Trusted Execution Environments (and Android)

Jan-Erik Ekberg
Director of Advanced Development, Trustonic
9.9.2015
Content:

1) What is a TEE

2) TEE on Android (today)

3) (Research) use cases
What is a TEE (Trusted Execution Environment)

**Hardware-assisted isolated execution**
- from ”normal world OS” and
- between ”trusted applications”

**Integrity of operation**
- ”part of” secure boot
- trusted path
- rollback protection

**(Unique) access to secrets**
- secure storage
- device authentication
- remote attestation

**(Availability)**
- code provisioning

**Typical properties**
- fast / full memory access
- runs at full processor speed
- ”native binaries / ”standard C”

The isolation is defined by
• Processor contexts
• Memory access / MMU, caches
• DMA / IRQs

New HW architectures are emerging:
• Intel SGX / TrustLite (research)
Where do we find TEEs today?

- Most(many) middle to high-end Android & Windows phones
- Set-top boxes, tablets & laptops

**WW Kinibji** Shipment Forecasts on Android Smartphones and Tablets (k Units)

- 2-digit growth > 40%
- Integration with tier-1 chip and device makers
- Potential integration with additional Operating Systems
- **150 M units deployed 2014**

<table>
<thead>
<tr>
<th>Year</th>
<th>&lt;i&gt;-base Shipments</th>
<th>Android Shipments</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013</td>
<td>103,833</td>
<td>879,910</td>
</tr>
<tr>
<td>2014</td>
<td>151,361</td>
<td>1,115,289</td>
</tr>
<tr>
<td>2015</td>
<td>225,168</td>
<td>1,285,817</td>
</tr>
<tr>
<td>2016</td>
<td>319,388</td>
<td>1,407,601</td>
</tr>
</tbody>
</table>

Expanding to Emerging Smart Connected Device Categories And Markets

*Gartner 2013, Trustonic Market Intelligence
*Take into account high-end devices only – Trustonic already has mid-end devices in scope
*Trustonic partnerships with Major MNOs will largely boost these figures
TEE usage on Android (Android 4.1 → ~5)

- SP
- TAM
- Client APP
- Dalvik / ART
- JNI
- Provisioning service
- TA
- Linux Kernel
- /dev/mobicore
- /dev/mobicore_user
- /dev/qsee /d/tzdbg/log
- Android NWd
- SWd
- TEE OS
Simple Trusted Application

A legacy TA. (A TA using standard GP TEE API does not fit on a slide)

```c
_TLAPI_ENTRY void tlMain(const addr_t buf, const uint32_t len)
{
    uint32_t secbuf;
    if ((NULL == buf) || (buflen != 4) || !tlApiIsNwdBufferValid(buf, 4))
        tlApiExit(EXIT_ERROR);

    for (;;)
    {
        tlApiWaitNotification(TLAPI_INFINITE_TIMEOUT);
        memcpy(&secbuf, buf, 4); secbuf |= 0xDEAD; memcpy(buf, &secbuf, 4);
        tlApiNotify();
    }
}
```

Open-source environments for testing GlobalPlatform TAs:

- **OpenTEE (D)**
- **OpTEE (E)**
TEE interaction (Kinibi) (Android 4.1→~4.4)
SEAndroid will change things to come in Android 6

- A problem specific to 3rd party use
- Provides for caller authentication
- Raises the abstraction level for the APIs (C → Java)
Use cases
1. Citizen Eld:s with TEEs

1) For TEEs, we need device **endorsement**

2) **Enrolment** different from smart cards

3) **Inter-service communication** not as well developed as in PC context
2. Better EMVCo tokenization security with TEEs

The tokenization is more or less orthogonal to modes of payment (offline, online, PinPresent..)

Using a TEE provides partial offline operation

NO Change here!

MWC’15 demonstrator
3. Private membership lookup (in cloud)
(alternative to homomorphic enc. Solutions)

Having direct memory access separates a TEE from a smart card or HSM. Other examples include DRM and trusted path.


E. Linaro project: https://github.com/OP-TEE/optee_os

People pay for better experiences

...security enables them