Royal Holloway University of London

Information Security Group

Using mobile devices in a secure environment

Chris Mitchell
Royal Holloway, University of London
www.isg.rhul.ac.uk/~cjm

1

Royal Holloway University of London

Information Security Group

Preliminary remarks

- Assumption underlying this talk is that a platform exists providing TPM and TSS functions (as in TCG specifications).
- This may not be such a problematic assumption for a mobile device.
- 'Locked down' devices may be closer to the norm, e.g. for mobile phones, where a high degree of reliability is expected/required.
- As a result we can investigate interactions between specified functionality (of a trusted platform) and needs of range of use cases.

2

Agenda

1. Background
2. Mobile device use cases
3. Public sector use cases
4. Trusted application download
5. Next steps …

Trusted computing research at RHUL

- RHUL research on trusted computing (TC) grew out of ongoing research interest in mobile security.
- Recent research on TC applications includes:
  - Internet single sign-on support;
  - Trusted application download for mobile devices;
  - Peer-to-peer security (establishment of stable identities);
  - Distributed PKI support;
  - Personal Information management.

Ongoing research

- Some of this work documented in the recent book:
  C. Mitchell (ed.), *Trusted Computing*, IEE Press (UK), 2005.
- Current work includes participation in two funded projects:
  - *Open Trusted Computing* (6th Framework IP involving over 20 partners; 2005-09);
  - *Trust Establishment in Mobile Distributed Computing Platforms* (UK EPSRC funded project, examining support for grid security on TC-enabled mobile devices; 2006-09).

OpenTC – trusted mobile devices

- Main role of RHUL in OpenTC is to investigate TC applications on mobile platforms.
- Will develop series of mobile use cases, analyse them to deduce security requirements, and will consider how best to meet requirements using TC.
- Help define minimal set of TC functionality for mobile environment, and also analyse 'how secure' mobile TC needs to be.
- Results will be fed into the TCG MPWG.

Royal Holloway University of London

Information Security Group

Trust Establishment in Mobile Distributed Computing Platforms

- Main goal is to provide mechanisms and protocols to establish trust in a mobile grid computing environment.
- Will investigate how TC technology can be used to provide assurance in integrity of remote platforms.
- Consider general distributed trust issues and possible solutions.

Royal Holloway University of London

Information Security Group

Agenda

1. Background
2. Mobile device use cases
3. Public sector use cases
4. Trusted application download
5. Next steps …

TCG MPWG

- The Mobile Phone Working Group (MPWG) has published a list of use cases for TC in a mobile environment.
- We briefly categorise these (categorisation is not mutually exclusive).

The 'obvious' use cases

- The following trusted functionality has already been implemented in mobile devices using proprietary trusted functionality:
  - IMEI protection;
  - SIMLock;
  - Robust implementation of OMA DRM v2.0.
- These are necessary but not 'killer' applications for TC technology.

Platform security use cases

- TC can be used to help provide guarantees regarding state of mobile platform (analogous to use for PCs):
  - Trusted boot (platform integrity);
  - Device authentication (e.g. TC support for SSL);
  - Secure storage (a TC-supported function of use in many applications).

Distributed application security

- A number of TC applications can be categorised as supporting distributed applications – these include:
  - Secure software download;
  - Robust DRM implementation;
  - Mobile payment.

User security

- Finally, a number of TC applications provide functionality to the end user:
  - Secure storage and secure processing of data;
  - Proving OS/application integrity to end user;
  - Authentication of remote devices;
  - User data protection (user privacy).

Agenda

1. Background
2. Mobile device use cases
3. Public sector use cases
4. Trusted application download
5. Next steps …

Key applications

- Of the range of applications of TC in a mobile environment, the following seem particularly appropriate to the public sector:
  - Platform security (trusted boot, device authentication, secure storage, …);
  - Secure distributed applications.

Distributed application management

- Range of ways in which TC can help with distributed computing:
  - secure download, installation and use of a sensitive application (the main focus of this talk);
  - secure inter-device authentication;
  - secure attestation regarding components of a distributed computing environment (e.g. for Grid), enabling trust regarding handling of sensitive data.

Agenda

1. Background
2. Mobile device use cases
3. Public sector use cases
4. Trusted application download
5. Next steps …

Existing work

- Whilst we have not considered the general problem of secure application download, we have looked at one particular instance of the problem.
- The context is the secure download of applications for accessing broadcast content.
- Work described is by Eimear Gallery and Allan Tomlinson.
- Seems likely that similar analyses will apply in the general case.

Protection of Broadcast Content

- Broadcast content is currently protected by Conditional Access (CA) systems that:
  - Scramble the video signal;
  - Manage keys and viewing rights using proprietary security mechanisms.
- DVB standards provide an interface to proprietary CA systems.

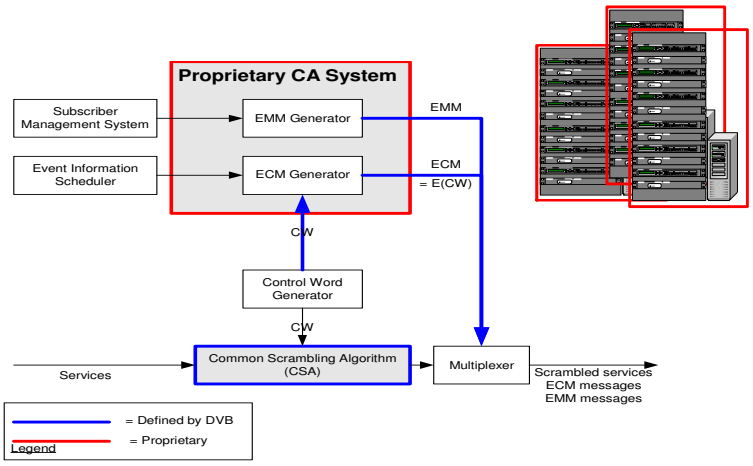
DVB Standards

- Common Scrambling Algorithm (ETSI ETR 289):
  - Used to scramble and descramble video;
  - Details available to all manufacturers.
- Simulcrypt (ETSI TS 103 197):
  - Multiple CA systems in parallel at transmitter;
  - Common key to scramble services;
  - Key encryption remains proprietary.
- Common Interface (CENELEC 50221)
  - Common Interface Modules – PC Cards;
  - Changes proprietary CA at receiver.

Royal Holloway University of London

Information Security Group

Simulcrypt

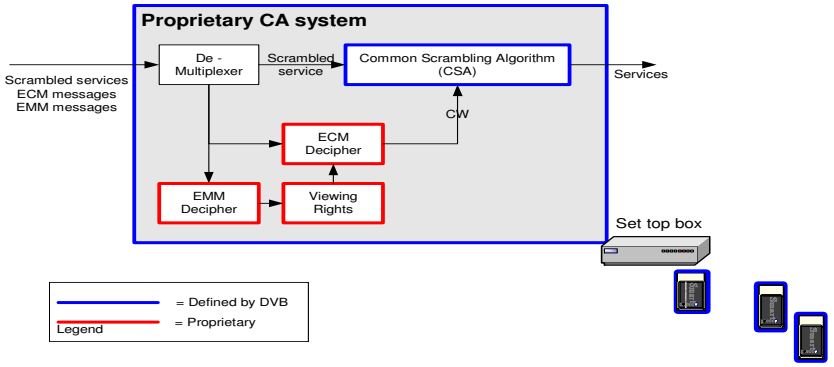


21

Royal Holloway University of London

Information Security Group

Common Interface



22

Problems in a mobile setting

- DVB Standards:
  - Provide a flexible interface to proprietary systems;
  - There are many proprietary systems.

DVB CA systems

CA System	Vendor
Viaccess	Viaccess SA
NagraVision	Kudelski
Videoguard	NDS
Mediguard	Canal+
Mcrypt	Irdeto
PiSys	Irdeto
CryptoWorks	Philips
BetaCrypt	BetaResearch
Conax	Telenor

Limitations of current protection mechanisms

- New business model:
  - Delivery of broadcast services to *mobile* receivers, with services available from many broadcasters.
- Current protection mechanisms:
  - Designed for relatively *static* receivers and services available from a small number of broadcasters.
- Common Interface:
  - Consumers require multiple PC-Card modules – cost, inconvenience, unsuitable for mobile devices.
- Simulcrypt:
  - Broadcasters install and maintain multiple CA systems – cost, maintenance issues.
- Current mechanisms not designed for mobile receivers.

Potential Solution

- Download proprietary applications to mobile devices on demand
- Problem:
  - Applications, and providers, are security sensitive
  - Lack of trust in the mobile host:
    - Piracy: protection of proprietary algorithms, keys
  - Host needs to demonstrate that it can be trusted:
    - Application needs protection – not the host
- Trusted Computing provides the mechanisms to demonstrate trust.

Requirements

- Demonstration of trustworthiness:
  - Integrity *challenge* mechanism;
  - Integrity *verification* mechanism.
- Application protection:
  - Secure *delivery* mechanism;
  - Secure *execution* environment.

Application of TCG technology

- Demonstration of trustworthiness:
  - Integrity metrics:
    - Authenticated boot – CRTM
    - Configuration measurements – PCR
    - Attestation of current platform configuration – TPM
- Application protection:
  - Secure *delivery* mechanism:
    - Key generation and exchange.
  - Secure *execution* environment:
    - Sealed storage.
    - Isolated domains.

Trusted download

- Demonstration of trustworthiness:
  - Authenticated boot;
  - Attestation of platform configuration (response to integrity challenge);
  - It is the challenger's responsibility to verify the response and determine whether to trust the platform or not;
  - Host must not change configuration.
- Application protection:
  - Key generation;
  - Keys in sealed storage to ensure consistent configuration;
  - Message Authentication Codes and Encryption;
  - Isolation of applications.

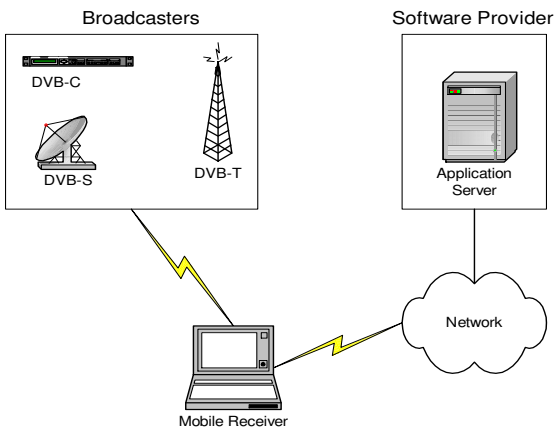
Required security services

1. Confidentiality of application in transit.
2. Integrity of application in transit.
3. Entity authentication:
   - Host;
   - Application provider.
4. Origin authentication of application.
5. Freshness of messages.
6. Confidentiality and integrity of application while stored on the device (AC mechanisms to protected the application on the device).
7. Confidentiality and integrity of application while executing on the device.

Corresponding security mechanisms

1. Symmetric encryption.
2. MACing of the application.
3. Entity authentication protocol runs as described in ISO/IEC 9798-3 (Host and application provider)
   - Attestation (Host) as described within TCG TPM specification set.
4. Digital signature of the application provider on the secret keys used in providing 1. and 2.
5. Nonces / timestamps.
6. Protected/secure storage, as described in TCG TPM v1.2 specification set.
7. Memory isolation techniques, e.g. as described by Microsoft with respect to NGSCB.

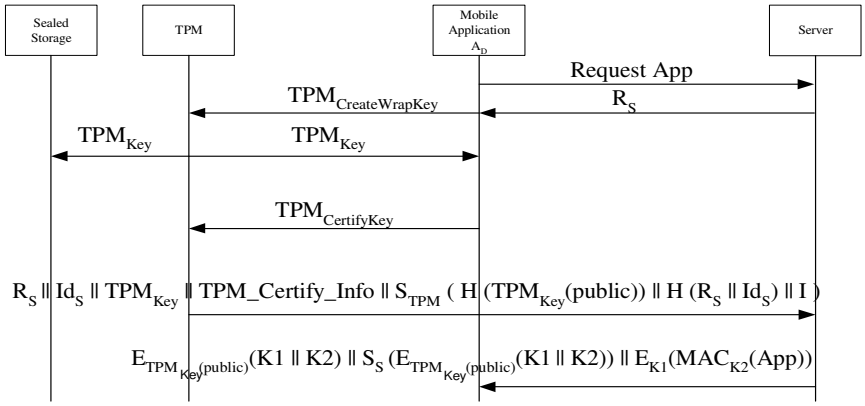
Model



Royal Holloway University of London

Information Security Group

Protocol 1

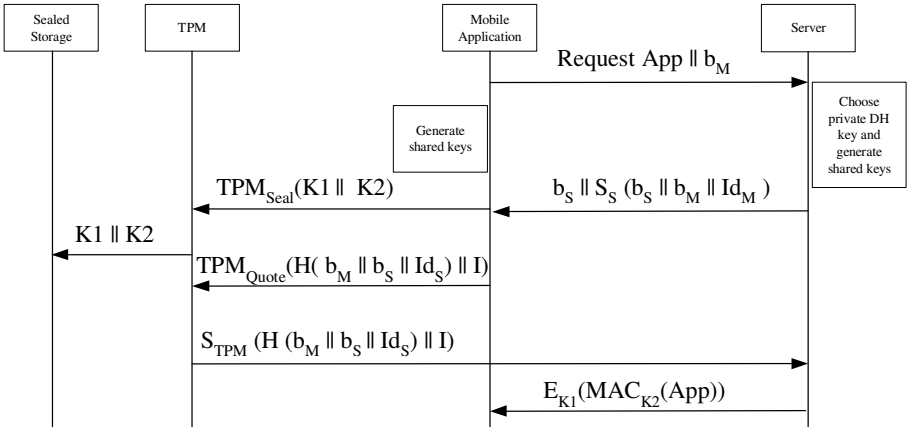


33

Royal Holloway University of London

Information Security Group

Protocol 2



34

Download protocol: Analysis

- RHUL-MA-2005-11 available at: www.rhul.ac.uk/mathematics/techreports
- Informal analysis
  - Completed against the seven security services required of the protocol.
- Formal analysis
  - Completed by Rob Delicata, University of Surrey.
- The scope of the informal analysis is wider than that of the formal analysis. The informal analysis also presents reasons for the protocol's correctness – as opposed to the pleasing, but rather underwhelming, Boolean response from a formal analysis.

Comparison of protocols

- The second protocol:
  - More applicable to resource limited devices since less reliant on asymmetric encryption.

Summary

- Using TC technology:
  - Host is able to demonstrate it is running a secure execution environment;
  - Application provider has confidence that software and data will not be tampered;
  - User has access to a wider range of applications.

Agenda

1. Background
2. Mobile device use cases
3. Public sector use cases
4. Trusted application download
5. Next steps …

Use cases

- The success of our work in OpenTC depends on identifying the most important use cases.
- We are already consulting mobile network operators.
- We would welcome input on what governments believe to be the most important mobile use cases.

Contacts

- For more information on any aspects of this talk, please contact me at:

Chris Mitchell
Information Security Group
Royal Holloway
University of London
Egham
Surrey TW20 0EX
UK
c.mitchell@rhul.ac.uk
http://www.isg.rhul.ac.uk/~cjm
+44 1784 443423 (fax: +44 1784 430766)