Secure Software Delivery and Installation in Embedded Systems

André Adelsbach, Ulrich Huber, Ahmad-Reza Sadeghi
Horst-Görtz-Institute, Bochum, Germany

ISPEC 2005 Presentation
Singapore, April 13, 2005
HW* and SW* will become separate products within an embedded system, thus providing an additional revenue source to SW providers

CHANGES IN THE ROLE OF SW IN AN EMBEDDED SYSTEM

<table>
<thead>
<tr>
<th>Current situation</th>
<th>Expected future situation</th>
</tr>
</thead>
<tbody>
<tr>
<td>• HW* and SW* as one product from same supplier</td>
<td>• HW and SW as separate products, potentially from different suppliers</td>
</tr>
<tr>
<td>• SW updates mainly necessary for warranty-based replacement of defective SW</td>
<td>• In addition, SW updates attractive due to new and/or enhanced functionality</td>
</tr>
<tr>
<td>• No revenues for SW provider due to warranty obligations</td>
<td>• Additional revenue source for SW provider due to value-added and customers’ willingness to pay</td>
</tr>
</tbody>
</table>

* HW: hardware, SW: software

There are four major difficulties when a provider installs a SW update in a vehicle

DIFFICULTIES WITH SW UPDATES IN A VEHICLE

- Service provider needs specific equipment, e.g., diagnostic tester, and skills.
- Service providers have different skill sets.
- Compatibility among SW components is not self-evident due to number of ECUs.
- High economic value of vehicle and failure consequences induce tough requirements.

The system model contains five different roles which correspond with current players in the automotive industry

**ROLES IN THE SYSTEM MODEL AND THEIR COUNTERPARTS IN THE AUTOMOTIVE INDUSTRY**

**Overall Equipment Manufacturer (OEM)**
- Develops and assembles the user platform in cooperation with his suppliers
- Automotive counterpart: car manufacturers such as Daimler Chrysler, GM, Toyota, etc.

**Software Application Programmer (SAP)**
- Develops and distributes SW components for the user platform in the form of updates and/or upgrades
- Automotive counterpart: suppliers such as Bosch, Delphi, Denso, Siemens, Visteon, etc.

**Installation Service Provider (ISP)**
- Maintains the user platform via HW repair/replacement and SW installation with specific equipment
- Automotive counterpart: car dealers, garages, road service teams, etc.

**User platform (UP)**
- Is an embedded system which consists of several components whose SW can be updated
- Automotive counterpart: car

**License Provider (LP)**
- Generates licenses for SW from OEM and SAPs, distributes them to user platforms via ISPs
- Automotive counterpart: not existing or assumed by OEMs and SAPs

**Additional role: Trusted Third Party (TTP)**

* Overall Equipment Manufacturer

There are many scenarios which lead to damage to an innocent party, four of which we detail.

**FOUR EXEMPLARY SCENARIOS LEADING TO DAMAGE TO INNOCENT PARTIES**

<table>
<thead>
<tr>
<th>Example</th>
<th>Scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>SW is not authentic</strong>&lt;br&gt;• An honest garage installs a supposedly correct SW component for the ABS&lt;br&gt;• The adversary has replaced the SW component with a defective one&lt;br&gt;• The car fails, leading to an accident</td>
</tr>
<tr>
<td>2</td>
<td><em><em>ISP</em> is not qualified</em>*&lt;br&gt;• An unqualified garage installs SW for the airbags&lt;br&gt;• Due to wrong parameterization, the airbags do not trigger off properly&lt;br&gt;• The victim sues the OEM*</td>
</tr>
<tr>
<td>3</td>
<td><strong>Innocent ISP is accused</strong>&lt;br&gt;• A SW component has a known error which might lead to a short circuit and set fire&lt;br&gt;• A malicious car owner burns his car and accuses his innocent garage of having installed the SW component</td>
</tr>
<tr>
<td>4</td>
<td><em><em>SAP</em> is discriminated</em>*&lt;br&gt;• An honest SAP develops a SW component&lt;br&gt;• The OEM has a SW component with identical functionality, but higher price&lt;br&gt;• The OEM configures each car such that only his SW can be installed</td>
</tr>
</tbody>
</table>

* ISP: Installation Service Provider, OEM: Overall Equipment Manufacturer, SAP: Software Application Programmer

Each role in the system model has specific requirements regarding any software installation.

REQUIREMENTS OF ALL ROLES IN THE SYSTEM MODEL

**OEM**
- Correctness
- Rights enforcement
- Compatibility enforcement
- ISP clearance enforcement
- Confidentiality
- Integrity

**Software Application Programmer (SAP)**
- All OEM requirements
- Non-discrimination

**User**
- Correctness
- Non-repudiation
- Unique installation origin
- Authenticity

**Installation Service Provider (ISP)**
- Correctness
- Non-repudiation
- Clearance enforcement
- Non-discrimination
- Frame-proofness

**License Provider (LP)**
- Non-repudiation

Three basic protocols are a prerequisite of any SW installation

SYSTEM SETUP – THREE BASIC PROTOCOLS PRECEDING ANY SW INSTALLATION

1. Assignment of clearance levels to ISPs
   - **ISP**
   - ClearReq
   - **TTP**
   - ClearIss
   - \( \xi_{\text{clear}} \)

2. Certification of SW components
   - **OEM/SAP**
   - SWSub
   - **TTP**
   - SWIss
   - \( \xi_{\text{sw}}, \sigma_{\text{integer}} \)
   - \( s_{\text{enc}} = \text{Enc}_{\text{PKBE}}(s), \sigma_{\text{comm}} = \text{PropComm}() \)

3. Distribution of SW licenses
   - **ISP**
   - LicReq
   - **LP**
   - LicIss
   - \( \gamma_{\text{lic}} \)
   - \( \xi_{\text{lic}} \)

Distribution of SW over broadcast channel

Based on asymmetric cryptography

**Message flow**

- **Party X participates in protocol**

---

* ISP: Installation Service Provider, TTP: Trusted Third Party, SAP: Software Application Programmer, LP: License Provider

In the SD scheme, each receiver obtains the keys just off his key path within each subtree

BROADCAST ENCRYPTION: KEYS OF AN EXEMPLARY USER IN THE SUBSET DIFFERENCE SCHEME

Tree of level 0 (root) Subtrees of level $i$

<table>
<thead>
<tr>
<th>$i = 0$</th>
<th>$i = 1$</th>
<th>$i = 2$</th>
<th>$i = 3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$U_5$</td>
<td>$U_5$</td>
<td>$U_5$</td>
<td>$U_5$</td>
</tr>
</tbody>
</table>

Example with $n = 16$ users and tree height $\log_2 n = 4$

| No. of stored keys | 4 | 3 | 2 | 1 | $\Sigma$ 10 |

Source: The LSD Broadcast Encryption Scheme, CRYPTO 2002, LNCS 2442, pp. 47 - 60
Compared to SD*, the basic LSD** scheme significantly reduces the storage requirements of the users by slightly increasing the message header length.

COMPARISON OF SD* AND BASIC LSD** PERFORMANCE PARAMETERS

<table>
<thead>
<tr>
<th></th>
<th>SD</th>
<th>Basic LSD</th>
</tr>
</thead>
<tbody>
<tr>
<td>User storage</td>
<td>$O(\log^2 n)$</td>
<td>$O(\log^{3/2} n)$</td>
</tr>
<tr>
<td>Example</td>
<td>406 keys for $2^{28}$ users</td>
<td>146 keys for $2^{28}$ users</td>
</tr>
<tr>
<td>Message header</td>
<td>$O(r)$</td>
<td>$O(2 \cdot r) = O(r)$</td>
</tr>
<tr>
<td>User computation</td>
<td>$O(\log n)$</td>
<td>$O(\log n)$</td>
</tr>
</tbody>
</table>

* Subset difference
** Layered subset difference, not lysergic acid diethylamide

Source: The LSD Broadcast Encryption Scheme, CRYPTO 2002, LNCS 2442, pp. 47 - 60
A SW installation consists of four basic steps

FOUR STEPS OF A SW INSTALLATION

1. SW request: \( \text{SWReq}(k, m, \bar{r}_n) \)
   - \( \text{UP}^* \)

2. SW delivery: \( \text{SWDel}(\sigma^{\text{enc}}, \gamma^{\text{lic}}) \)
   - \( \text{ISP}^* \)

3. Installation confirmation: \( \text{ExtInstConf}(\gamma^{\text{lic}}, \text{ind}) \)
   - \( \sigma^{\text{inst}} \)

4. Acknowledgment of confirmation: \( \text{ConfAck}(\sigma^{\text{conf}}) \)
   - \( \sigma^{\text{ack}} \)

* UP: User Platform, ISP: Installation Service Provider
** In order to execute \( \text{SWDel}() \), the ISP must have executed \( \text{LicReq}() \) and received \( \gamma^{\text{lic}} \)

In each step of a SW installation, the party in charge verifies several necessary conditions

NECESSARY CONDITIONS FOR EACH SW INSTALLATION STEP (1/2)

① Conditions for a user platform to issue a SW request
- User platform and SW are compatible
- ISP* has sufficient clearance level
- All certificates match
- SW certificate $\xi^\text{SW}$ is authentic, i.e., generated by the TTP*
- Property commitment $\sigma^\text{comm}$ is authentic, i.e., generated by the SW provider
- Clearance level certificate is authentic, i.e., generated by the TTP

② Conditions for an ISP to deliver a SW installation package
- SW request is authentic, i.e., generated by the user platform
- The set of requested rights is a subset of the allowed usage rights of the SW, i.e., does not violate the terms and conditions
- License provider issues a valid license
- ISP possesses the requested SW
- User platform has a valid ID

Main criteria
- Compatibility, clearance enforcement, and authenticity
- Authenticity, rights enforcement, and soundness

* ISP: Installation Service Provider, TTP: Trusted Third Party
In each step of a SW installation, the party in charge verifies several necessary conditions

**NECESSARY CONDITIONS FOR EACH SW INSTALLATION STEP (2/2)**

1. **Conditions for a user platform to deliver an installation confirmation**
   - SW installation package is authentic, i.e., generated by the ISP*
   - License is authentic, i.e., generated by the LP, and grants the requested rights
   - SW is integer, i.e., identical to the SW which the TTP certified
   - Decryption of SW succeeds
   - Internal installation in target component succeeds (details follow)

2. **Conditions for an ISP to deliver an acknowledgment**
   - Installation confirmation is authentic, i.e., generated by the user platform
   - Installation result was "success"

---

* Installation Service Provider

The user platform has an internal structure consisting of three elements: a trusted component, regular components and an internal communication network.

**INTERNAL STRUCTURE OF THE USER PLATFORM**

- **$u_0$**: trusted component based on trusted computing HW
- **$u_i$**: regular low cost component

Internally, a SW installation within a user platform consists of three basic steps.

**THREE INTERNAL STEPS OF A SW INSTALLATION WITHIN A USER PLATFORM**

1. **Installation instruction:**
   - **Instlnstr\((i,m,\hat{\rho}^n)\)**
   - **SW installation succeeded internally**

2. **Installation confirmation:**
   - **IntInstConf\((m)\)**
   - Based on symmetric cryptography

3. **Usage instruction:**
   - **UseInstr\((i,m,\hat{\rho}^n)\)**

\(u_0\): Trusted component
\(u_i\): Target component
\(1 \leq i \leq n\)
The paper makes two major contributions

CONCLUSION: TWO MAJOR CONTRIBUTIONS OF THE PAPER

Requirements model for SW installation in embedded systems
- Major roles included in requirements model
- Compatibility of SW components and skill set of ISPs considered
- Basic license and DRM scheme

Secure installation protocol meeting the requirements
- Public Key Broadcast Encryption (PKBE) for achieving non-discrimination
- Trusted Computing for achieving trust in user platform with little additional hardware

Open Problem
Reduced need for TTP in setup phase by aggregating the PKBE key material bottom-up