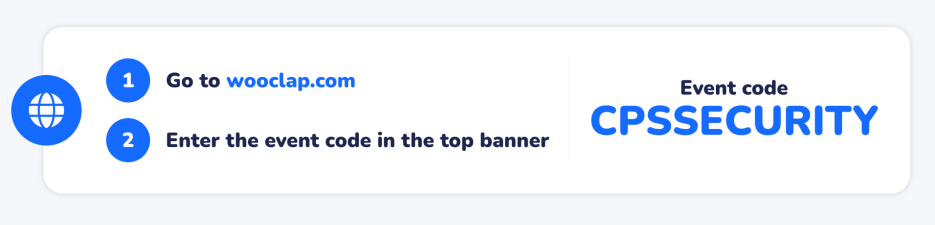
Key Management using HSM: Utimaco Example



The central management and monitoring solution for Atalla and CryptoServer LAN V5 HSMs

Contents

- Key Management Systems
- *Key Management for Wireless Sensor Networks*
- Discussion



1 Go to wooclap.com

2 Enter the event code in the top banner

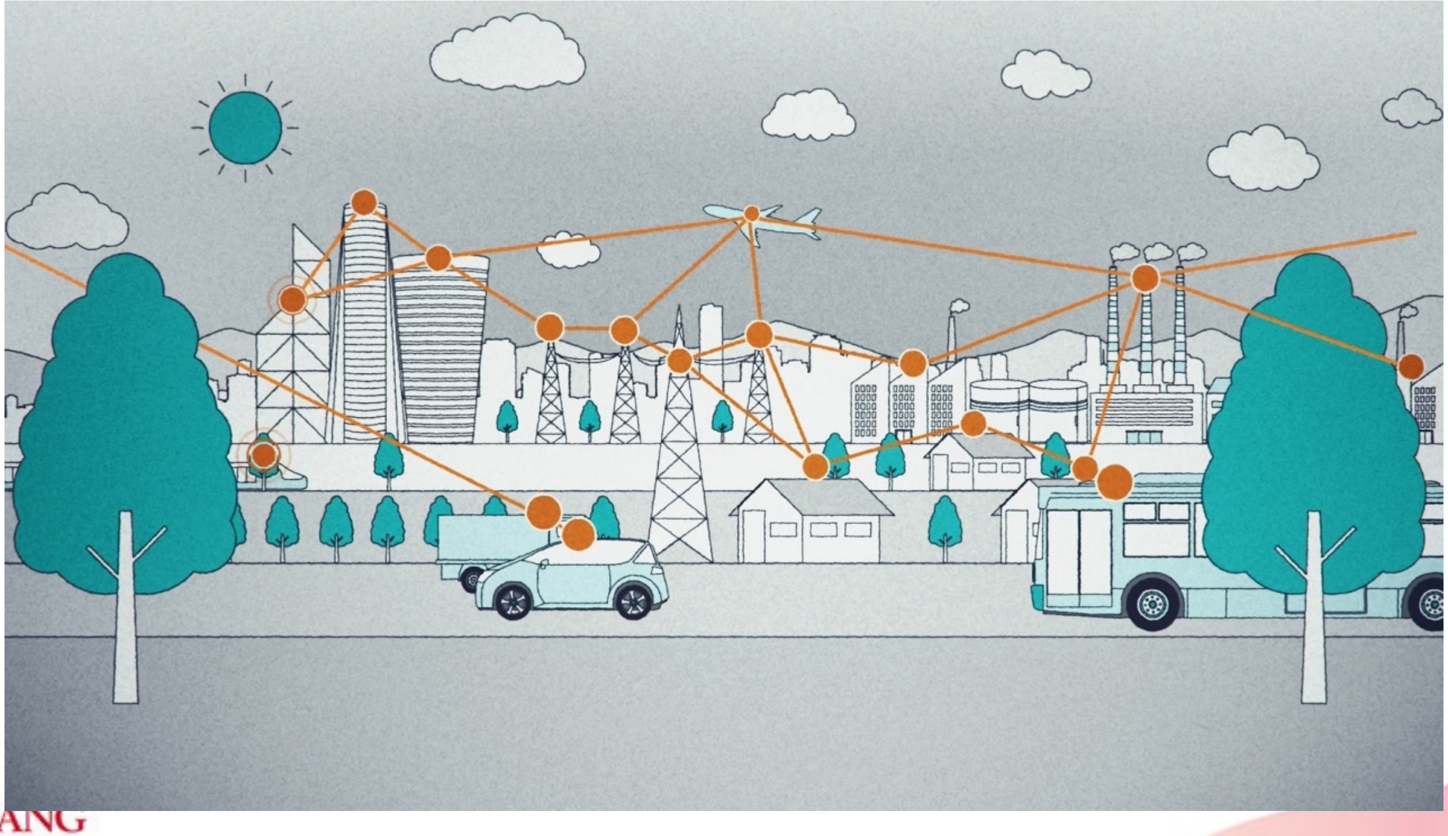
Event code

CPSSECURITY

NANYANG TECHNOLOGICAL UNIVERSITY

Key Management for Sensor Networks

- Key distribution in large networks
  - Total number key exchanges for n-users is $n(n-1)/2$



Key Pre-distribution

- Loading Keys into sensor nodes *prior to deployment*
- Two nodes find a common key between them after deployment
- Challenges
  - Memory/Energy efficiency
  - Security: nodes can be compromised
  - Scalability: new nodes might be added later

Key Distribution Schemes

- Three keying models are used to compare the different relationships between WSN Security and operational requirements

- **Network Keying**
- **Pairwise Keying**
- **Group Keying**

Network Keying

- One Key for the Network

All the nodes in the network have the same key

Benefits	Problems
Simple	Lacks Robustness If one of the node is compromise, all the nodes will be compromise
Allows data aggregation and fusion	
Scalable	
Able to self-organize	
Flexible	

Group Keying

A single node can belong in multiple groups and hold multiple keys for the groups

- One Key for a Group within the Network

Form different groups in a network to prevent network keying vulnerability

Benefits	Problems
Allows Multicast.	Lacks efficient storage for group keying.
Allows group collaboration.	Difficult to set up securely.
Better robustness than network keying.	Cluster formation information is application dependent.
Adjustable scalability.	
Flexible.	
Able to self-organize within cluster.	

Not easily scalable cos if add = form new cluster = reassociate the keys but if one group is compromise, only that group in the network is compromise instead of the whole network

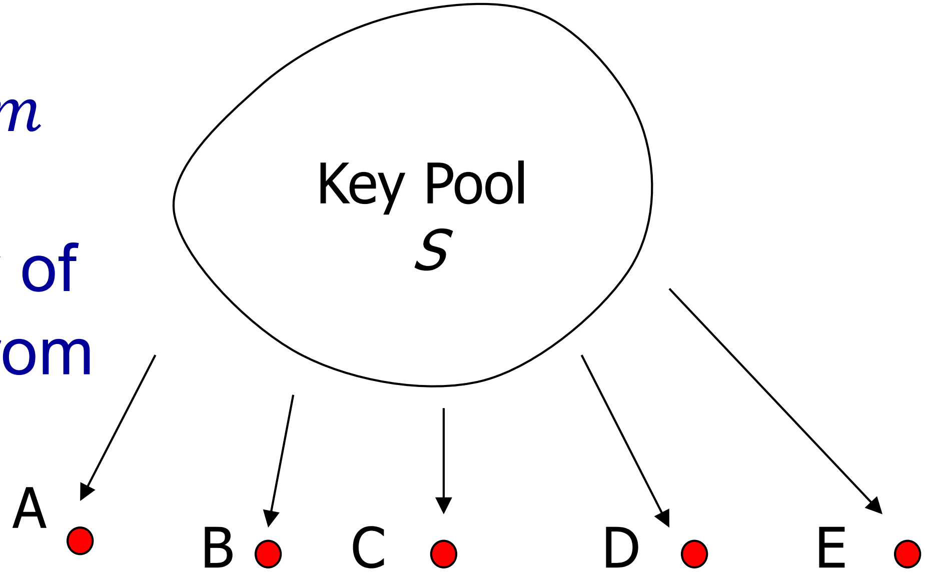
Pairwise Keying

- One Key for each Pair within the Network

Benefits	Problems
Provides best robustness. If one node is compromise, the rest of the nodes won't be compromise	Non-scalable.
	Unable to self-organize.
Authentication for each node.	Not flexible.

Eschenauer-Gligor Scheme

- Each node randomly selects m keys
- Can determine the probability of two nodes being connected from random graph theory
- Constraints
  - Size of key pool
  - Capacity of nodes
  - Desired Graph connectivity



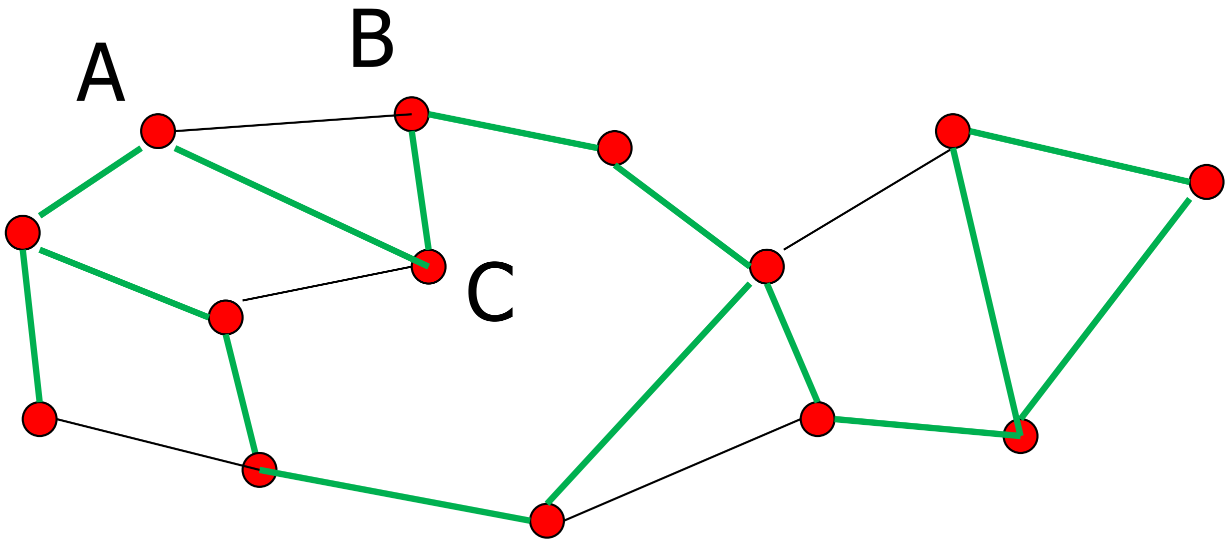
- When $|S| = 10{,}000, m = 75$

  Pr (two nodes have a common key) = 0.50

L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks", ACM CCS 2002

Establishing Secure Channels

- Establish a path by identifying nodes with common keys



IoT Key via Digital Fingerprinting

- Every device has a unique fingerprint, which can be used as the built-in key.
- Resolves the key distribution problem.

- Main Concept: **Physically Unclonable Function (PUF)**

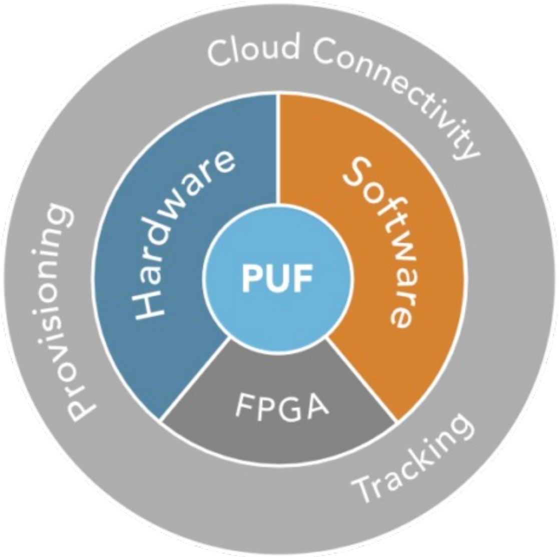
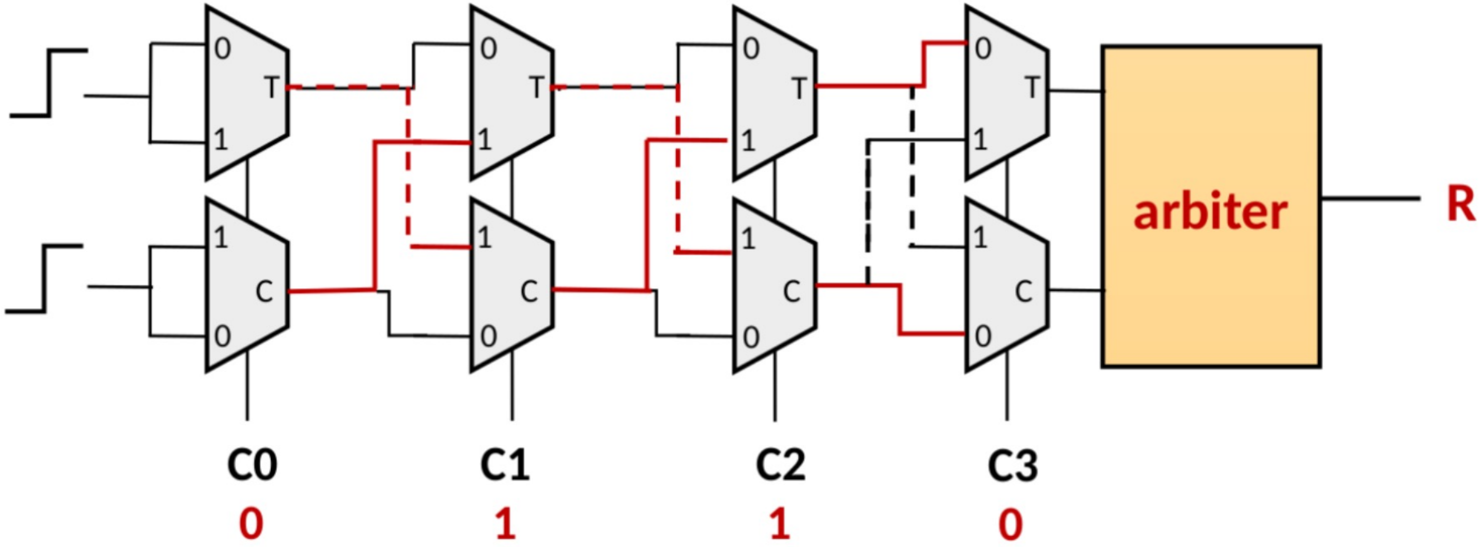


image source: Intrinsic ID

Arbiter PUF Design



- C_i acts as challenge and R is obtained as response.
- The digital fingerprint (PUF) consists of a database - Challenge-Response Pairs (**CRP**)

PUF Properties

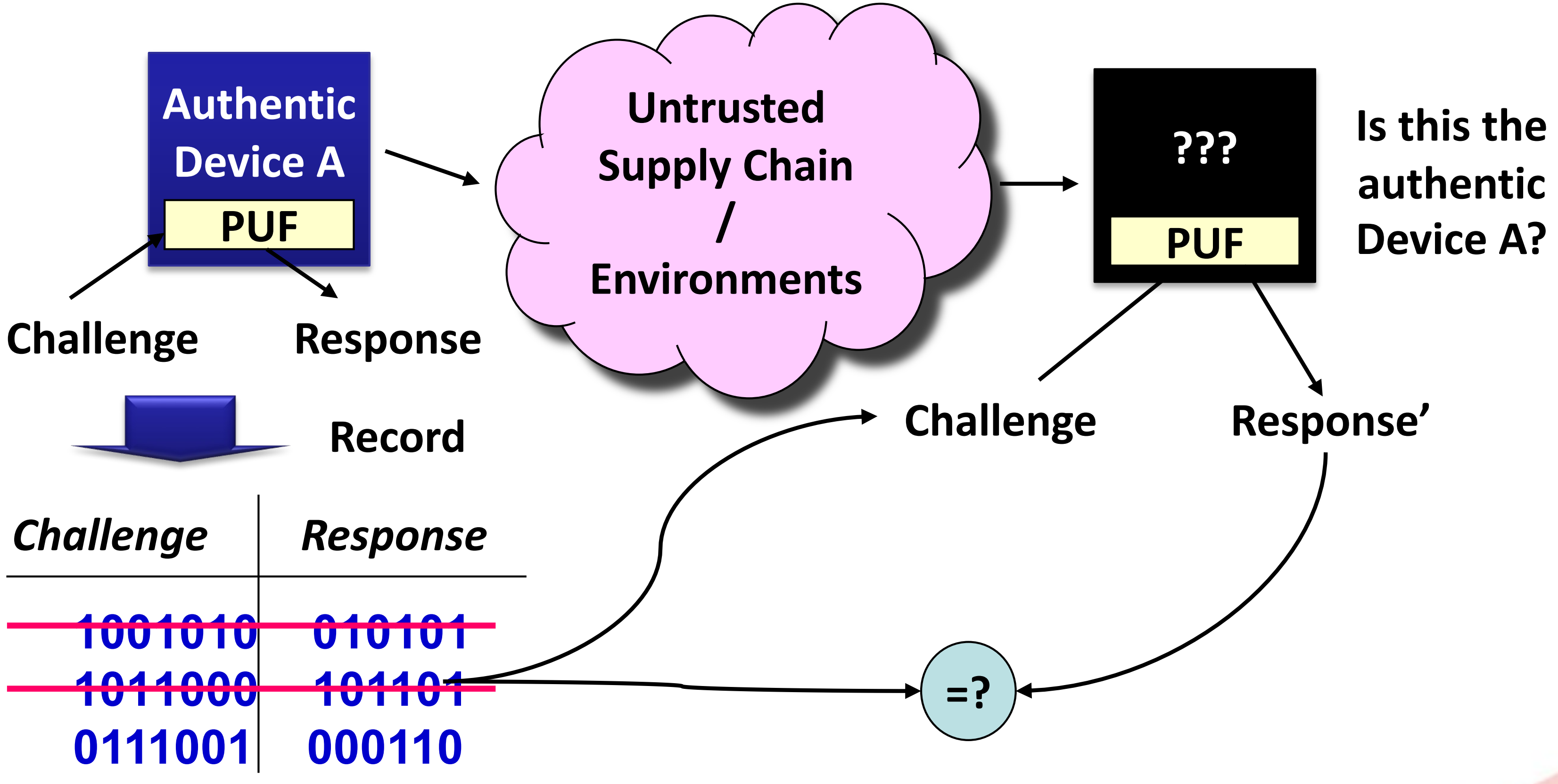
- **Evaluatable:** given PUF and x, it is easy to evaluate y = PUF(x).
- **Unique:** PUF(x) contains some information about the identity of the physical entity embedding PUF.
- **Unclonable:** given PUF, it is hard to construct a procedure *PUF'*

$$PUF' \neq PUF \quad and \ \forall x \in C \ \ PUF'(x) \approx PUF(x)$$

- **Unpredictable:** given only a subset of CRP, it is hard to predict y_c = PUF(x_c)
- **One-way:** given only y and the corresponding PUF instance, it is hard to find x such that PUF(x) = y
- **Tamper-evident:** altering the physical entity embedding PUF transforms *PUF →PUF'*

PUF Usage: Authentication

Protect against counterfeits



Authentic Device A

PUF

Challenge

Response

Record

Untrusted Supply Chain / Environments

???

PUF

Is this the authentic Device A?

Challenge

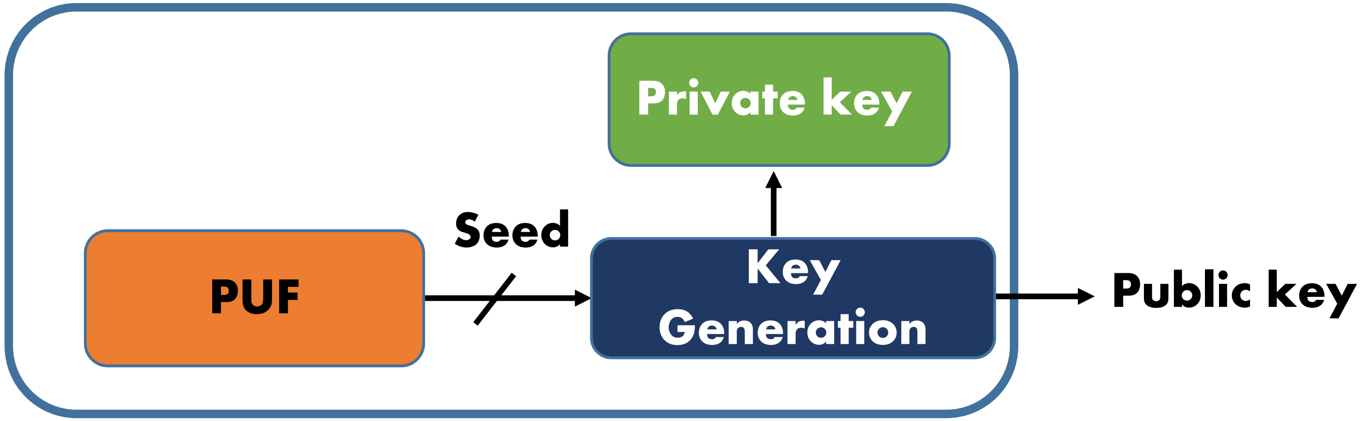
Response'

=?

Challenge	*Response*
~~1001010~~	~~010101~~
~~1011000~~	~~101101~~
0111001	000110

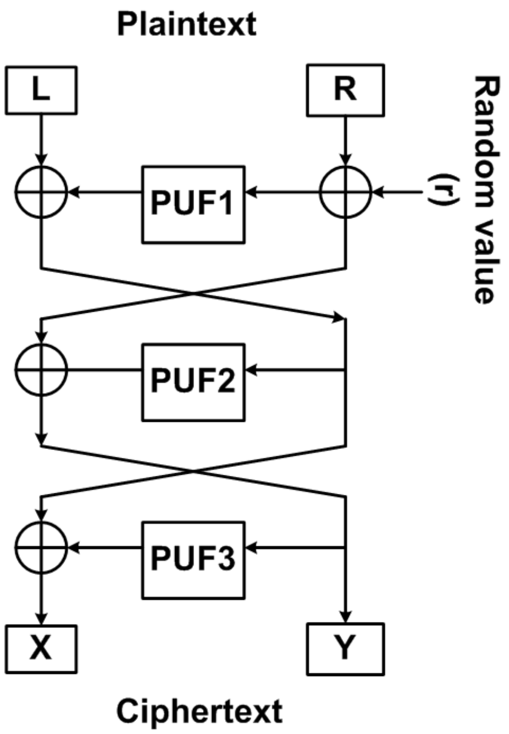
Database for Device A

PUF Usage: Key Pair Generation



- PUF response is used as a random seed to a private/ public key generation algorithm
- No secret needs to be handled by a manufacturer
- A device generates a key pair on-chip, and outputs a public key

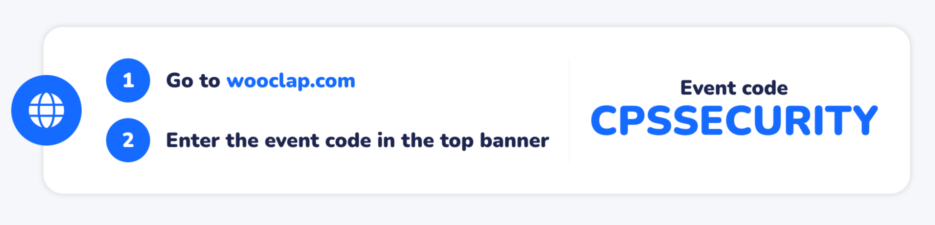
PUF Usage: Keyless Cipher



- A randomized 3-round Luby-Rackoff cipher
- Round functions are replaced by PUF instances
- This is a keyless cipher

Contents

- Key Management Systems
- Key Management for Wireless Sensor Networks
- ➔ *Discussion*



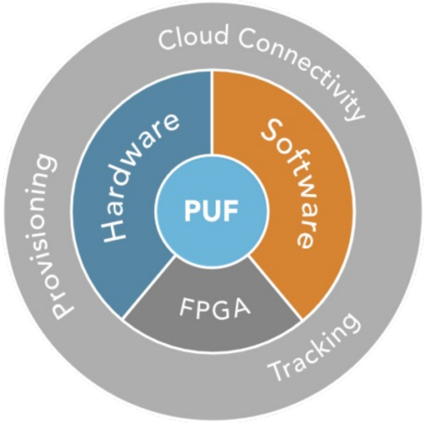
1. Go to wooclap.com
2. Enter the event code in the top banner

Event code
CPSSECURITY

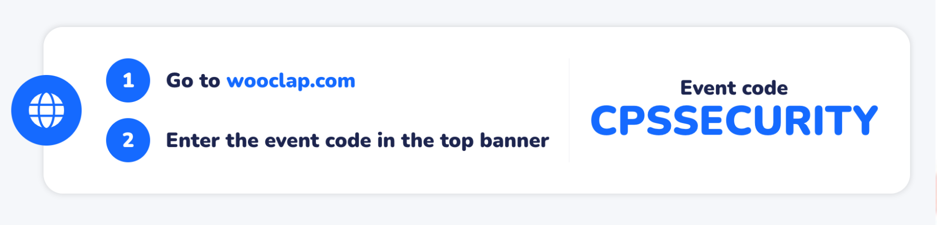
What did we learn?

- **Key Management Systems**
  - Hardware Security Modules
  - Processes of Key Management

- **Key Management for Sensor Networks**
  - Pairwise, Group, Network Keying
  - Eschenauer-Gligor Scheme
  - PUF-based IoT Security



The End



1 Go to wooclap.com

2 Enter the event code in the top banner

Event code
CPSSECURITY

NANYANG
TECHNOLOGICAL
UNIVERSITY