The Role of Secure Flash Memory in Automotive Applications

Anthony Le
Vice President Marketing
Macronix America

August 6, 2019
Agenda

• Security Objectives
• Why Secure Flash in Automotive?
• Types of Information that Needs to be Kept Secure
• Flash Comparisons
• Conclusion
Security Objectives in Auto Designs

- Confidentiality
  - Secure storage
  - Secure boot
  - Secure data exchange

- Integrity
  - Replay protection
  - Bus protection
  - Anti cloning
  - Anti-tamper
  - Identification
  - Authentication

- Availability
  - Access Management
Why Secure Flash in Automotive?

- ADAS and electrification functions/features in automobiles rapidly growing
- Exponential rise in stored data, particularly in ADAS functions
- Connectivity to public networks creating a unsecure environment
- More onboard pay-for-use apps and capabilities requiring numerous authorization credentials
- Auto as a payment platform on the rise (Tolls, Parking, etc.)
- Strong correlation with security and safety and a need for deterministic behavior
- Support for Root of Trust (RoT) requirements through unique ID, authentication, and an encrypted link
- *Traditional embedded flash densities are increasingly becoming inadequate to store all this data*
## Flash Comparisons

<table>
<thead>
<tr>
<th></th>
<th>eFlash</th>
<th>External SPI Flash</th>
<th>Secure Flash</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Interface</strong></td>
<td>Parallel</td>
<td>Standard SPI</td>
<td>Standard SPI (with ArmorFlash)</td>
</tr>
<tr>
<td><strong>Density Options</strong></td>
<td>Low</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td><strong>Information Confidentiality</strong></td>
<td>Usually Strong</td>
<td>Weak</td>
<td>Strong</td>
</tr>
<tr>
<td><strong>Information Integrity</strong></td>
<td>Usually Strong</td>
<td>Weak</td>
<td>Strong</td>
</tr>
<tr>
<td><strong>Security Availability</strong></td>
<td>Usually Strong</td>
<td>Weak</td>
<td>Strong</td>
</tr>
</tbody>
</table>
The ETSI TR-102-638 Intelligent Transport Systems technical report exemplifies that the opportunities for hacking are enormous.
Some Examples of Information Being Stored in Automobiles

<table>
<thead>
<tr>
<th>Keys</th>
<th>Authorized users &amp; access levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credentials</td>
<td>Secure Logs</td>
</tr>
<tr>
<td>DRM (Digital Rights Management)</td>
<td>Financial / eCommerce information</td>
</tr>
<tr>
<td>Biometrics (fingerprints, facial etc.)</td>
<td>Vehicle experience authentication keys to unlock additional capabilities</td>
</tr>
<tr>
<td>Passwords</td>
<td>Contacts</td>
</tr>
<tr>
<td>Device identity / identities</td>
<td>Audio/video streaming</td>
</tr>
<tr>
<td>Secure Logs</td>
<td>Medical info.</td>
</tr>
<tr>
<td>Financial / eCommerce information</td>
<td>Financial / eCommerce information</td>
</tr>
<tr>
<td>Vehicle experience authentication keys to unlock additional capabilities</td>
<td>Vehicle experience authentication keys to unlock additional capabilities</td>
</tr>
<tr>
<td>Passwords</td>
<td>Contacts</td>
</tr>
<tr>
<td>Biometrics (fingerprints, facial etc.)</td>
<td>Vehicle experience authentication keys to unlock additional capabilities</td>
</tr>
</tbody>
</table>
Other Use Cases for Secure Flash

• Secure data storage along with code storage
• Design upgrades for security without changing CPUs/MPUs (or MPUs without secure embedded memory)
• Combining non-volatile memory with a secure element (lowering BOM costs)
• OS architectures with several users requiring multiple sets of credentials (multi-tenancy / hypervisors)
• Secure (re)provisioning in unsecure manufacturing environments or in the field
• Protecting firmware rollback and anti-cloning
• Securing against host/device ease-dropping and memory tampering
Conclusion

The growth of connected vehicles & ADAS applications continues to explode and along with it the exponential growth of data.

Safety and security
- A robust security framework protects against unauthorized actions taken by individuals, while improving safety by incorporating additional controls in the system design.

Non-volatile memory requires a range of security mechanisms and policies to ensure identity, confidentiality, integrity, authenticity, and availability.

Advanced secure memory storage features found in devices such as the Macronix ArmorFlash™, is a critical component to achieving security objectives in future automotive systems.

Integrating secure non-volatile in internet of vehicles article in Electronic Design magazine