DIGITAL AUTHENTICATION AND EMBEDDED SECURITY

VALUE OF TRANSACTIONS CONDUCTED VIA MOBILE HANDSETS AND TABLETS

World Market, Forecast: 2014 to 2019

TRANSACTION VALUE VIA MOBILE

THREATS
- Malware
- Malicious applications
- Privacy violations relative to application collection and distribution of data
- Security weakness in any part of the wireless carrier infrastructure
- Vulnerabilities in the payment infrastructure/ecosystem
- SMS Vulnerabilities
- Hardware and operating system vulnerabilities
- Man in the middle attacks
- Complex supply chain and new entrants into the mobile ecosystem

SOLUTIONS

The trusted platform module (TPM), designed by the Trusted Computing Group, is a specialized chip on an endpoint device that stores encryption keys specific to the host system for hardware authentication. TPM 2.0 is designed to offer comprehensive protections based on hardware roots of trust, and addresses the growing market demand for enhanced security and privacy. It is also designed to offer flexibility for industry implementations across a broad range of platforms, including servers, desktops, embedded systems, mobile devices, and network equipment. Microsoft already requires a TPM chip on any device running Windows 8, including phones and tablets, as well as servers.

HCE (Host card emulation) is a cloud-based mechanism that allows banks to launch mobile NFC products without needing to make use of the SIM or other secure element. It does so by allowing the mobile device OS to communicate directly over the NFC interface in card emulation mode. Since its introduction in the KitKat version of the Android operating system, HCE support in smartphones has been growing at a fast pace.

The secure element (SE) is a secure microprocessor (a smart card chip) that includes a cryptographic processor to facilitate transaction authentication and security, and provide secure memory for storing payment applications.

A TEE (Trusted execution environment) provides a way of enhancing the security of mobile devices and executing sensitive operations on devices running standard operating systems. It relies on hardware roots of trust for boot and storage, provides cryptographic functionalities, allows for the secure storage of data and keys, and executes trusted applications (TAs) in a controlled environment separate from the mobile OS. With ARM integrating its TrustZone architecture into every Cortex-A family processors, future connected devices will have an embedded software environment that can secure devices from the hardware level and upward.

MARKET PROJECTIONS

EMBEDDED SECURITY SHIPMENTS BY TECHNOLOGY

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Embedded Secure Element</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trusted Platform Module</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trusted Execution Environment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Host Card Emulation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

TRANSACTION VALUE VIA MOBILE

World Market, Forecast: 2014 to 2019

TRANSACTION VALUE VIA MOBILE

THREATS
- Malware
- Malicious applications
- Privacy violations relative to application collection and distribution of data
- Security weakness in any part of the wireless carrier infrastructure
- Vulnerabilities in the payment infrastructure/ecosystem
- SMS Vulnerabilities
- Hardware and operating system vulnerabilities
- Man in the middle attacks
- Complex supply chain and new entrants into the mobile ecosystem

SOLUTIONS

The trusted platform module (TPM), designed by the Trusted Computing Group, is a specialized chip on an endpoint device that stores encryption keys specific to the host system for hardware authentication. TPM 2.0 is designed to offer comprehensive protections based on hardware roots of trust, and addresses the growing market demand for enhanced security and privacy. It is also designed to offer flexibility for industry implementations across a broad range of platforms, including servers, desktops, embedded systems, mobile devices, and network equipment. Microsoft already requires a TPM chip on any device running Windows 8, including phones and tablets, as well as servers.

HCE (Host card emulation) is a cloud-based mechanism that allows banks to launch mobile NFC products without needing to make use of the SIM or other secure element. It does so by allowing the mobile device OS to communicate directly over the NFC interface in card emulation mode. Since its introduction in the KitKat version of the Android operating system, HCE support in smartphones has been growing at a fast pace.

The secure element (SE) is a secure microprocessor (a smart card chip) that includes a cryptographic processor to facilitate transaction authentication and security, and provide secure memory for storing payment applications.

A TEE (Trusted execution environment) provides a way of enhancing the security of mobile devices and executing sensitive operations on devices running standard operating systems. It relies on hardware roots of trust for boot and storage, provides cryptographic functionalities, allows for the secure storage of data and keys, and executes trusted applications (TAs) in a controlled environment separate from the mobile OS. With ARM integrating its TrustZone architecture into every Cortex-A family processors, future connected devices will have an embedded software environment that can secure devices from the hardware level and upward.

MARKET PROJECTIONS

EMBEDDED SECURITY SHIPMENTS BY TECHNOLOGY

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Embedded Secure Element</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trusted Platform Module</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trusted Execution Environment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Host Card Emulation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

TRANSACTION VALUE VIA MOBILE

World Market, Forecast: 2014 to 2019

TRANSACTION VALUE VIA MOBILE

THREATS
- Malware
- Malicious applications
- Privacy violations relative to application collection and distribution of data
- Security weakness in any part of the wireless carrier infrastructure
- Vulnerabilities in the payment infrastructure/ecosystem
- SMS Vulnerabilities
- Hardware and operating system vulnerabilities
- Man in the middle attacks
- Complex supply chain and new entrants into the mobile ecosystem

SOLUTIONS

The trusted platform module (TPM), designed by the Trusted Computing Group, is a specialized chip on an endpoint device that stores encryption keys specific to the host system for hardware authentication. TPM 2.0 is designed to offer comprehensive protections based on hardware roots of trust, and addresses the growing market demand for enhanced security and privacy. It is also designed to offer flexibility for industry implementations across a broad range of platforms, including servers, desktops, embedded systems, mobile devices, and network equipment. Microsoft already requires a TPM chip on any device running Windows 8, including phones and tablets, as well as servers.

HCE (Host card emulation) is a cloud-based mechanism that allows banks to launch mobile NFC products without needing to make use of the SIM or other secure element. It does so by allowing the mobile device OS to communicate directly over the NFC interface in card emulation mode. Since its introduction in the KitKat version of the Android operating system, HCE support in smartphones has been growing at a fast pace.

The secure element (SE) is a secure microprocessor (a smart card chip) that includes a cryptographic processor to facilitate transaction authentication and security, and provide secure memory for storing payment applications.

A TEE (Trusted execution environment) provides a way of enhancing the security of mobile devices and executing sensitive operations on devices running standard operating systems. It relies on hardware roots of trust for boot and storage, provides cryptographic functionalities, allows for the secure storage of data and keys, and executes trusted applications (TAs) in a controlled environment separate from the mobile OS. With ARM integrating its TrustZone architecture into every Cortex-A family processors, future connected devices will have an embedded software environment that can secure devices from the hardware level and upward.

MARKET PROJECTIONS

EMBEDDED SECURITY SHIPMENTS BY TECHNOLOGY

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Embedded Secure Element</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trusted Platform Module</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trusted Execution Environment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Host Card Emulation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>