SAND2022-11642C

Securing Firmware Over The Air (OTA) updates

S. Peter Choi

September 8 | 4:10 – 4:40 pm

U.S. DEPARTMENT OF ENERGY NNSA

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.
SAND2019-11784 PE

AUTO-ISAC
Automotive Information Sharing and Analysis Center

Sandia National Laboratories: SAND2022-10928 C ==> Need to be replaced with new SAND #

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Peter's Education & Employment History

Andrews University

B.S., Physics, 1988

PURDUE UNIVERSITY

Ph.D. & M.S. Computational Physics, 1997

VP of Corporate Information Security Officer **(CISO),** 2001

Systems Engineering – **Cybersecurity Lead**, 2011

Sandia National Laboratories

S. Peter Choi, Ph.D., 1997
CISSP, CSSLP

S-FOTA (PI-Peter Choi)

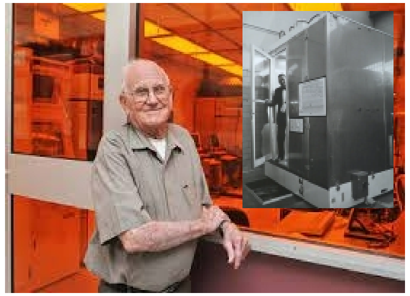
2021 R&D 100 WINNER
2021 WINNER

UNIVERSITY OF MARYLAND GLOBAL CAMPUS
Adj. Professor

National Security

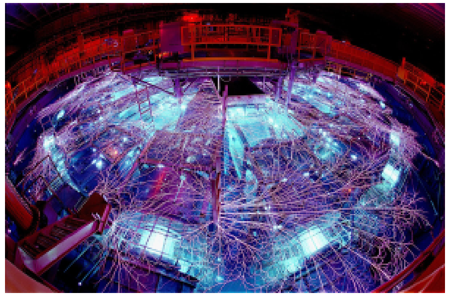
NNSA
National Nuclear Security Administration

Clean Room



Inventor - Willis Whitfield

Z Machine



Fusion Technology

Using the solar power to roast green chili

Alternative Energy

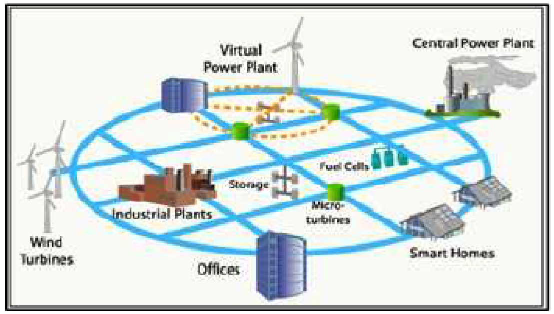
“Know yourself and know your Enemy”

- **Information Age**
  - Personally Identifiable Information (PII)
  - Intellectual Properties, national secrets
  - Credit cards and bank accounts


- **Age of “Cyber-Physical Systems”**
  - Information Age Assets plus
    - Physical devices
    - Operational and industrial assets
    - Safety and security of human beings





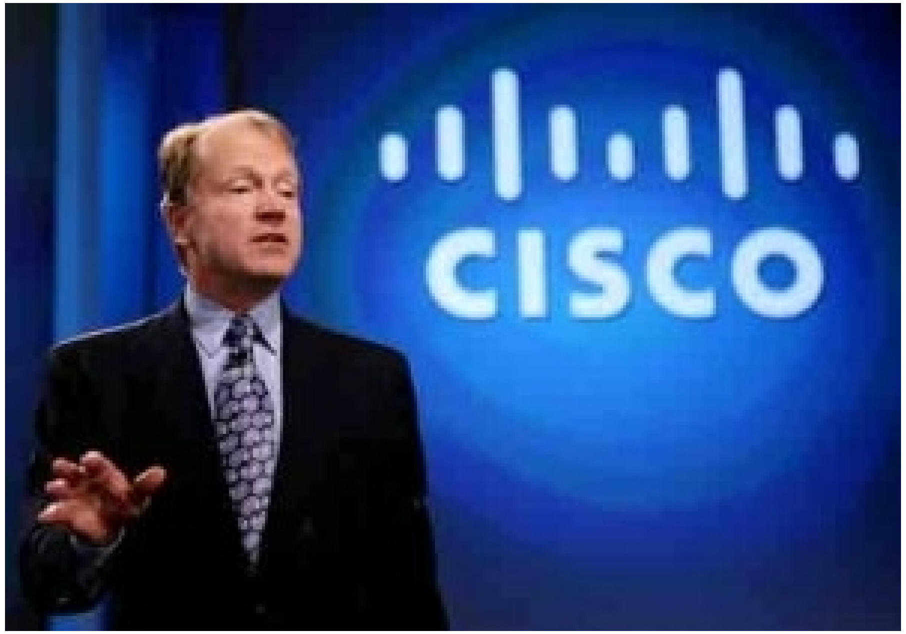


Sandia National Laboratories: SAND2022-10928 C ==> Need to be replaced with new SAND #

"Know yourself and know your Enemy"

- **Information "insecurity"**
  - OPM
  - IRS
  - LMC
  - Boeing
  - Ashley Madison
  - Amazon
  - Yahoo
  - Target
  - JP Morgan
  - HBO
  - Hilton Hotel
  - etc.

- **Colonial Pipeline**
- **SolarWinds**
- Cisco
- Equifax
- Facebook
- Apple
- Citibank
- Home Depot
- eBay
- Linkedin
- Cisco
- Sony
- Chipotle
- McDonald
- Johns Hopkins University
- Anthem Inc.
- Premera Blue Cross
- Others……



"There are two types of companies: those that have been hacked, and those who don't know they have been hacked."

-John Chambers, Former CEO CISCO

Sandia National Laboratories: SAND2022-10928 C ==> Need to be replaced with new SAND #

AUTO-ISAC
Automotive Information Sharing and Analysis Center

"Know yourself and know your Enemy"

- **For ever 1000 lines of professionally written code (LOC), expect 15 to 50 errors***
- **Windows 10 Operating System ~50 million LOC**
  - **1.625 million errors (taking ave of 32.5 errors)**
  - **Attackers have buffet of attack possibilities**
- **An experiment was conducted where software coders were told that errors were injected into the codes for them to find…they were unable to find them**
- **Increasing use of digital technology in "Cyber-Physical Systems"**
  - **Modern cars (built after 2015) ~150 million Lines of Code**
  - **For autonomous vehicle types ~300 million LOC**

* Steve McConnell's book, Code Complete

Joshua Brown –Ex Navy officer who used to dismantle bombs during Iraq war.

AUTO-ISAC
Automotive Information Sharing and Analysis Center

Sandia National Laboratories: SAND2022-10928 C ==> Need to be replaced with new SAND #

OTA – An Essential Capabilities of the Future Cars

Which is your model of modern cars, (A) or (B)?

The Risk of Insecure OTA

- **Malware installation ➔ Risk of Death and Destruction**
- **Software theft ➔ Loss of competitive edge**
- **Public Key Infrastructure (PKI) and Key Management Service (KMS) ➔ Attack surface for hackers**

- **~300 million lines of codes**

  Windows 10 OS has about ~50 million LOC

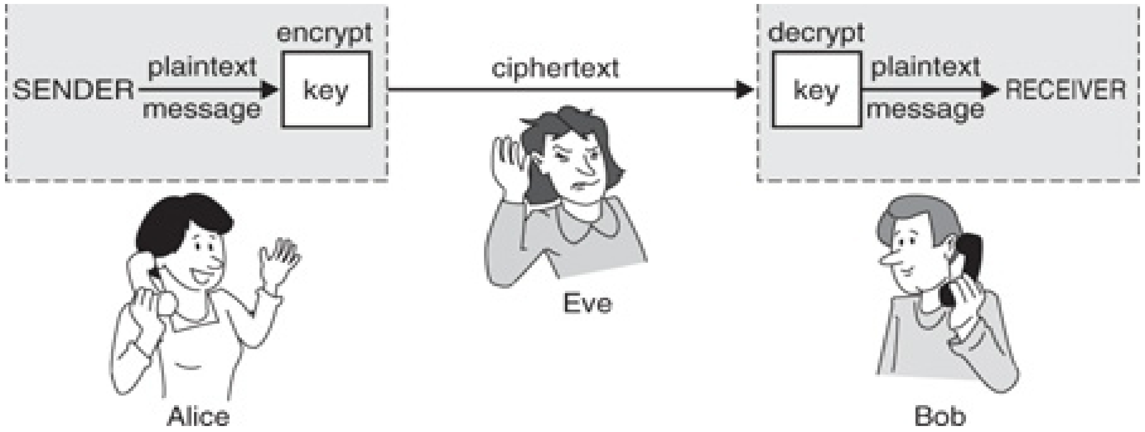
- **OTA support – life time of the vehicle?**

  "Are we in the business of selling cars or in the business of software maintenance?"

- **In 2021, Tesla had over 150 OTA updates**

  For Tesla, the prospect of getting one's vehicle fixed without "taking it to the shop" is instantly meaningful for the would-be buyer … as new Tesla owners laugh while their friends must continue heading to the dealer to iron out typical bug fixes for a new car. – Wired, February 2014

Zero Knowledge Cryptography



***Z (Zero trust)-engine is built on US Patent # 11,070,532 B1: Methods for Communicating data Utilizing Sessionless Dynamic Encryption**

Encryption	Information Security	Who can expose the secret?
Symmetric	The "secret" key is known to both Alice and Bob.	Both Alice & Bob can intentionally/ unintentionally expose their shared secret.
Asymmetric	The exposure risk of secret (i.e., private key) is reduced by 50%.	Only Alice can intentionally/ unintentionally expose her Private Key.
Z Hardware	No one, including Alice & Bob knows the inner workings of Z-engine	No one has the knowledge or digital access to the inner workings of Z-engine*.

Strategy: Design Principles for Cyber Physical Systems

Laws of Physics: the source of message must be anchored in the "first principles of physics" (i.e., message must be anchored to physical world)

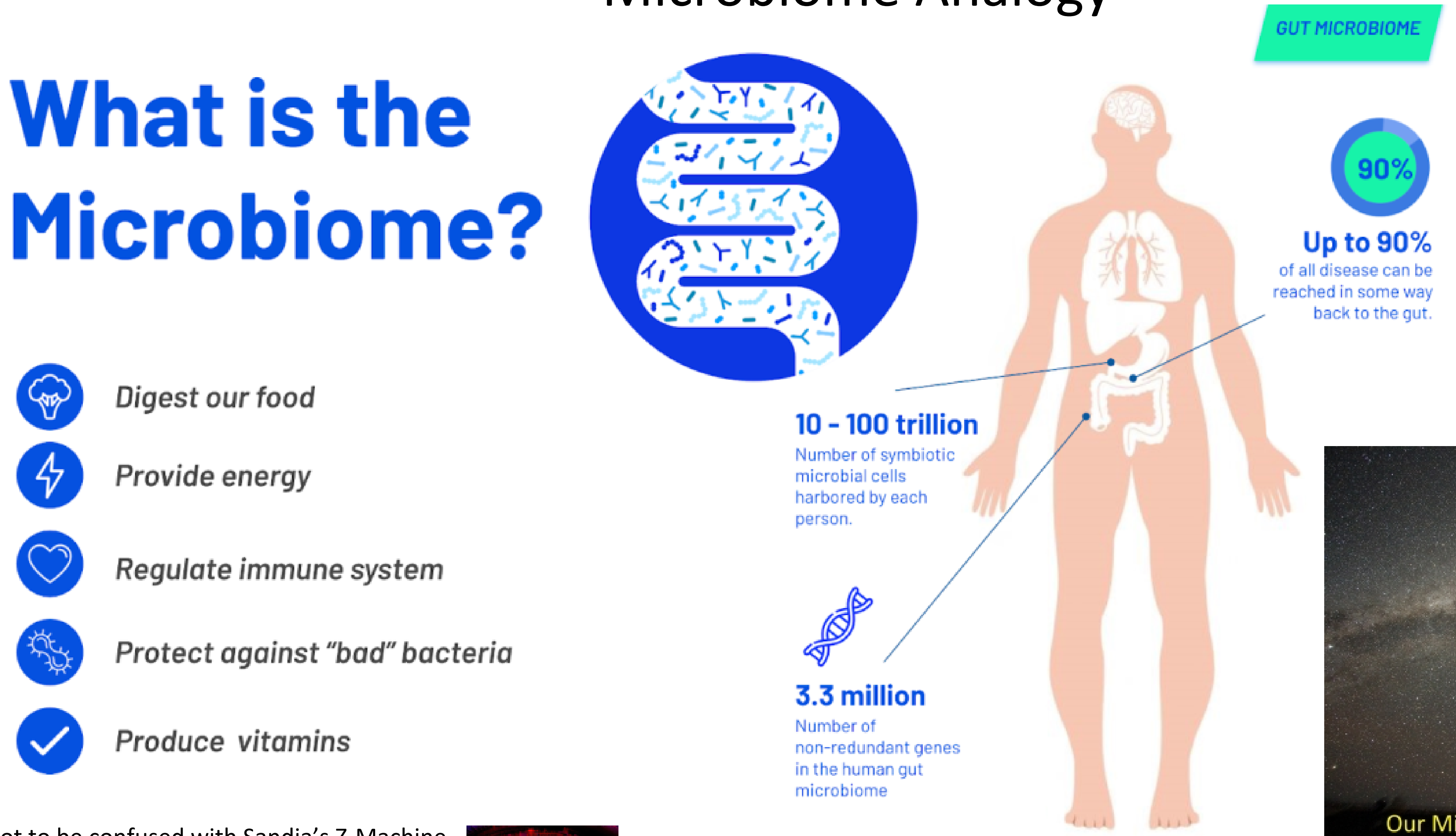
Always: Every messaging must satisfy ***Authenticity*** and ***Integrity*** verification

Never: Never accept unknown/unverified commands

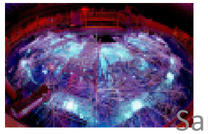
All digital commands are built on "whitelisted" rules with bounded, manageable complexity

How many commands are possible in the drone, for that matter in ECUs?

Z*- Cryptographic Engine Explained
- Microbiome Analogy



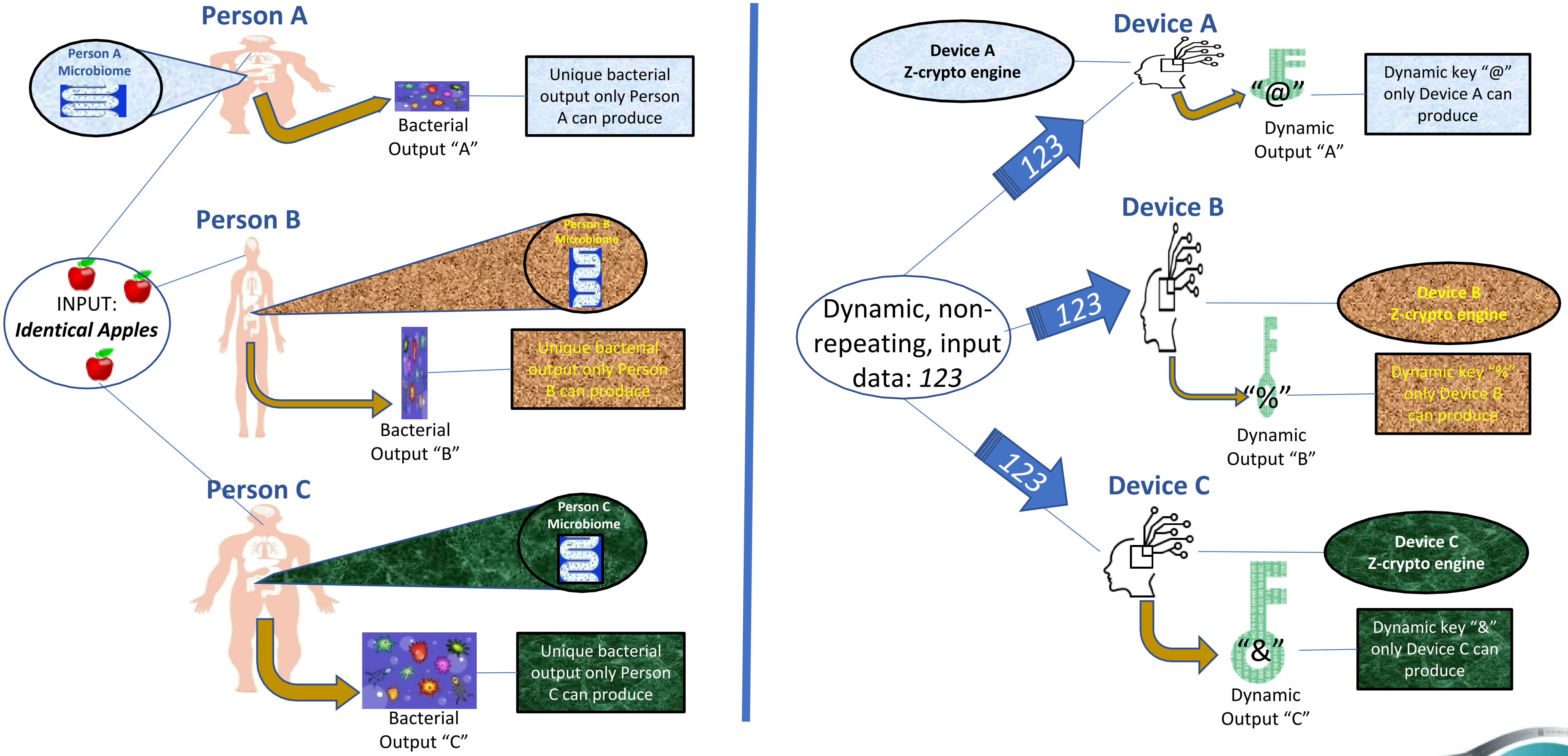
* Not to be confused with Sandia's Z-Machine



Sandia National Laboratories: SAND2022-10928 C ==> Need to be replaced with new SAND #

AUTO-ISAC
Automotive Information Sharing and Analysis Center

Z- Cryptographic Engine Explained



Sandia National Laboratories: SAND2022-10928 C ==> Need to be replaced with new SAND #

What’s so hard about OTA firmware update?

[Tesla car software update via satellite Starlink:](https://youtu.be/wt2b_1Wi_DU)

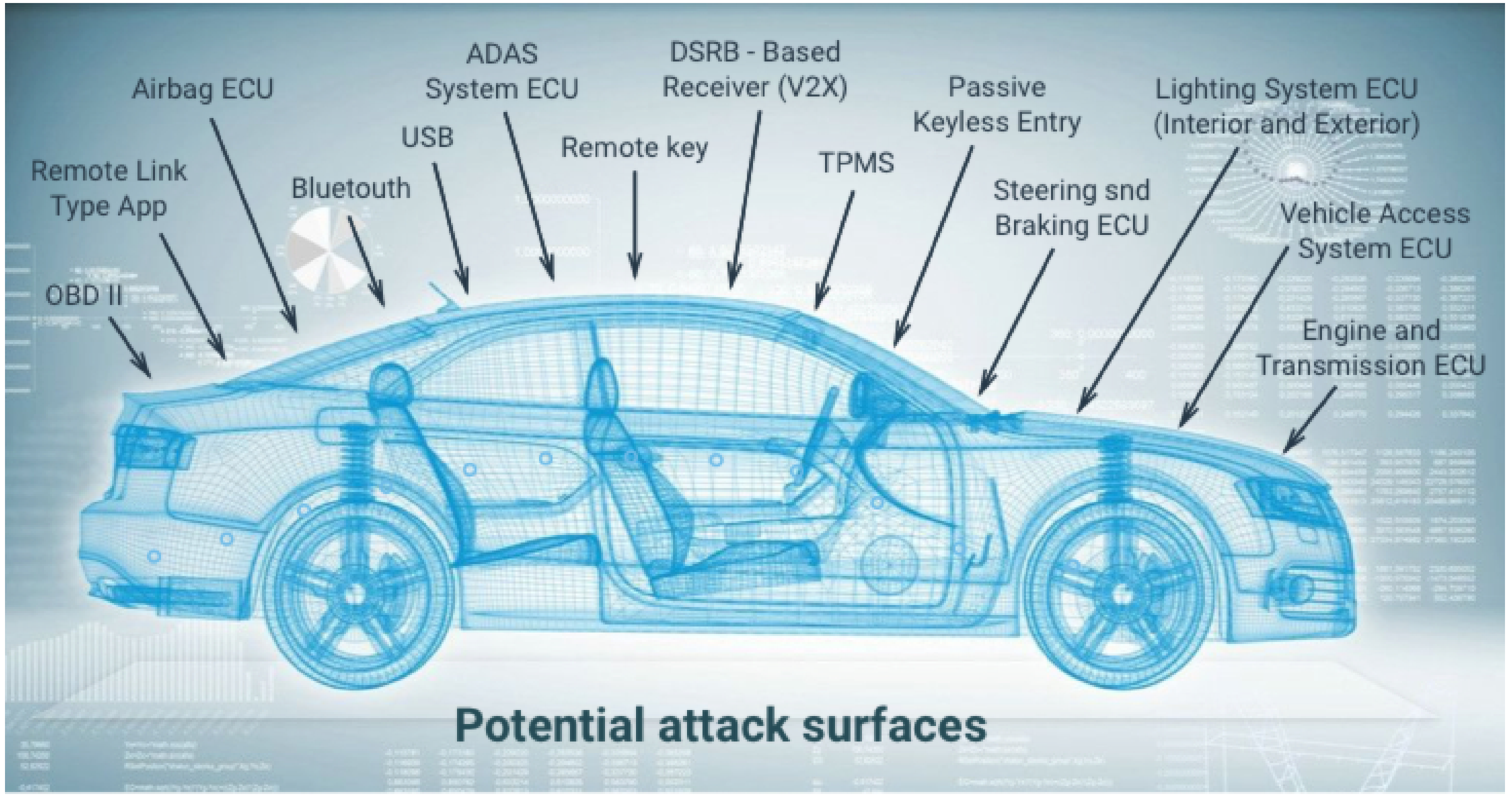
https://youtu.be/wt2b_1Wi_DU

It looks really simple doesn’t it?

Sandia National Laboratories: SAND2022-10928 C ==> Need to be replaced with new SAND #

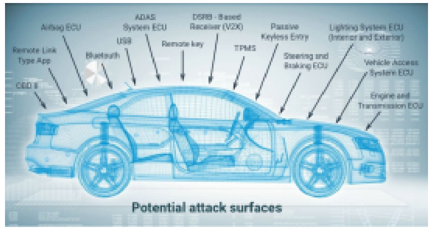
AUTO-ISAC
Automotive Information Sharing and Analysis Center

OTA Environment:



- For modern cars, we have 100 to 150 ECUs, not all ECUs are equal
- Codes in each ECU are proprietary solution
- Not all ECUs need firmware update
- PKI certs, asymmetric keys, symmetric keys, or no encryption at all requiring physical connection
- Vehicle needs automated central intelligence to distribute firmware to various ECUs

Secure OTA, Industry Best Practice - PKI



Cybersecurity Triad/Principles:

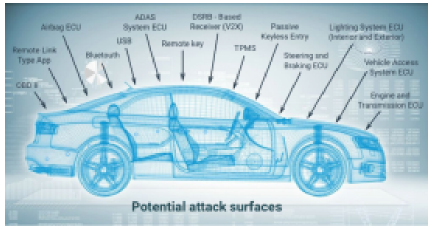
- Confidentiality – Protect proprietary codes running ECU (competition and hackers)
- Integrity – Assure that codes are intact (not corrupted, modified)
- Authenticity – Only the authorized OEM can update the codes

Centralized Public Key Infrastructure (PKI) – authentication & integrity check

- All ECU OEM must agree to comply with Vehicle OEM Certificate Authority
  - ECU OEM must purchase digital certificate for every ECUs
  - Some ECUs may not have enough CPU power to store and process PKI certificate
  - ECU must have online connection to verify the certificate
- PKI is complex and expensive to maintain, secure
  - Digital certificates must be generated and stored on each ECUs
  - Digital certificates have shorter lifespan then operational lifespan of the vehicles, requires renewal
  - PKI, under the threat of “quantum supremacy”

PKI is expensive, hard to maintain and secure. Requires all tier 1 suppliers to comply!

Secure OTA, Industry Best Practice -KMS



Cybersecurity Triad/Principles:

- Confidentiality – Protect proprietary codes running ECU (competition and hackers)
- Integrity – Assure that codes are intact (not corrupted, modified)
- Authenticity – Only the authorized OEM can update the codes

Centralized Key Management Service (KMS) – Confidentiality

- ECU OEMs' best interest to encrypt their intellectual property (i.e., software/firmware)
  - Competitive edge
  - Less opportunity for hackers to find vulnerabilities
  - Using KMS has "cost"
- KMS is complex and expensive to maintain, secure
  - Key generation, distribution, expiration, & access privileges must be planned and agreed upon by all ECU OEMs (to enable OTA, ECU OEMs must relinquish the encryption keys to vehicle OEM)
  - Digital certificates (PKI) are the default technology for linking access privileges to encryption/decryption keys
  - Compromising KMS has much lower threshold vs conducting full scale cryptographic analysis (e.g., Quantum Computer)

KMS is expensive, hard to maintain and secure. Requires all tier 1 suppliers to comply!

Sandia National Laboratories: SAND2022-10928 C ==> Need to be replaced with new SAND #

AUTO-ISAC
Automotive Information Sharing and Analysis Center

Secure OTA without PKI or KMS

Firmware as a Service (FaaS)*

Database of Vehicle ECU firmware: Year, Make, & Model

E_1	E_2	E_3	E_x	E_n
E_1, f_1	E_2, f_1	E_3, f_1	E_x, f_1	E_n, f_1
	E_2, f_2	E_3, f_2		E_n, f_2
	E_2, f_3			⋮
	E_2, f_4			E_n, f_7

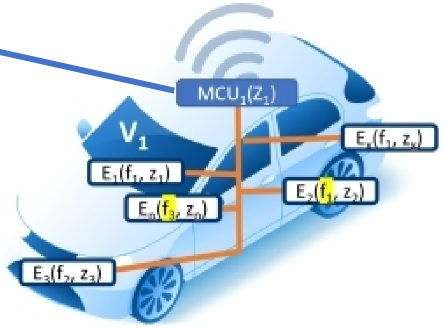
Latest firmware are highlighted green

V_1; Z_1
V_2; Z_2
⋮
V_n; Z_n

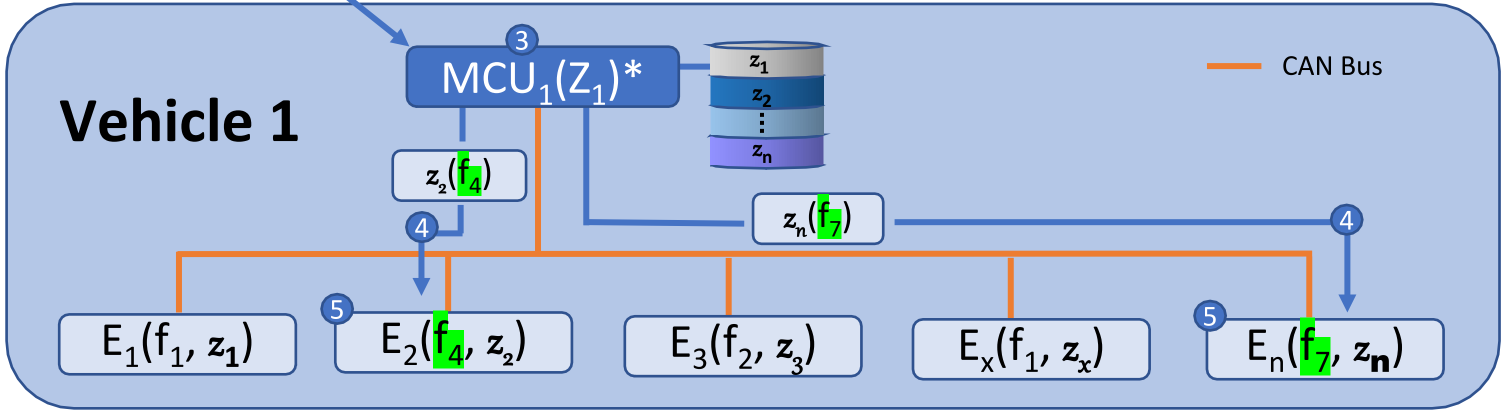
Database of Vehicle crypto-Z engines

1 Z_1 sends V_1's ECU firmware status.

2 Encrypted firmware update is sent back to V_1: $Z_1(E_2(f_4); E_n(f_7))$



1. Z_1 sends V_1's ECU firmware status.
2. FaaS compiles latest firmware and packages it to be sent to V_1. For V_1, these are: $E_2(f_4)$; $E_n(f_7)$
3. MCU_1 decrypts $E_2(f_4)$ & $E_n(f_7)$; re-encrypts $E_2(f_4)$ with $z_2(f_4)$ and $E_n(f_7)$ with $z_n(f_7)$.
4. The encrypted firmware is broadcasted over the CAN Bus.
5. Only V_1's E_2 can decipher $z_2(f_4)$ and E_n decipher $z_n(f_7)$.
6. V_1 now has the latest firmware updated.



V_i = (Vehicle)$_i$
Z_i = (Zero trust cryptographic engine)$_i$
f_i = (firmware version)$_i$
z_i = (ECU$_i$ zero trust crypto engine)$_i$

E_i = (Electronic Control Unit)$_i$

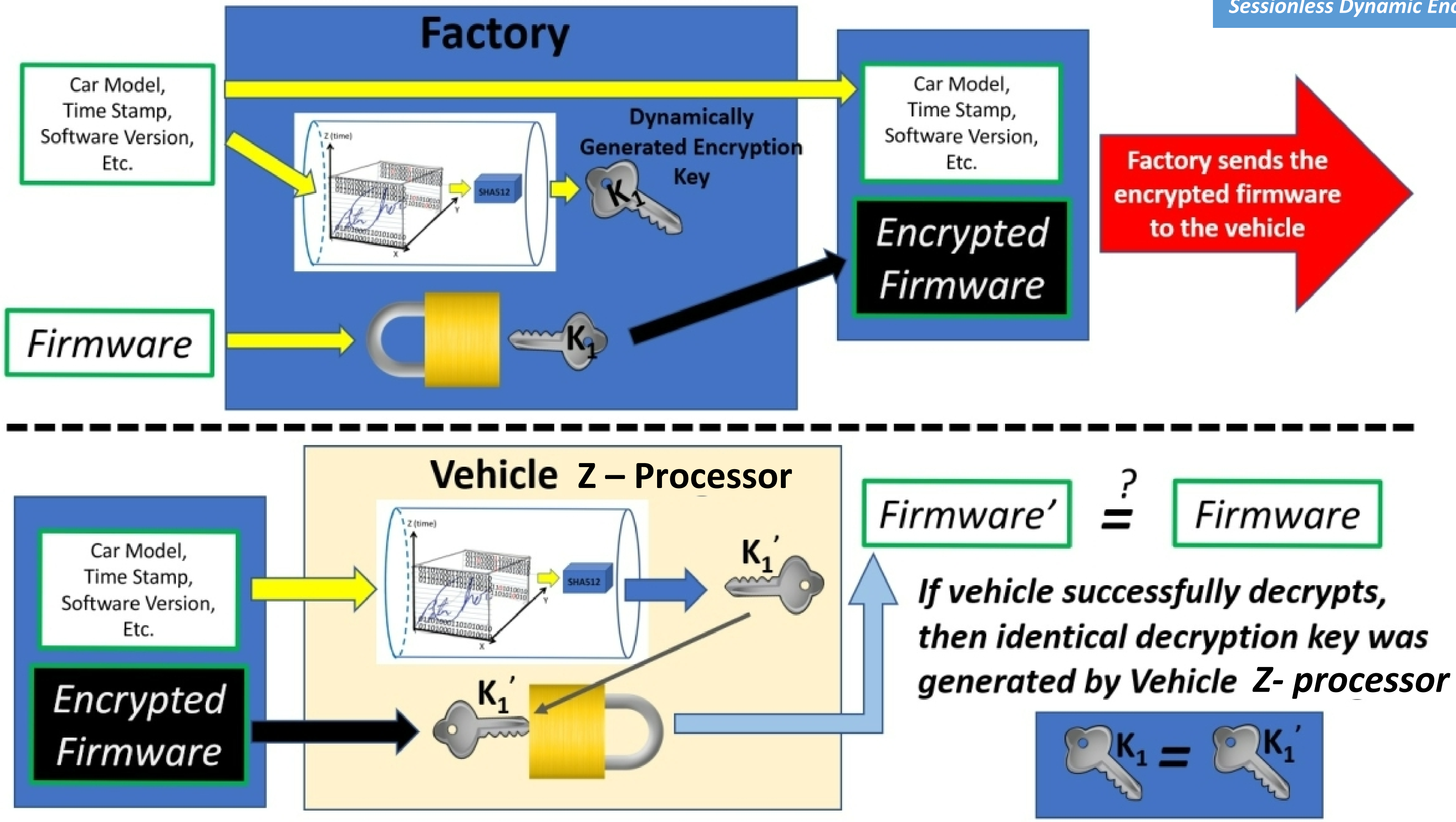
***FaaS** = Firmware as a Service
***MCU**$_i$ =(Master Control Unit)$_i$

*Patent Pending

3 Sandia National Laboratories: SAND2022-10928 C ==> Need to be replaced with new SAND #

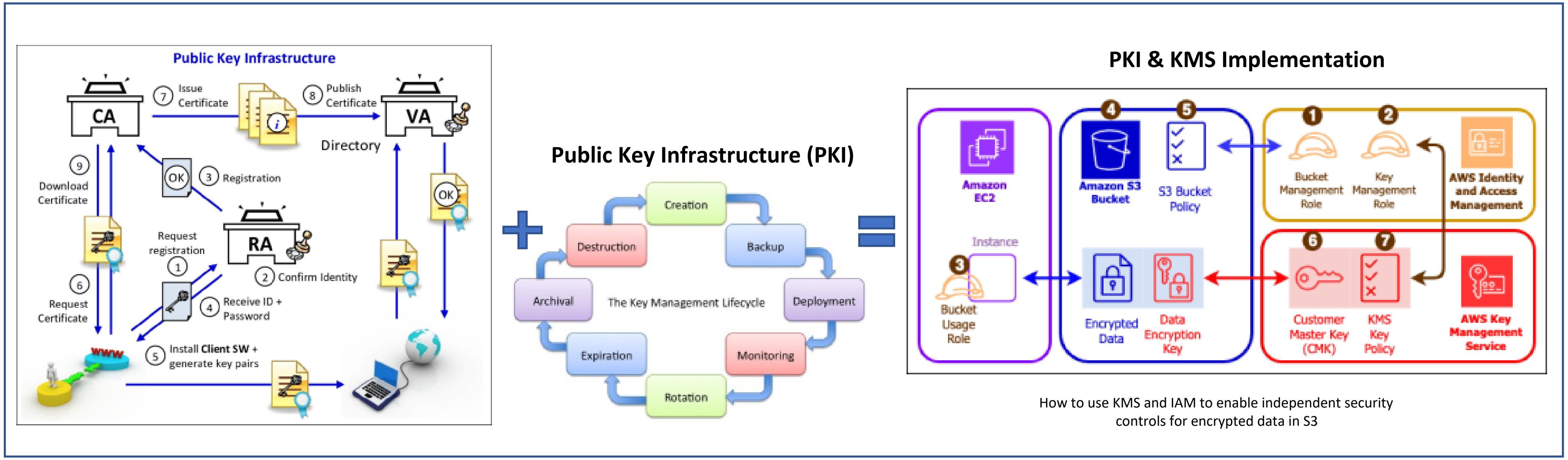
Secure OTA Firmware Update Data Flow Diagram*

* *US Patent # 11,070,532 B1: Methods for Communicating data Utilizing Sessionless Dynamic Encryption*



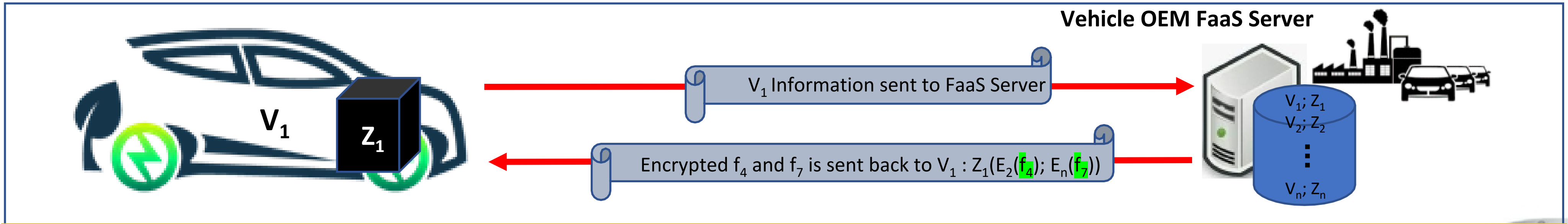
Z-processor dynamically generates the decryption keys that are automatically matched to the encrypted file…as well as providing *Integrity* and *Authenticity* checks on the received message.

Secure OTA Process Comparison



How to use KMS and IAM to enable independent security controls for encrypted data in S3

Every icon in this diagram is a potential attack surface digitally.



No icon in this diagram is digitally susceptible.

Every single Z-OTA messages are protected with unique set of cybersecurity triad: Confidentiality, Integrity, Authenticity/Availability (i.e., CIA)

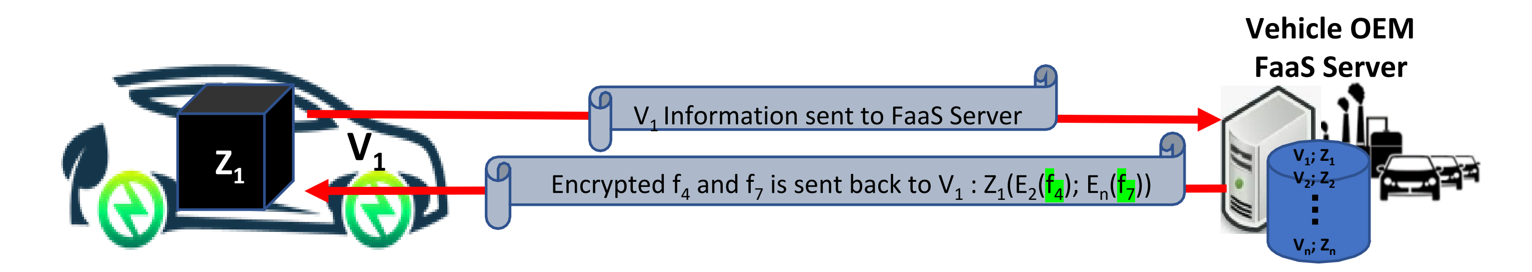
Sandia National Laboratories: SAND2022-10928 C ==> Need to be replaced with new SAND #

AUTO-ISAC
Automotive Information Sharing and Analysis Center

Technology Transfer from National Lab to Automotive Industry

1. Specialized ECUs (alternatively called Master Control Unit *) specially designed to receive, distribute, and store.
2. Cloud services for firmware update – Firmware as a Service (FaaS)
3. Z-OTA Prototyping and Demonstration

Product	Functional Benefits	DOE Sponsorship
MCU	Defense against side-channel attack (anti-tamper, true RNG, etc.)	SIBR/STTR, CRADA, TCF
FaaS	Efficient and Secure Cloud based solution (Firmware as a Service (FaaS))	SIBR/STTR, CRADA, TCF
ZAV-OTA Demo	Licensable Working model of ZAV-OTA firmware: HW Registration Agent; Secure OTA Firmware Update Agent	SIBR/STTR, CRADA, TCF



From the start to finish, every Z-OTA messages are protected with real-time, automated key and identity management as well as providing high fidelity integrity check!

*Patent Pending

Questions?

Sandia National Laboratories: SAND2022-10928 C ==> Need to be replaced with new SAND #