Securing Vehicle ECUs Update Over the Air

Kevin Daimi
University of Detroit Mercy, USA

Mustafa Saed, Scott Bone, Muhammad Rizwan
HATCI Electronic Systems Development, USA

Electronic Control Units

- Modern vehicles are equipped with 50-70 embedded electronic control units (ECUs)
- Tasks: overseeing door looks, climate, sunroof, body systems, transmission, advanced safety and collision avoidance systems, and pressure monitoring systems
- On each ECU, a specialized firmware is executed
- ECUs receive signals sent by sensors and based on these signals, ECUs control various key units in the vehicle
- ECUs are connected to various System Buses
- Local Interconnect Network (LIN), Controller Area Network (CAN), Media-Oriented System Transport (MOST)

Vulnerabilities in the In-Vehicle Network

- The in-vehicle networks connecting the ECUs to the buses are open networks attracting many cyber-attacks.
- Some ECUs are equipped with specific security capabilities but does not rule out the reality that the security requirements are not satisfied
- A security analysis showed that an adversary might tamper with the brakes when the car is running once access to the in-vehicle network via the Bluetooth is assured
- Compromising one ECU allows the attacker full access and control of all other ECUs

Firmware Update

- Urgent firmware fixes through recalls
- Feature upgrade, security patches, and customer complaints fixes.
- It is also possible to replace the whole firmware with a brand new one.
- All firmware updates are performed at the dealership. When the work is completed, the technician checks the targeted ECU to ensure it is functioning correctly
- Such updates are time and resource consuming, result in higher cost of labor and customer dissatisfaction, and prevent parallel updates as a result of physical equipment connection

Firmware Over The Air Updates

- A future trend in auto industry is to adopt Firmware Over-The-Air (FOTA) updates.
- FOTA refers to the process of wireless firmware transfer to the ECUs
- It is anticipated that FOTA will gain wide acceptance in automotive industry following the great success in mobile phone industry
- With FOTA, updates will be performed at the customer (any) location and not at the dealership site
- Fast, effective, and cost efficient approach of firmware updating

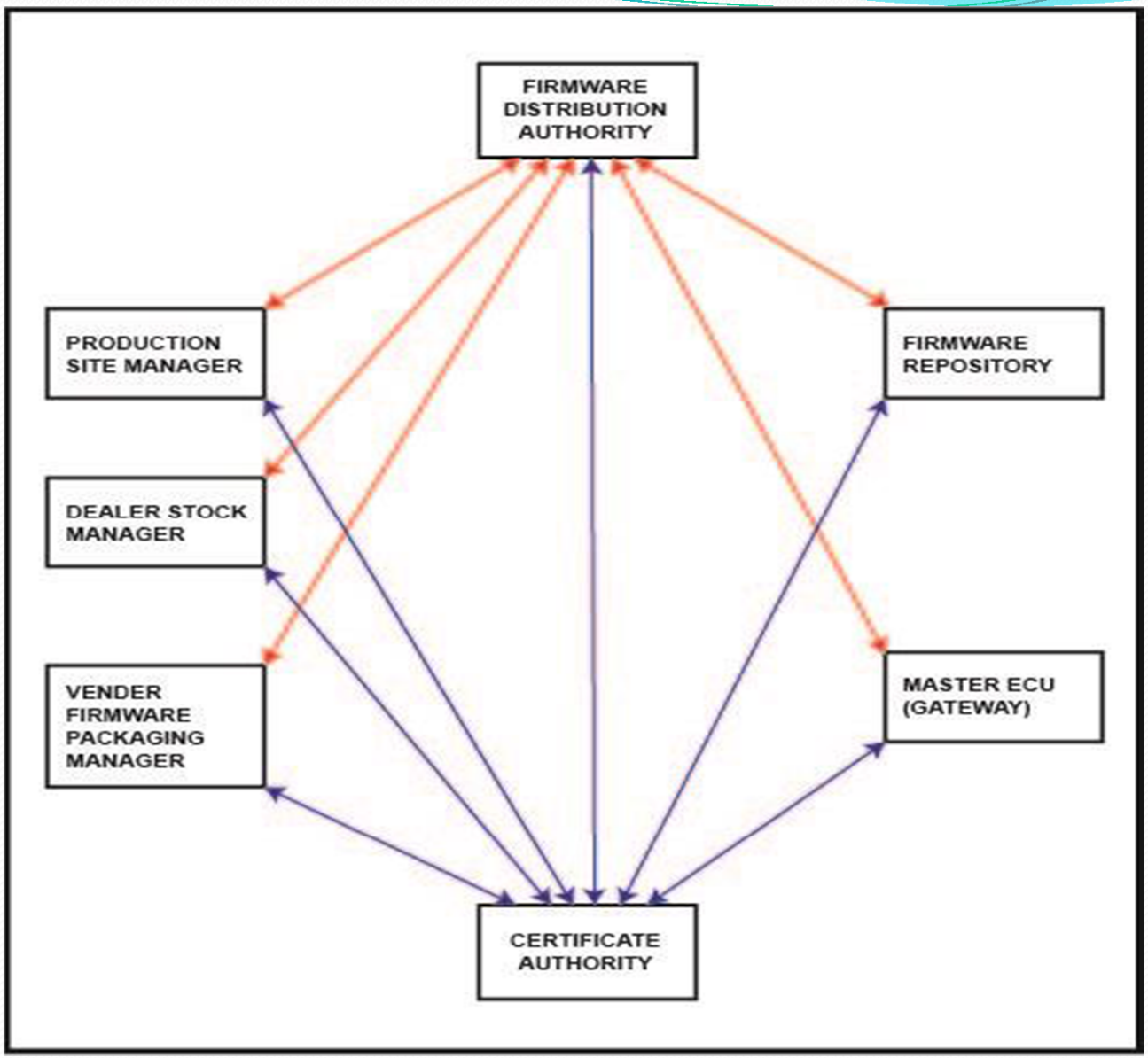
FOTA Updates Problem

- Firmware Over-The-Air (FOTA) definitely implies wireless communications
- Opens the door for many cyberattacks
- The consequences will be disastrous as safety is involved
- Therefore, there should be a serious and imminent move by auto industry to protect their vehicles' ECUs against all the possible attacks

Our Approach

- This paper presents security architecture for Over-The-Air update of ECUs
- It covers the update of firmware at the production site, dealer site, and customer location
- Updates include improving the ECU's functionality, firmware bug fixes, and brand new firmware to completely replace the old version
- A security protocol to implement this architecture is introduced
- Both symmetric and asymmetric cryptology will be used
- The suggested architecture and protocol will ensure that the security requirements will be satisfied

FOTA Security Architecture



FOTA Components

- Certificate Authority (CA) is in charge of issuing certificates to all components including the Firmware Distribution Authority (FDA). The CA can be part of the manufacturing site or an independent party
- Firmware Distribution Authority (FDA) is responsible for firmware updates to all vehicles at the dealership, production lines, and customer locations (garages, parking lots, streets, etc.)
- FDA receives the packaged firmware update from vendors and stores them in the firmware repository prior to sending it to vehicles
- It ensures all vehicles of that type and model have been updated and the updated ECUs are functioning properly
- The FDA is also in charge of issuing the session keys and the Message Authentication Code (MAC) keys

FOTA Components

- Firmware Repository (FR) is the firmware storage at the manufacturer's site
- FR is in charge of storing the firmware received from the FDA and providing the FDA with the needed firmware when requested
- Additional information including update version number, update type (full, bug fix, and enhancement), ECU type, date received, size of updates in bytes, vehicle model, vendor ID, and checksum are stored
- The Vendor Firmware Packaging Manager (VFPM) is responsible for preparing the firmware update and securely forwarding it to the Firmware Distribution Authority at the manufacturer's site to be stored in the Firmware Repository (FR)
- The Production Site Manager (PSM) is charge of updating all the vehicles in the production lines before sending them to dealerships
- Updating all the used and new cars at the dealership is the responsibility of the Dealer Stock Manager (DSM)

FOTA Components

- The Master ECU (MECU) plays a major role in the firmware update. It is a gateway equipped with the needed hardware, software, and memory
- For this purpose, the Telematics Control Unit (TCU) can also be used. Telematics includes GPS, mobile calling, navigation, …
- The MECU receives the firmware updates from the Firmware Distribution Authority and updates the ECUs in question in addition to updating its own
- It informs the FDA when the firmware update is completed
- Both DSM and PSM communicate with MECU of their vehicles, and thus behave like brokers

Certificate Authority (CA)

- The CA shares its public key (PU_{CA}) with the components. The component requests its certificate by sending its public key (PU_X), its ID (ID_X) and a nonce (N_X) all encrypted with the public key of the CA

- $CR_X = E [PR_{CA}, (PU_X || ID_X || T_1 || T_2)]$
- CA → X: $E [PU_X, CR_X || N_X]$

- Assuming the private key of the component (PR_X) is not compromised, this will assure no one but the requester can access the certificate
- In addition to the public key and ID, the certificates include a timestamp, T_1, and a certificate validity period (expiration date), T_2
- Both T1 and N_X are attached for additional assurance that the message involving the certificate is not a replay

Firmware Distribution Authority (FDA)

- FDA exchanges its certificate (CR_{FDA}) with all other components
- FDA creates the session keys; KS_{FR}, KS_{VFPM}, KS_{PSM}, KS_{DSM}, and $KS_{MECU,}$ to be shared with each component, encrypts them with the corresponding public keys; PU_{FR}, PU_{VFPM}, PU_{PSM}, PU_{DSM}, and PU_{MECU}
- FDA creates the MAC keys KM_{FR}, KM_{VFPM}, KM_{PSM}, KM_{DSM}, and KM_{MECU}, and sends them to the respective components
- VFPM informs the FDA about the packaging of a firmware (F) update
- FDA sends a notification message to the Firmware Repository and proceeds as follows:

$$X_1 = E\ [PR_{FDA}, C\ (KM_{FR}, F)\ ||\ Info\ ||\ ID_U\ ||\ T_{S1}]$$

$$FDA \rightarrow FR: E\ [KS_{FR}, F\ ||\ E\ (PU_{FR}, X_1)]$$

- Info= update version, update ID (ID_U), date received, ECU ID, vendor ID, vendor name, and type of update, T_{S1} is time stamp
- Authentication, Confidentiality, and Signature are enforced

Firmware Distribution Authority (FDA)

- Similar messages will be sent to the other parties with the exception of *info*

$$X_2 = E\,[PR_{FDA}, C\,(KM_{VFPM}, F) \,||\, ID_{ECU} \,||\, ID_U \,||\, T_{S2}]$$
$$FDA \rightarrow VFPM: E\,[KS_{VFPM}, F \,||\, E\,(PU_{VFPM}, X_2)]$$

$$X_3 = E\,[PR_{FDA}, C\,(KM_{PSM}, F) \,||\, ID_{ECU} \,||\, ID_U \,||\, T_{S3}]$$
$$FDA \rightarrow PSM: E\,[KS_{PSM}, F \,||\, E\,(PU_{PSM}, X_3)]$$

$$X_4 = E\,[PR_{FDA}, C\,(KM_{DSM}, F) \,||\, ID_{ECU} \,||\, ID_U \,||\, T_{S4}]$$
$$FDA \rightarrow DSM: E\,[KS_{DSM}, F \,||\, E\,(PU_{DSM}, X_4)]$$

$$X_5 = E\,[PR_{FDA}, C\,(KM_{MECU}, F) \,||\, ID_{ECU} \,||\, ID_U \,||\, T_{S5}]$$
$$FDA \rightarrow MECU: E\,[KS_{MECU}, F \,||\, E\,(PU_{MECU}, X_5)]$$

Firmware Repository(FR)

- After performing the required decryptions on the received message, calculating and verifying the MAC, and ensuring T_{S1} is current, FR stores the firmware, F, together with *Info* and any other data needed for indexing
- Upon receiving a request from the FDA, it retrieves the firmware in question and sends it to FDA within the following message:

$$X_6 = E\,[PR_{FR}, C\,(KM_{FR}, F) \,||\, ID_{ECU} \,||\, ID_U \,||\, T_{S6}]$$

$$FR \rightarrow FDA: E\,[KS_{FR}, F \,||\, E\,(PU_{FDA}, X_6)]$$

- FR stores the date the request was received and the date the firmware, F, was sent for auditing purposes

Vendor Firmware Packaging Manager (VFPM)

- Auto manufacturers deal with several vendors. Therefore, the the vendor ID is needed

  $X_7 = E\,[PR_{VFPM}, C\,(KM_{VFPM}, F) \,||\, ID_V \,||\, ||\, ID_{ECU} \,||\, ID_U \,||\, T_{S7}]$

  $VFPM \rightarrow FDA: E\,[KS_{VFPM}, F \,||\, E\,(PU_{FDA}, X_7)]$

- ID_V ,ID_{ECU}, ID_U, are the IDs for Vendor, ECU, and Update
- FDA can request updates when a bug is discovered or an improvement is needed

  $X_8 = E\,[PU_{VFPM}, B \,||\, E\,(PR_{FDA}, H\,(B) \,||\, ID_V \,||\, ID_{ECU} \,||\, T_{S8})]$

  $FDA \rightarrow VFPM: X_8$

  $X_9 = E\,[PU_{VFPM}, I \,||\, E\,(PR_{FDA}, H\,(I) \,||\, ID_V \,||\, ID_{ECU} \,||\, T_{S9})]$

  $FDA \rightarrow VFPM: X_9$

- Here, B is the bug detail, I the improvement detail, H (B) and H (I) represent the hash function of *B* and *I* respectively

Production Site Manager (PSM)

- After receiving the message X_3 from the FDA, PSM has to send the firmware to the MECU of the vehicles in that line
- PSM will act like the FDA and communicate similar encrypted messages with the MECU of each vehicle
- The update will be implemented in parallel for all vehicles
- The MECUs will inform the PSM when the updates are completed for that update ID (ID_U)
- PSM will then inform the FDA of all the vehicles that have their firmware updated by sending a message containing the list of vehicles VIN numbers, L
- L is needed for ensuring that all vehicles are updated and for reporting purposes

$$X_{10} = E\,[PR_{PSM}, C\,(KM_{PSM}, L) \,||\, U_{ID} \,||\, T_{S10}]$$

$$PSM \rightarrow FDA: E\,[KS_{PSM}, L \,||\, E\,(PU_{FDA}, X_{10})]$$

Dealer Stock Manager (DSM)

- The firmware updates at the dealership site are controlled by the DSM
- The task of the DSM is similar to that of the PSM
- The work will be completed by the MECUs in parallel here too

Master ECU (MECU)

- MECU will communicate with the driver through the vehicle screen or via email to warn about a new update and request the vehicle to be turned off, as soon it is possible
- Vehicles in the production lines and at the dealerships are assumed to be not running since they are under control
- Once the the MAC is verified, MECU will extract the firmware F, ID_{ECU}, and ID_U from the message sent by FDA
- The MECU will then communicate with the desired ECU based on the ID_{ECU} to start the updating process.
- MECU of customer's vehicle will then inform the FDA (update done)

$$X_{11} = E\,[PR_{MECU}, \,||\, ID_{ECU} \,||\, ID_U \,||\, VIN \,||\, T_{S11}]$$

$$MECU \rightarrow FDA: E\,(PU_{FDA}, X_{11}]$$

- For firmware update at the dealership and production sites, the MECU will send a similar message to DSM and PSM respectively

Extending the Architecture with SOTA

- To accommodate software download and software update, two components need to be added to the architecture; Software Download Manager (SDM) and Software Charge Manager (SCM)
- Both SDM and SCM will be connected to FDA and CA
- With these two new components, the auto manufacturer will be able to implement Software On-The-Air (SOTA) in addition to FOTA
- Extend with Remote Diagnosis Manager (RDM)
- Upon customer request, it is anticipated that RDM will connect to the vehicle and diagnose problems, and send a message requesting firmware update for the particular ECUs to FDA
- RDM will be responsible for testing the update to certify the ECU is functioning as expected
- RDM will be connected to both FDA and CA

More on MECU

- In the aforementioned protocol, it was assumed that one MECU will take care of updating all the ECUs
- An extension would be adding more MECUs and dividing the ECUs among them
- The added MECUs can play a backup role too in case an MECU is not functioning
- If an MECU is compromised, it will not impact other MECUs (other ECUs)
- A further extension will be replacing the Master ECU with the Telematics Control Unit (TCU)
- The TCU is a small computer that listens in on the communications of other electronic systems (ECUs) in the vehicle, and then disseminates that information as necessary
- TCU is connected to a server and we can have FDA as the server

Conclusion and Future Work

- To account for possible security attacks, this paper presented a security architecture and protocol to protect the updating of firmware of various ECUs at the customer location, the dealership site, and the production lines
- The suggested security architecture and protocol can be further extended to include Software On-The-Air (SOTA)
- Future work will concentrate on the most suitable algorithms for symmetric and asymmetric cryptography, MAC and hash functions, and the length of the various keys

Questions?

Thank You!