Rollout of Security Credentials in Industrial Environments

SECURWARE 2010

Rainer Falk, Steffen Fries
GTF IT Security
Corporate Technology
Networking the integrated technology company

Customers

Chief Technology Officer (CTO)
- Review innovation strategies
- Drive technology based synergies
- Secure innovation power
- Technology assessments
- Governance and guidance

Sectors / Divisions

Industry

Energy

Healthcare

Siemens IT Solutions and Services (SIS)
Siemens Financial Services (SFS)

Regions

Corporate Research and Technologies (CT T)
- GTFs with multiple impact
- Pictures of the Future
- Accelerators

Corporate Development Center (CT DC)
- Software-Entwicklungs-partner für die Sektoren

Corporate Intellectual Property and Functions (CT I)
- Intellectual Property services & strategy
- Standardization, environmental affairs
- Global information research

Corporate Technology (CT)
Industrial Environments: Process Automation
Industrial Environments: Factory Automation
Industrial Environments: Building Automation
Industrial Environments: Energy Automation
IT-Security Becomes a Pre-requisite for Future Control Systems Driven by Convergence of Safety & Security

**Status**
- Predominantly isolated communication networks
- Often proprietary networks and applications
- Physically secured access to networks
- Long lifetime of control equipment
- Systems are mainly designed for performance, reliability and safety, not security
- Often availability is the most important security objective

**Trends**
- Increasing usage of standard OSs and applications
- Widespread usage of Ethernet and TCP/IP (including Internet)
- Increasing usage of wireless networks
- Interconnection of formerly isolated networks
- Increasing intelligence in peripheral components (e.g. Intelligent Access Devices)
- IT-security becomes a pre-requisite for safety applications
Security and Safety

Security / IT Security:
Prevention of consequences of threats to a system (intentionally) caused by humans and/or environment

Safety:
Prevention of threats to humans and environment caused by technical systems
Interrelation Between IT-Security and Dependability of a System

**IT-Security**

Helps to ensure the functional correctness in case of (active) attacks

- system (SW and data)
- controls
- access

**Dependability**

- Reliability
- Availability
- Maintainability
- Safety

Security Incident: may threaten the dependability of a system

Consequences: functional behavior may be changed; potential limitation of availability and safety

Reliability / Availability: Probability of deficiency of the security measures

Remark: Failures caused by security attacks cannot be assumed to be independent! ⇒ Therefore classical safety/failure analyses do not cover them properly
Example: Maroochy Waste Water Incident

Queensland, Australia, 2000:
Former contractor took control of 150 sewage pumping stations. Over a 3-month period, he released one million liters of untreated sewage.

Unauthorized access to the control system over a unsecured communication path.

Communications sent by radio links to wastewater pumping stations were being lost
Pumps were not working properly
Alarms put in place to alert staff to faults were not going off

Remark: Failures caused by security attacks cannot be assumed to be independent! Therefore classical safety/failure analyses do not cover them properly
Example:
Potential Derogation of Dependability through Security

- The usage of standard anti-virus software may lead to blocking of safety relevant communication
- Standard anti-virus software typically requires human interaction
- Usage of IT-security mechanisms may occupy too many system resources

Standard IT-security mechanisms known from the office world have to be adapted to meet dependability requirements
Example: Usage of “Plagiarisms” Influences System Behavior

China, 2008:
System performance of mobile networks were decreased noticeably. The service company instructed for maintenance used cheaper plagiarisms instead of original spare parts.

IT-security measures (e.g. not forgeable “genuineness chip“) can help to identify and thereby reduce the usage of plagiarisms.
Differences and Security Applications
Automation Network Specifics:
Focus on Different Security Requirements

- Confidentiality (Data): High (Office) vs. Low – Medium (Automation Network)
- Integrity (Data): Medium (Office) vs. High (Automation Network)
- Availability / Reliability (System): Medium (Office) vs. High (Automation Network)
- Non-Repudiation: Medium (Office) vs. High (Automation Network)
- Component Lifetime: Short - medium (Office) vs. Long (Automation Network)

“Office“ Security Concepts are not directly applicable for Automation Networks
## Embedded Security Mechanisms Provide Essential Functionality for Ensuring System Integrity

Security is required to ensure Safety-relevant system properties in environments exposed to attacks.

<table>
<thead>
<tr>
<th>Security Mechanism</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Plant Integrity Check</strong></td>
<td>Verify integrity of overall plant installation (deployed components, cabling, software). This ensures detection of unauthorized changes of the plant installation.</td>
</tr>
<tr>
<td><strong>Original spare parts (Anti-Counterfeiting)</strong></td>
<td>Ensure that original spare parts are installed, and not counterfeited replacements with poor quality.</td>
</tr>
<tr>
<td><strong>Software Integrity Check</strong></td>
<td>Ensure that firmware and configuration has not been altered. Device is going to regular operation only with valid software configuration.</td>
</tr>
<tr>
<td><strong>Secure Software Update</strong></td>
<td>Ensure that only approved software updates are installed. Ensure that software is installed in compliance with defined update procedures.</td>
</tr>
<tr>
<td><strong>Encrypted Machine Communication</strong></td>
<td>Encrypted communication prevents manipulation and interception of machine control and service data when transmitted over networks (device control, plant, and public networks / remote service).</td>
</tr>
</tbody>
</table>
Credential Lifecycle
Security Credential Have to be Managed Along Their Whole Lifecycle

- Session keys destructed after session ending
- Long term keys are deleted, after keys have been renewed.
- Lifetime may end regularly or if the key has been compromised.

- Typically long term (secure or private) keys are archived to enable access to encrypted data
- Cryptographic keys have a dedicated lifetime
  - may be performed by the security protocol
  - based on a given security policy

- Internal Generation (e.g., CSR)
- External Generation
- Long term keys, session keys

- Typically done for asymmetric keys through a certificate authority (CA)
- May be part of the key generation, depending on the credential

- Distribution
  - Depends on generation method
  - offline/online (in-band, out-of-band)

- Storage
  - obfuscated in firmware, software
  - in secured memory (e.g., flash)
  - separate hardware module (e.g., smart card or a trusted platform module)

- Archiving
  - Typically long term
  - (secure or private) keys are archived to enable access to encrypted data

- Certification
  - Depends on generation method
  - offline/online (in-band, out-of-band)

- Update
  - Sessions keys destructed after session ending
  - Long term keys are deleted, after keys have been renewed.
  - Lifetime may end regularly or if the key has been compromised.

- Generation
Security Credential Lifecycle Management – a Service Accompanying Products

- **Generation**
  - Product Design: Definition of necessary security features in base architecture

- **Manufacturing**
  - Generation of vendor specific security parameter supporting the product individualization.

- **Projection**
  - Projection of use case and/or customer specific security parameter

- **Installation**
  - Deployment in customer infrastructure comprises key generation, certification, distribution and storage. Base can be the vendor specific credentials.

- **Operation**
  - Security parameter maintenance: key update, revocation and/or key archival

- **Decommissioning**
  - Secure deletion of security parameter: comprises key archiving, key destruction

- **Development and Manufacturing of Products, Security Service Definition**

- **Development and Deployment of Security Services**

- **Certification**

- **Distribution**

- **Storage**

- **Update**

- **Archiving**

- **Destruction**
Potential Approaches
Different Approaches can be Followed for Security Parameter Rollout

**Offline parameter distribution**
- Performed using dedicated engineering tools directly connected to the device or via a separate network
- Requires a (mobile or fixed) engineering station in the offline network having all parameter sets for the devices to be bootstrapped available.

**Out-of-band parameter distribution**
- Separate logical or physical communication channel used to configure security parameter. Basically resembles the offline distribution approach using an online connection instead of the separate physical network.
- Devices may already possess a cryptographic credential, which can be provided by the device manufacturer.

**In-band parameter distribution**
- Distribution using the same communication channels as used during regular operation
- May be based on pre-configured device identifier (like the MAC address), manufacturer installed security credentials or even liaison devices.
Credential Bootstrapping has to be Suitable for Addressed Environment
Outlook
Research Topics – Security and Device Authentication

Situation

- Machine-2-Machine connectivity down to field devices is a major driver for Future Internet. Potentially more than 60 Billion devices will be connected. All industries are affected including manufacturing, process, building, energy automation, transportation, health.
- Device authentication is the prerequisite to ensure an appropriate protection of communication between different devices. This is the basis to realize secure device-oriented services like secure control, monitoring, remote service, metering, licensing or anti counterfeiting.
- Device credentials (keys, certificates) have to be generated and managed efficiently
- The non-human security environment requires new device-oriented security and identity infrastructures.
- The huge number of devices and the specific application environment require a zero-configuration effort.
- Process comprises the generation (short and long term), distribution and implementation of initial security parameter of the target devices.

Topics

- Efficient cryptographic mechanisms for device authentication and secure device communication
- Device security platform module
- Device-oriented security and identity infrastructure (processes, scalability, limits of authority, privacy)
- Plug-and-play security to avoid administrative burden
- Secure device-oriented services

Industrial systems for all verticals like energy, transportation, automation systems, health require secure device authentication and machine-2-machine communication as a core security feature. Siemens is a leading provider for technology and solutions in these areas.