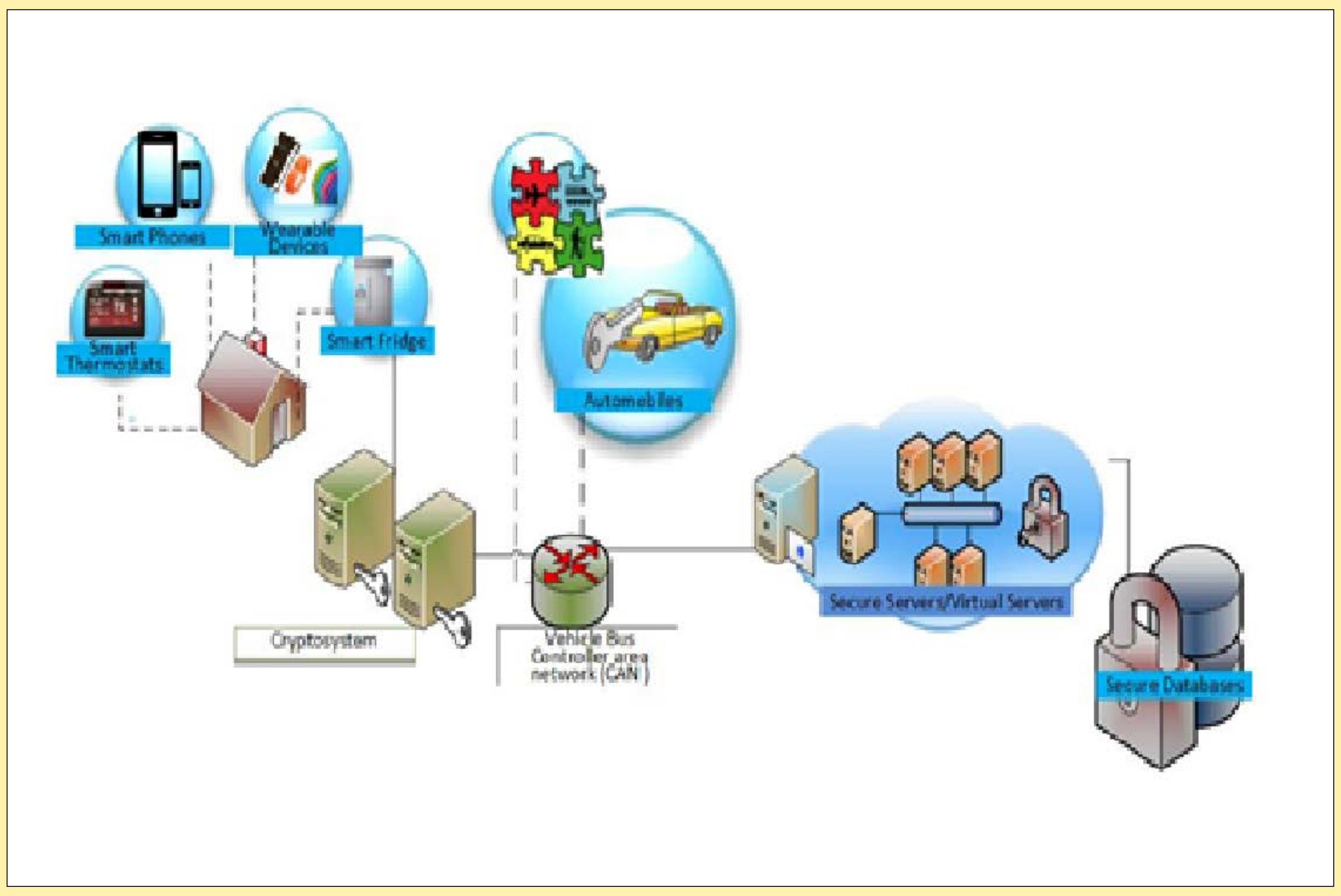
Hardware based Authentication and Trusted Platform Module functions (HAT) for IoTs

PIs: Fareena Saqib
Affiliations: Florida Institute of Technology
https://www.nsf.gov/awardsearch/showAward?AWD_ID=1566530&HistoricalAwards=false

Introduction

The resource-constrained devices create additional vulnerabilities and provide ever-widening opportunity for malicious adversaries to steal private information, subvert systems, and destroy property in a manner that in extreme cases results in the loss of human life.

These problems are becoming critical with the propagation of mobile computing and the emergence of new information-sharing and control systems such as the health information exchange, smart grid, home automation, smart cars, sensor networks, and many more applications in commercial, industrial and military systems. It is, therefore, imperative that a stronger level of security be put in place to counter these security challenges faced by the resource-constrained mobile and wirelessly-connected devices or IoTs.



The over-arching model of this project is to investigate the benefits to the overall system when the constituent components are designed from the perspective that security and trust needs to be provided as a fundamental feature of the hardware and investigating hardware based security solutions.

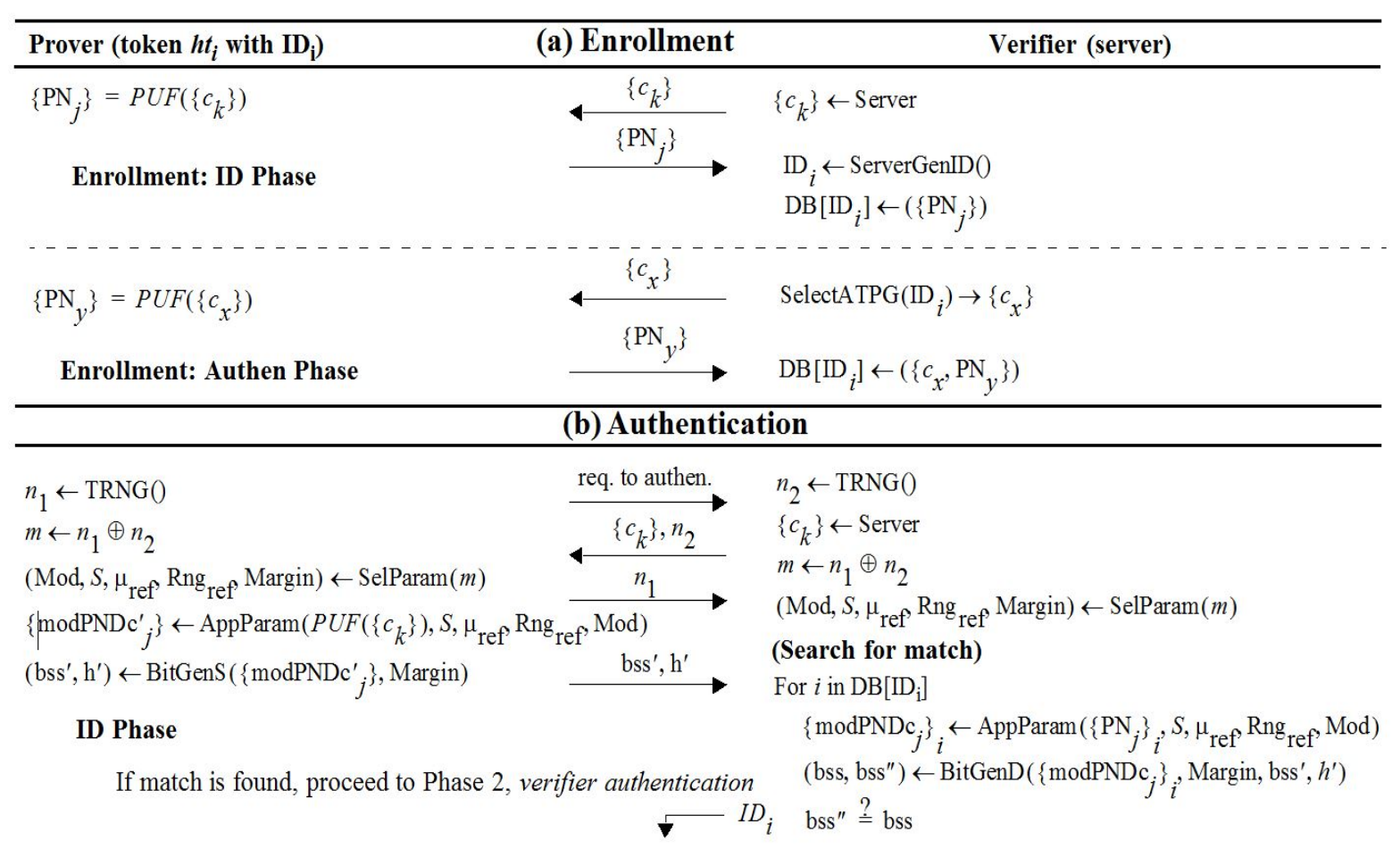
Approach

Traditional cryptographic primitives are computation intensive and rely on secrecy of shared or session keys, applicable on large systems like servers and secure databases. This is unsuitable for embedded devices with fewer resources to allocate dedicated hardware for implementing security protocols with extra storage requirements, as flash memory, for key management, thus, making these devices the weakest link of CPS.

Project advances the state of the art of ubiquitous/embedded device authentication protocol using hardware primitives in the following:

- Design and evaluation of novel hardware based authentication protocols for embedded devices with varied resources. New authentication techniques using strong PUF challenge and response pairs incorporating with the cryptographic primitives,
- Investigation of PUF capabilities to extend the security features of TPM by providing pre-boot authentication and secure storage encryption.

A Privacy-Preserving, Mutual PUF-Based Authentication Protocol



Prover (token ht_i with ID_i) | (a) Enrollment | Verifier (server)

$\{\text{PN}_j\} = PUF(\{c_k\})$ | $\{c_k\}$ ← | $\{c_k\} \leftarrow \text{Server}$
Enrollment: ID Phase | $\{\text{PN}_j\}$ → | $\text{ID}_i \leftarrow \text{ServerGenID}()$
$\text{DB}[\text{ID}_i] \leftarrow (\{\text{PN}_j\})$

$\{\text{PN}_y\} = PUF(\{c_x\})$ | $\{c_x\}$ ← | $\text{SelectATPG}(\text{ID}_i) \rightarrow \{c_x\}$
Enrollment: Authen Phase | $\{\text{PN}_y\}$ → | $\text{DB}[\text{ID}_i] \leftarrow (\{c_x, \text{PN}_y\})$

(b) Authentication

$n_1 \leftarrow \text{TRNG}()$ | req. to authen. → | $n_2 \leftarrow \text{TRNG}()$
$m \leftarrow n_1 \oplus n_2$ | $\{c_k\}, n_2$ ← | $\{c_k\} \leftarrow \text{Server}$
$(\text{Mod}, S, \mu_{\text{ref}}, \text{Rng}_{\text{ref}}, \text{Margin}) \leftarrow \text{SelParam}(m)$ | n_1 → | $m \leftarrow n_1 \oplus n_2$
$\{\text{modPNDc}'_j\} \leftarrow \text{AppParam}(PUF(\{c_k\}), S, \mu_{\text{ref}}, \text{Rng}_{\text{ref}}, \text{Mod})$ | | $(\text{Mod}, S, \mu_{\text{ref}}, \text{Rng}_{\text{ref}}, \text{Margin}) \leftarrow \text{SelParam}(m)$
$(\text{bss}', h') \leftarrow \text{BitGenS}(\{\text{modPNDc}'_j\}, \text{Margin})$ | bss', h' → | (Search for match)
ID Phase | | For i in $\text{DB}[\text{ID}_i]$
$\{\text{modPNDc}_j\}_i \leftarrow \text{AppParam}(\{\text{PN}_j\}_i, S, \mu_{\text{ref}}, \text{Rng}_{\text{ref}}, \text{Mod})$
$(\text{bss}, \text{bss}'') \leftarrow \text{BitGenD}(\{\text{modPNDc}_j\}_i, \text{Margin}, \text{bss}', h')$
If match is found, proceed to Phase 2, *verifier authentication* | ID_i | $\text{bss}'' \overset{?}{=} \text{bss}$

Activity/Component	LUTs	FFs	Time (us)
ID Phase			
Network delay	-	-	44,347
PN generation using sbox-mixedcol	3170	128	577,834
Token timing engine	721	828	
Token bitstring gen. engine	1104	385	2359
Token controller and I/O	705	297	-
Verifier authentication	-	-	80
Mutual Phase			
Network + verifier delays	-	-	50,830
Verifier bitstring gen.	-	-	54
Token timing engine + bitgen engine	-	-	577,037
Token authentication	338	86	571
TOTAL	6038	1724	1.25 sec.

Wenjie Che, Mitchell Martin, Goutham Pocklassery ,Venkata K. Kajuluri, Fareena Saqib , and Jim Plusquellic “**A Privacy-Preserving, Mutual PUF-Based Authentication Protocol** . Cryptography Journal 2016

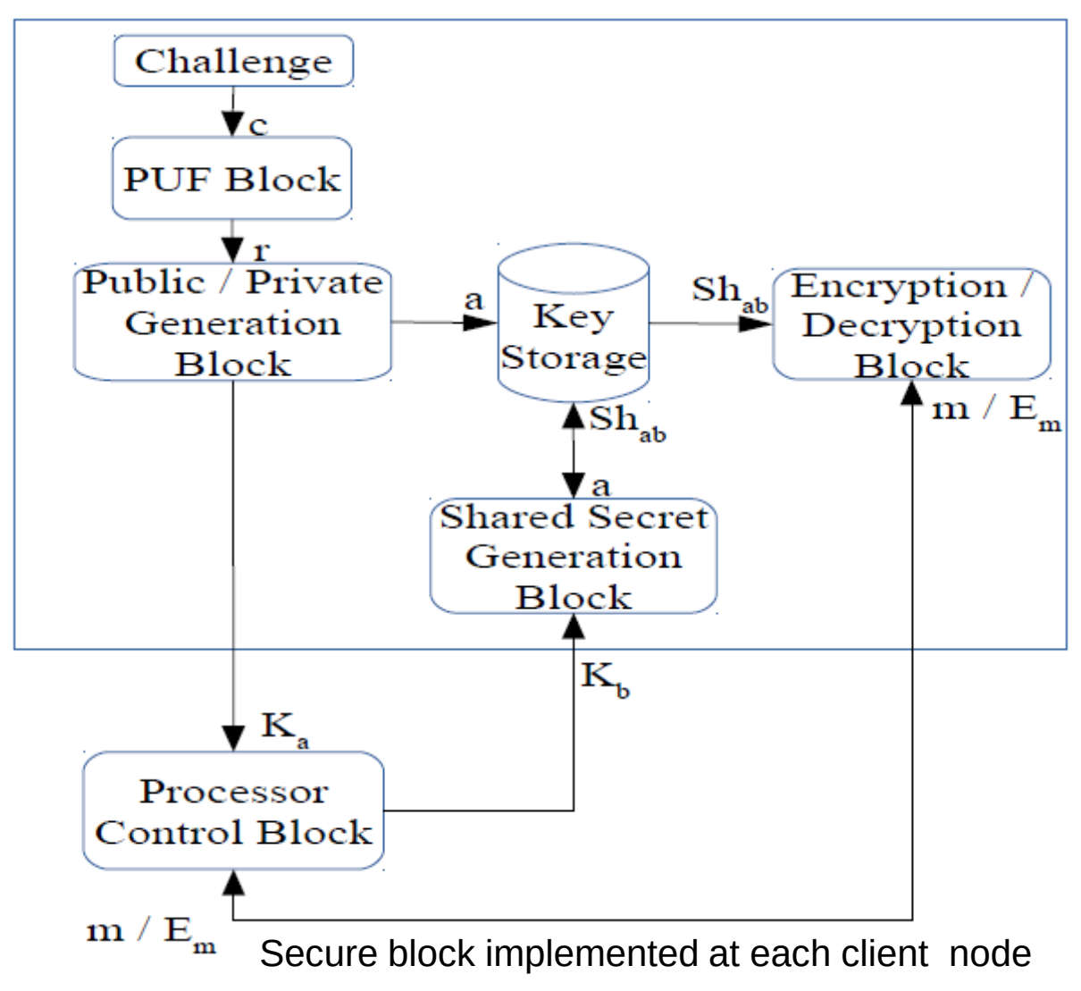
Hardware Based Security Enhanced Framework for Automotives

Algorithm: Enrollment process of client nodes in a trusted environment.
Input: Challenge c, configuration parameters for the ECC curve.
Output: Public key K_a of ECU.

```
1: At each client node, input a challenge $c$ for the PUF Block.
2: PUF block computes a response $r$.
3: Generate a public private key pair (a, $K_a$) using PUF response r and configuration parameters.
4: $K_a$ for each ECU is stored communicated to server, where it is stored in a public database accessible to every node on the bus.
5: Public key of the server, $K_s$ is stored in non-volatile memory at each client node for later access.
```

Algorithm: Initialization process.
Input: None.
Output: None.

```
1: Each ECU generates PUF response r using stored challenge c, and helper data.
2: With $r$ as the input to the Public / Private Key Generator Block, generate public and private keys, $K_a$ and $a$ respectively.
3: With public key of the server $K_s$ and private key $a$, generate shared symmetric encryption key $Sh_{ab}$ using the Shared Key Generation Block.
4: Encrypt the generated public key $K_a$ with the shared key $Sh_{ab}$.to form message $E_m$.
5: Transmit $E_m$ to the server.
6: At the server, once an encrypted message $E_m$ is received, Server decrypts it to get message $m$, which holds the public key of node A, $K_a$.
7: If $K_a$ received is equal to the $K_a$ stored in the database then consider node A authorized for the rest of the session.
8: Wait for other nodes to register themselves.
9: Server prepares a message for each ECU encrypting with the ECU public key containing the public keys of all the registered nodes.
10: Once this message is received at a node, decrypt it using the shared key.
11: Each node communicates with the other nodes and generates session keys using both its private key and other nodes public key.
```


Challenge
c
PUF Block
r
Public / Private Generation Block
a
Key Storage
Sh_ab
Encryption / Decryption Block
m / E_m
Sh_ab
a
Shared Secret Generation Block
K_b
K_a
Processor Control Block
m / E_m

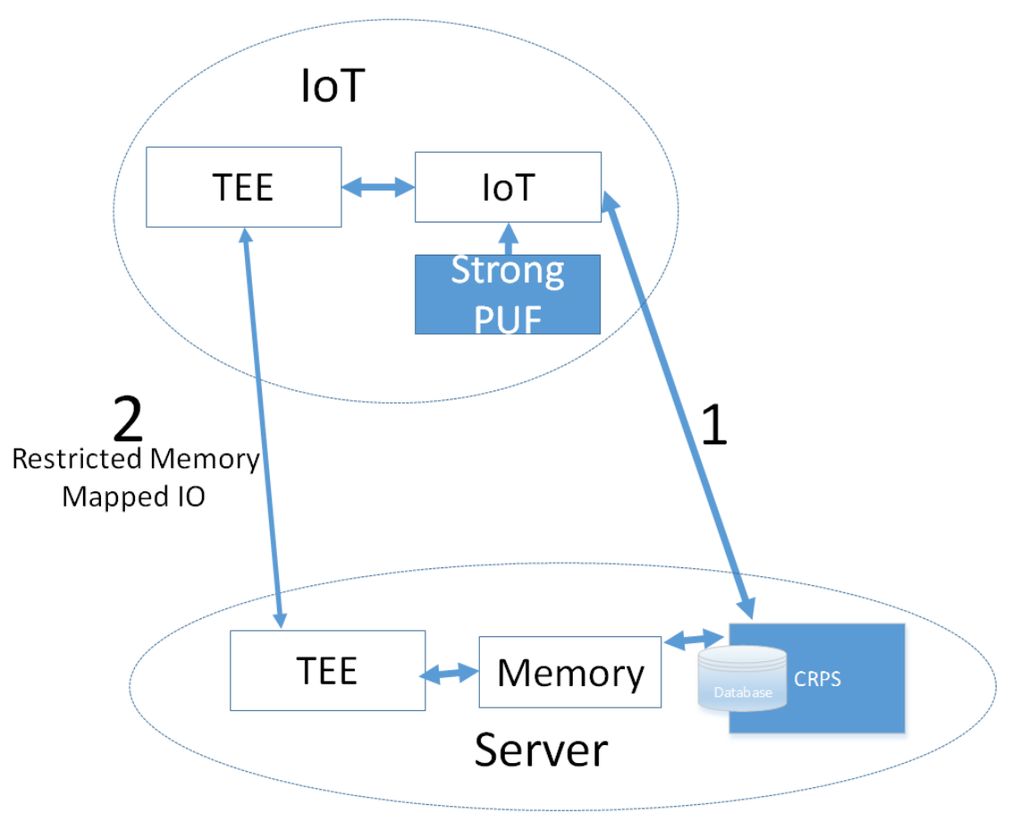
Secure block implemented at each client node

Ali Shuja Siddiqui, Yutian Gui, Jim Plusquellic, Fareena Saqib, “ **Hardware Based Security Enhanced Framework for Automotives**”. VNC 2016

Extending Security of IoTs using Physical Unclonable Functions PUF

Discusses the architecture to enable root of trust using Strong PUF and Trustzone to provide the following functions:

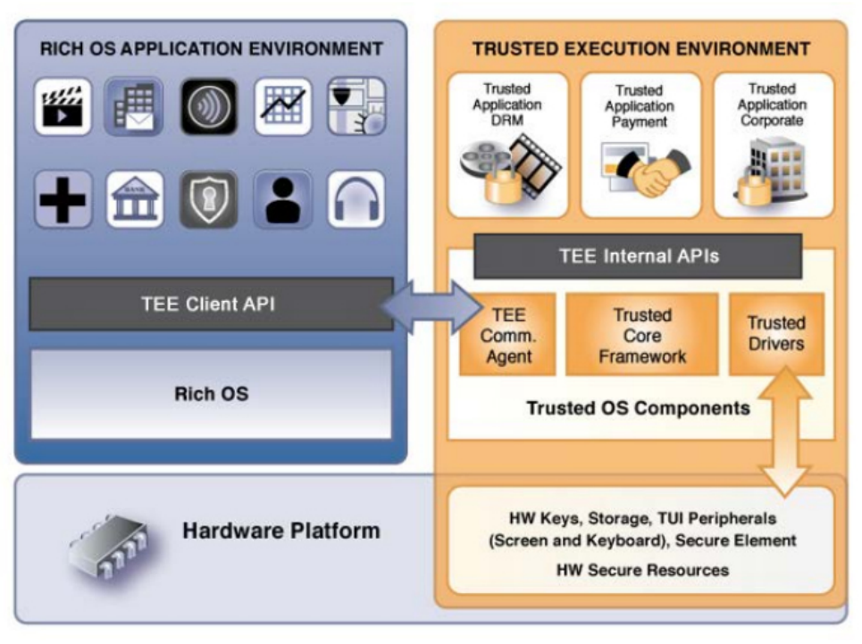
- Remote attestation.
  - Using hash of system state.
- Key Binding and hardware encryption
  - TPM provides information security but does not provide physical security.
  - Replace key generation and key storage with PUF, traditionally stored NVM
  - Provides CRPs authentication replaces password (benefit of PUFs)



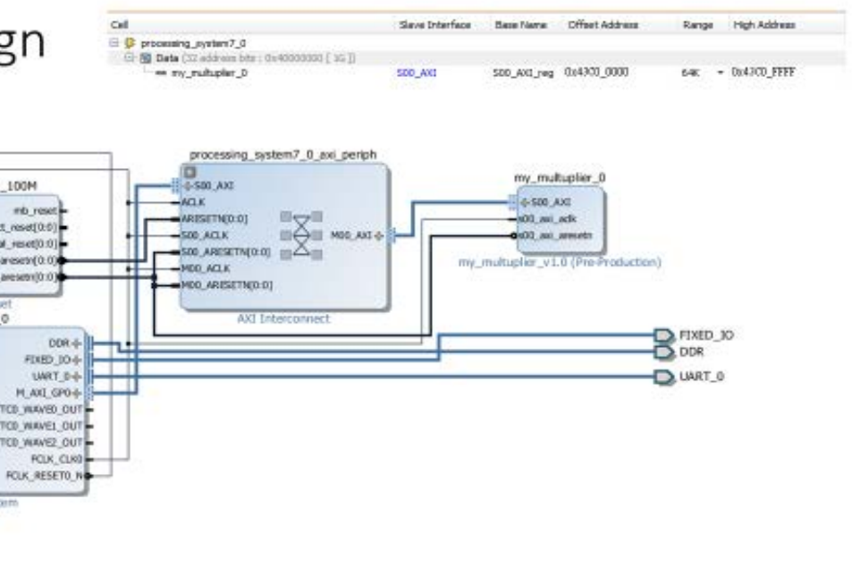
Ali Shuja Siddiqui, Jim Plusquellic, Fareena Saqib, “**Extending Security of IoTs using Physical Unclonable Functions PUF**”. FICS 2016

Hardware-Based Encryption using ARM TrustZone technology

Investigated ARM trustZone on ARM family for protection from illegal memory access


RICH OS APPLICATION ENVIRONMENT
TRUSTED EXECUTION ENVIRONMENT
Trusted Application DRM
Trusted Application Payment
Trusted Application Corporate
TEE Internal APIs
TEE Client API
TEE Comm. Agent
Trusted Core Framework
Trusted Drivers
Rich OS
Trusted OS Components
Hardware Platform
HW Keys, Storage, TUI Peripherals (Screen and Keyboard), Secure Element
HW Secure Resources

Block Design



Integration of HELP PUF with ARM trustZone to provide provide secure key for encryption using AES

Chia Che Lee, Fareena Saqib, “**Hardware-Based Encryption using ARM TrustZone technology** ”. Master Thesis 2016

Interested in meeting the PIs? Attach post-it note below!

National Science Foundation
WHERE DISCOVERIES BEGIN

The 3rd NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
January 9-11, 2017
Arlington, Virginia

Florida Institute of Technology
High Tech with a Human Touch™