How to achieve streaming HD video Content & DRM Protection using TEE Security & DRM client Integration

ARM – Taiwan Multimedia Application Seminar

"Securing Smart/Connected Devices in an Open World: the Trusted Execution Environment (TEE)"

Karl J. Weaver 魏卡爾
Greater China Sales/Biz Dev Manager 大中華區手機事業發展部
手機號碼: 86-138-1078-0592 | 電子郵件: karl.weaver@gemalto.com
TRUSTED LOGIC MOBILITY
Trusted Logic / Trusted Logic Mobility

- Created in 1999 with support from INRIA
- Where open meets secure
- Creation of Trusted Labs in 2004
  - Consulting et security evaluation
- September 2009: acquired by Gemalto and became a subsidiary
- December 2011: creation of Trusted Logic Mobility
Trusted Logic Mobility

Product lines
- Security: Trusted Foundations™
- NFC: Trusted NFC™
- Digital Right Management (DRM): TrustedShow™

- Integrated at device level
- Leveraging platform hardware features
- Focused on open Operating Systems

Solutions for connected devices

Operations in France, USA, Greater China, South Korea and Japan

Worldwide Presence

Mass-deployed solutions
- Recognized security expertise
- References within the industry leaders (silicon vendors, device vendors/OEMs, service providers)
- Driving standardization

Unique Leading Position
Recent Achievements on Tablets and Smartphones

- Securing High-Definition Video-On-Demand on tablets and smartphones in line with Studio’s premium content distribution requirements
- Integrated with semiconductor vendors, device vendors and service providers
MOBILE SECURITY THREATS
Smart Devices Operate in a Hostile and Open Environment!

- DNS Poisoning
- Key loggers
- Viruses
- Bluetooth Attacks
- Botnets
- Man in the Middle
- Theft
- Pharming
- Spoofing
- Money Mules

- Social Engineering
- Man in the Browser
- Trojans
- Phishing
- Malicious Employees
- Worms
- Fake Applications
- Sniffing
Three out of 10 Android gadget owners are likely to encounter a Web-based threat on their device each year, with the number of Android apps infected with malware soaring from 80 apps in January to more than 400 apps through June 2011. - “Lookout Mobile Security in 2011 Mobile security Threat report”
One million Android devices have been malware infected in 2011 – Hacker Paradise revisited!

Currently 500,000 to 1 million Android handset users are affected by Malware on their Smart phone or tablet, 2.5 times more likely to be affected by malware since Q1, 2011. – “Lookout Mobile Security in 2011 Mobile security Threat report”

Attackers are deploying a variety of increasingly sophisticated techniques to take control of your phone’s, personal and payment data.
Apps stores present mobile security threat

**Online Applications Stores:**

- Causing rapid development, distribution and proliferation of malware applications, ideal transport mechanism for the delivery of malicious software to a high volumes of mobile devices.

- Users are also downloading apps from “unaffiliated third-party app stores, a catalyst for the launch of renegade applications affected by malware.

- Infected applications on Google, Android OS handsets/Tablets had to use a remote “kill switch” to remove Malware installed on Android devices.

- “Droid Dream” is a powerful zombie agent that can install any applications silently and execute code with root privileges at will; uses an exploit to gain root permissions, thereby giving it a substantial amount of control over an infected device.
2011 Malware Research Summary

- Threats targeting mobile devices increased more than 600 percent between 2010 and 2011. In December more new malicious apps that target mobile devices was found than in the entire 2004-2010 period.

- SMS-based Trojan attacks are most common, then "backdoor" attacks that can give attackers full access to users' devices especially if those devices are "rooted. Next up is mobile spyware, which steals users' personal data or information related to their devices.

- Most targeted OS for Malware in 2011, Android (65%); Java 2 Platform, Micro Edition (J2ME)(27%); Symbian (7%); Windows Mobile(1%).

- Mobile malware for Android can be broken down into two groups: threats designed to steal money or data(30%); and threats designed to take control of infected devices(almost 30%). (Source: Kaspersky Labs 2012)
TRUSTED EXECUTION ENVIRONMENT
Trusted Foundations™ - Leading TEE

- Proven Technology through Mass Deployment and growing references
- State-of-the-Art Security
- Rapid Time-to Market
- Multi Use Cases
  - Premium content protection
  - Mobile financial services
  - Corporate services
  - Device management
- Easy-to-use SDK
- Compliant with standards
Device Manufacturers & Silicon Vendors use Trusted Foundation - TEE

- **What is special about Trusted Foundations?**
  - It works on all mobile and connected devices and supports any security use case.
  - It is a proven solution, deployed by top-5 smartphone and tablet vendors and included on millions of shipped units.
  - It includes production versions for Android™, Symbian™ OS, Windows Mobile™, and Linux, and can be ported easily to other environments.
  - It delivers a high-performance combination of hardware and software security, supporting ARM® TrustZone® and ARM-based application processors and other processor architectures.
  - It communicates with a **Trusted Service Manager** (TSM) infrastructure for easy and secure service management and Over-The-Air (OTA) deployment of trusted applications.
  - It complies with GlobalPlatform, GSMA and Trusted Computing Group industry standards.
  - It includes a uniform, platform-independent, rich Software Development Kit (SDK) that can be used by any security-service provider.
What is a TEE?

Open to

malware

any user modification (e.g. “Jailbreaking”/“Rooting”)

Protection of

• Payment engine
• Bank authentication

Premium content management

• Device integrity and management
• Corporate service
• Sensitive user data

TEE Client API

TEE Secure Service API

Trusted Foundations™
(Trusted Execution Environment OS)

Crypto
Secure Storage
Trusted User Interface

Trusted Execution Environment

Main OS Environment

APPLICATIONS

Operating System

Application processor

NFC

Secure Elements

Trusted UI for pin code entry to make payment

Confidential Trusted Logic Mobility
Standardization:

- Reference for security of mobile platforms and TEE: OMTP (Open Mobile Terminal Platform) and GSMA
  

- Committee « GlobalPlatform Device »

- Participants
  - Mobile phone hardware platform manufacturers
  - Device manufacturers
  - Service providers

- http://www.globalplatform.org
TEE Added Value

Open Environment

- **APPLICATIONS**
- **TEE Internal API**
- **OS**

**APPLICATIONS**

- **Trusted Execution Environment**
- **Trusted Applications**
- **TEE Secure Service API**

**Trusted Foundations™** (GlobalPlatform Device)

**SECURE ACCESS TO HANDSET’S RESOURCES**

**Secure Element**

- **APPLETS**
- **JavaCard + GlobalPlatform Card**

**Application processor**

- The only environment capable of isolating and securing the screen and the touchpad of the mobile phone
  - Enable complete end-to-end secure services
- **Is executed in a secure and a high performance environment**
  - Rely on ARM TrustZone™ hardware security features
  - High memory capacities
  - Fast processing
- The only environment to have privileged access to the handset’s resources
  - User Interface, Cryptographic engine…
- **Pre-integrated within application processors**
- Complementary to Secure Elements
- Bulletproof against any software attacks
- Remote Administration

**Ex: PIN code entry, Video HD, VPN**

**Ex: PIN code entry, transaction validation**
Secure Mobile Wallets using Trusted Foundations with Trusted Execution Environment (TEE)

- **TEE Secure Mass Storage**
  - Storing sensitive data such as the wallet PIN code, coupons and transaction logs inside the TEE makes it impossible for an attacker to have access to them.

- **Trusted User Interface**
  - During PIN code entry, the screen and the touchpad of the smartphone are solely controlled by the TEE and completely isolated from the main OS, meaning that no malware can spy on the PIN code entry. Moreover, the screen isolation ensures that what you see is what you sign, since no malware can tamper the information displayed to the end user.

- **Trusted Application running within the TEE**
  - The TEE provides a secure environment that is isolated from the OS. It enables PIN verification within the TEE, in combination with Secure Mass Storage and the Trusted User Interface. In addition, the TEE offers high memory capacity, and can host additional sensitive applications such as NFC loyalty applications.
Trusted User Interface

The screen and the touchpad/keyboard of the mobile phone are solely controlled and isolated by the TEE.

Trusted Execution Environment

TEE Secure Service API

Trusted Logic Mobility

Trusted Foundations™

Mobile Applications Processor chip
Trusted User Interface – Key Advantages

Message to be signed

▪ Transaction summary displayed by Trusted Foundations™
▪ Main application environment cannot tamper with the message
▪ The user signs exactly what s/he is seeing

Validation Means

▪ Trusted PIN/password entry →
  Main application environment cannot have access to entered credential

Security Indicator

▪ Text or image
▪ “Sign-in Seal concept”
▪ Information securely configured by the user and securely controlled by Trusted Foundations™
▪ Proove to the user that the screen is TRUSTED by seeing this known information
SECURING HD CONTENT
TrustedShow™ - Multi-DRM Scheme

- Fast and easy integration
- State-of-the-art security
- Support of leading DRM schemes (PlayReady, Marlin, OMA DRM v2, HDCP, DTCP-IP,...)
- Field-proven solution
- Supports simultaneous multi-DRM schemes
TrustedShow™
Premium Video on Demand Service

- Content portal
- Multimedia Player
- TrustedShow™ Application Interface (API)
- TrustedShow™ Services
  - Trusted Foundations™
    - Secure storage
    - Secure clock
    - Secure cryptography
- License Server
- Encrypted content
- Licenses & keys

Confidential Trusted Logic Mobility
Presentation Title
23
Certified solution by VOD services providers such as Netflix
Solution for High Definition movies including 1080p
Enable transfer through HDMI connection
Fast and easy integration
State-of-the-art security
Deployed solution on Famous brand name tablet PCs now!
Supports simultaneous multi-DRM schemes (PlayReady, Marlin, OMA DRM v2...)
"Netflixiation" of America

Streaming to devices is the future

- A tablet's a blank slate without applications. Tablets value lies in the consumption and to a lesser extent the creation of content, but only marginally in communications.

More than 50% of users use the Tablet PC to watch movies and TV shows
LENOVO IDEALPAD K1 – With TEE security

- **First Android 3.1 “Honeycomb” tablets certified for streaming from Netflix**
  - As the first Honeycomb tablets certified for Netflix, Lenovo tablets can help turn every night into “movie night.” With HDMI output and Digital Rights Management (DRM) built directly into the IdeaPad and ThinkPad tablets, Netflix members can instantly watch movies and TV shows streaming from Netflix directly to a big screen TV.

- **Lenovo IdealPad K1’s Security + Streaming integration of Netflix VOD services provided from Trusted Logic Mobility**

Lenovo IdealPad K1 is powered by NVidia Tegra2 Mobile Applications Processor and embedded with mobile security + DRM client from Trusted Logic: **Trusted Foundations** (known as SecureOS from NVidia) and also is Integrated and Certified on Netflix (VOD) Video-on-Demand services Streaming and protection for HD premium video content by MS Playready Scheme and **Trusted Show**.
2012 Tablet Trends in China: Streaming VOD services, POS mobile payment usage

- Video sharing web sites (Tudou, Youku) drive content viewing and streaming to tablets, new business models can spring up, Hollywood is not waiting for Netflix to come to Asia, expect to partner with local studios, online aggregators for content distribution now.
- Video streaming to Smart tablets will be big in airplanes equipped with WiFi services, major airlines are lining up now globally and also in China to trial such services.
- Look for Smart Tablets to add Contactless Mobile NFC connectivity, to turn into wireless POS devices for peer-to-peer communications with Mobile NFC payment Smart phones and other NFC connected devices.
Tablets enhance online video viewing

182 million Americans watched online video content in September U.S. video audience tallied a total of 39.8 billion video views

- Using tablets results in higher level of engagement in online video viewing
- Viewer engagement was generally higher on mobile devices than on desktops

### Video Viewers use Smartphones to Watch content

**Total Hours Watched**
- Mobile: 47%, Tablet: 53%

**Total Video Plays**
- Mobile: 40%, Tablet: 60%

---

**U.S. mobile video viewers (in millions)**

<table>
<thead>
<tr>
<th>Quarter</th>
<th>Mobile Video Feature Phone</th>
<th>Mobile Video Smartphone</th>
<th>Mobile Video Viewer Penetration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q3 2010</td>
<td>7</td>
<td>10%</td>
<td>16</td>
</tr>
<tr>
<td>Q4 2010</td>
<td>7</td>
<td>11%</td>
<td>18</td>
</tr>
<tr>
<td>Q1 2011</td>
<td>7</td>
<td>12%</td>
<td>22</td>
</tr>
<tr>
<td>Q2 2011</td>
<td>6</td>
<td>13%</td>
<td>24</td>
</tr>
<tr>
<td>Q3 2011</td>
<td>5</td>
<td>14%</td>
<td>26</td>
</tr>
</tbody>
</table>

*Source: Nielsen*

---

### Facebook and Google properties dominate Android application usage across age groups

**Mobile Application Reach by Age**

- Nielsen Smartphone Analytics, Device Metering Data, September 2011

<table>
<thead>
<tr>
<th>Age Group</th>
<th>Android Market</th>
<th>Facebook</th>
<th>Google Search</th>
<th>Gmail</th>
<th>Google Maps</th>
<th>YouTube</th>
<th>Angry Birds</th>
<th>Pandora Radio</th>
<th>Quickoffice</th>
<th>Amazon Appstore</th>
<th>Adobe Reader</th>
<th>Adobe Flash Player</th>
<th>Windows Media Player</th>
<th>The Weather Channel</th>
<th>Volleyball</th>
<th>NBA.com</th>
<th>The Weather Channel</th>
<th>Yahoo Mail</th>
<th>Yahoo News</th>
</tr>
</thead>
<tbody>
<tr>
<td>18-24</td>
<td>99%</td>
<td>90%</td>
<td>77%</td>
<td>70%</td>
<td>70%</td>
<td>64%</td>
<td>30%</td>
<td>26%</td>
<td>23%</td>
<td>22%</td>
<td>22%</td>
<td>19%</td>
<td>19%</td>
<td>16%</td>
<td>14%</td>
<td>12%</td>
<td>12%</td>
<td>12%</td>
<td>12%</td>
</tr>
<tr>
<td>25-34</td>
<td>99%</td>
<td>90%</td>
<td>82%</td>
<td>79%</td>
<td>79%</td>
<td>59%</td>
<td>20%</td>
<td>23%</td>
<td>28%</td>
<td>28%</td>
<td>26%</td>
<td>20%</td>
<td>20%</td>
<td>16%</td>
<td>14%</td>
<td>12%</td>
<td>12%</td>
<td>12%</td>
<td>12%</td>
</tr>
<tr>
<td>35-44</td>
<td>99%</td>
<td>90%</td>
<td>82%</td>
<td>79%</td>
<td>79%</td>
<td>59%</td>
<td>20%</td>
<td>23%</td>
<td>28%</td>
<td>28%</td>
<td>26%</td>
<td>20%</td>
<td>20%</td>
<td>16%</td>
<td>14%</td>
<td>12%</td>
<td>12%</td>
<td>12%</td>
<td>12%</td>
</tr>
</tbody>
</table>

*Source: Nielsen*
China: New Mobile Apps Download Dragon

- Occupies second spot behind the U.S now
- Might overtake the U.S. by the end of 2013
- Will Become the largest Tablet PC user market
Hollywood Partnering to License Video Content in China

- Online Video sites buy expensive international content with payments for licensing fees from Hollywood Studios needed upfront, they then charge advertisers to place video commercials when movies, content are played.
- Major Hollywood studios are cooperating with China’s online video sites for paid viewing of their content gives them a way to make money in China. You Tube has signed a deal to allow PPTV to view its content.
- Youku's and Sohu's online video platforms have already cut deals with Disney and CBS Corporation, Youku will add 400~450 Warner Bros movies in 2012, In March 2012, Tudou and YouKu agreed to merge.
- Advertising revenue in the domestic online video market, which was virtually non-existent five years ago, is now estimated to be worth 1 billion yuan ($155 million)
- Baidu’s QiYi joint-venture with Providence Equity Partners has cut deals with Disney to show all seasons of Desperate Housewives, Cougar Town and Grey's Anatomy.
- China’s Web portals are starting to offer premium content and charging users for each viewing or for a monthly subscription or Pay-Per-View.
- Streaming video is a “grey area”, content censorship in China limits the number of foreign programming, which will benefit video-sharing/streaming web portals.
- Motion Picture Association consists of the six major film studios Disney, Paramount Pictures Corporation, Sony Pictures Entertainment, Twentieth Century Fox Film Corporation, Universal City Studios and Warner Bros.
Asia is the leader in Mobile Video Usage

- Asian countries rank amongst the top globally for media consumption with four of the top five nations for home TV and online video usage located in the region. Asian countries also took all five spots when it comes to mobile video usage.
- Smartphone popularity has surged ahead and more than half of consumers in Asia Pacific (52%) currently own or intend to buy a smartphone in the next 12 months.

Source: Nielsen Global How We Watch Report, Global Online Survey-2010
Tablet PC Users Pay for Video Content

- Most U.S. tablet owners have paid for downloaded music (62%) and books (58%) for usage on their device. Approximately half have paid for movies (51%).
  - News is the top content category among the European tablet owners surveyed: 44 percent of tablet owners in Italy, 19 percent of tablet owners in the UK, and 15 percent of tablet owners in Germany say they have paid for tablet news content.
  - Among the European countries, Italians are the most willing to pay for media content on their tablet.
Traditional Broadcast TV

By 2020, 75% of channels will be transmitted by Internet traffic, and video will be about 90% of that traffic.

Internet Connected Video — Are you Streaming?

OTT players & video Web portals with video on demand services have mobile streaming plans.

Trusted Logic Mobility’s Trusted Show DRM CLIENT + Security solutions Integrate DRM Schemes on Smartphones/Tablet PCS to Video-on-Demand (VOD) Services, We are certified on Netflix for NVidia (Tegra3) and Texas Instruments (OMAP4) Mobile Applications processor chips.
Smart/Connected TVs – (Netflix) VOD is important

- 38% of all US households have at least one TV set connected to the Internet via a video game system, a blue ray player, an Apple TV or Roku set-top box and/or the TV set itself.
- Overall, 16% of all adults use Netflix’s Watch Instantly feature weekly — compared to 12% last year, and 4% two years ago.
- 79% of Netflix Watch Instantly customers use it to watch movies and television shows on a TV set, and 59% of this group access Netflix via a video game system.
- 50% of Netflix subscribers are satisfied with the service, and 11% are likely to stop subscribing to Netflix in the next six months.
- 7% of Netflix subscribers are likely to switch from their multi-channel video provider in the next six months — compared to 12% of non-Netflix subscribers.
- 13% of Netflix subscribers would consider reducing spending on their multi-channel video service because of Netflix — compared to 21% last year.
- 16% of all adults watch full length TV shows online at least weekly — compared to 12% last year, and 10% three years ago.
- Among all mobile phone owners, 19% watch video on their phones weekly — compared to 15% last year, and 6% three years ago.
- 9% of all adults watch video on an iPad/tablet computer weekly — compared to 2% last year.
- Overall, 1.6% of households in the sample paid to subscribe to a multi-channel video service in the past year and do not currently subscribe.

Source: Leichtman Research Group