Trusted computing and mobile systems

Chris Mitchell
Information Security Group
Royal Holloway
http://www.isg.rhul.ac.uk/~cjm

Contents

- What is trusted computing?
- The need for trusted computing
- A multiplicity of specifications …
- Application I: Single Sign-On
- Application II: DRM for broadcast
- Application III: Privacy of Personal Information
- Application IV: Co-operation enforcement

Computer security

- Computer security has a long history, and many secure computer systems have been produced and sold.
- Almost all of them depend on the assumption that the computer hardware will be physically secure, and managed by trusted personnel.
- Physical access to the machine will typically allow software integrity to be compromised

Multi-user systems

- Many systems (e.g. Unix, Windows 2K/XP) designed to allow users to protect their data and resources against other users of same machine.
- All based on access control systems.
- Again typically dependent on physical security of machine.

Computer security – external view

- If a (secure) computer digitally signs a message, then trust in messages depends on:
  - trust in computer software, and
  - trust in physical security of hardware (and in correct application of security procedures by administrators).
- Makes sense in conventional ‘computer centre’.

PC security

- Perhaps an inherent contradiction!
- PCs are not stored in a physically secure environment.
- Even though modern versions of Windows (and Linux) have multi-user security features, users and programs often run as administrator.
- There are many ways that the operating system integrity can be damaged.

Contents

- What is trusted computing?
- The need for trusted computing
- A multiplicity of specifications …
- Application I: Single Sign-On
- Application II: DRM for broadcast
- Application III: Privacy of Personal Information
- Application IV: Co-operation enforcement

Trusting a PC

- Today, neither the user of a PC nor a communicating party can trust very much at all about a PC.
- This is despite major efforts to improve security of Windows.
- Anyone with access to the PC hardware can modify Windows (e.g. by removing hard disk and changing files).

Trusting a PC – more bad news …

- Even if the user looks after the physical security of their PC, there are many other threats to system integrity.
- Modern operating systems and applications are highly complex and it is almost impossible to remove all vulnerabilities.
- Users can easily accidentally run malicious software which can damage system integrity.

Need for trust I

- User may want to trust the integrity of their PC.
- For example, the PC may be used for:
  - managing a bank account,
  - performing e-commerce transactions,
  - managing personal information,
  - …

all of which require *user* trust in the PC.

Need for trust II

- Third party may want to trust integrity of PC.
- This could be for a variety of reasons, e.g.:
  - 3rd party is a bank: PC being used for e-commerce,
  - 3rd party is a content provider: PC performing DRM,
  - PC performing other security functions (e.g. authentication, key management) on behalf of 3rd party,

all of which require *third party* trust in the PC.

Role of Trusted Computing

- Enables trust in integrity of PC based on combination of software and hardware.
- Third parties can measure PC integrity.
- Trusted Computing does not just apply to conventional PCs: equally relevant to PDAs, mobile phones, broadcast receivers, …

On uses of trusted computing

- It seems plausible that such technology – some proprietary, some standards conformant – will be included in most future computing devices (PDAs, notebooks, phones, …)
- Many applications for such technology have been proposed, most controversially for DRM.
- In this talk we look at a range of possible applications relevant in a mobile environment.

Contents

- What is trusted computing?
- The need for trusted computing
- A multiplicity of specifications …
- Application I: Single Sign-On
- Application II: DRM for broadcast
- Application III: Privacy of Personal Information
- Application IV: Co-operation enforcement

TCG

- Trusted Computing in the sense of this talk dates back to late 1990s.
- Consortium of major manufacturers started TCPA (Trusted Computing Platform Alliance).
- This has morphed into TCG, the Trusted Computing Group.

Current position

- May 2003: Operational technical working groups for:
  - Future TPM, trusted platform module
  - PC specific implementation specifications
  - New TSS, TCG software stack specifications as well as for
  - The development of common criteria protection profiles.
- Followed closely by formation of working groups for:
  - Server, PDA, mobile phone platform specific implementation specifications.

TCG specifications

- TCG TPM main specification (general platform specification) version 1.2:
  - Design principles.
  - Structures of the TPM.
  - TPM commands.

↰ (superseded TCG main specification version 1.1).

- TCG software stack specification version 1.1.
- TCG software stack specification header file.
- TCG PC specific implementation specification version 1.1.

Trusted Platforms: TCG definition

- A trusted platform:
  - A computing platform that has a trusted component;
  - Usually in the form of built-in hardware which is used to create a foundation of trust for software processes.

Trusted Platform functionality (1)

- Trusted platform technologies aim to provide:
  - Confidentiality and integrity of application code and data;
  - Confidentiality and integrity of application code and data during storage;
  - Integrity of the operating system and underlying hardware so that the above properties can be satisfied.

Trusted Platform functionality (2)

- Platform authentication to external entities.
- Trusted path to user ensuring confidentiality of user input.
- Secure channels to devices and between applications to ensure confidentiality, integrity, and authenticity of inter-application communication.
- Ensure reliability by restricting size of trusted critical components:
  - Common estimate: 1 security-related bug per 1000 lines of code.

NGSCB

- *Next Generation Secure Computing Base* (NGSCB) is Microsoft’s take on Trusted Computing.
- Version of Windows that uses trusted hardware (e.g. hardware conformant to TCG specifications) to build a trusted kernel.
- Allows trusted applications to run under control of a trusted operating system, in parallel to ‘regular’ Windows applications.

LaGrande

- Set of enhancements to Intel chip sets incorporating everything needed to build a Trusted Computing Platform.
- Also provides a potential platform for NGSCB-enabled PCs.

Contents

- What is trusted computing?
- The need for trusted computing
- A multiplicity of specifications …
- Application I: Single Sign-On
- Application II: DRM for broadcast
- Application III: Privacy of Personal Information
- Application IV: Co-operation enforcement

Acknowledgement

- This is based on work done by Andreas Pashalidis.

Background

- Desire for an Internet single sign-on solution.
- That is, instead of a user authenticating him/herself to multiple service providers (SPs), the user authenticates him/herself to an Identity Provider who then provides assurances (*assertions*) regarding the user identity to SPs.
- This requirement becomes even more important in a ubiquitous computing/mobile environment, where a user will not wish to authenticate him/herself to every device/service.

Microsoft Passport

- (Originally) a proprietary SSO solution, which also (originally) involved the possibility of managing other personal data, all stored on a server somewhere ...
- Problems with guardians of end-user privacy, including European Commission.
- MS appears to be moving towards a Web Services based solution.

Liberty Alliance

- Consortium set up to provide an open system (protocol suite) to support SSO.
- Provides variety of alternative means of transferring assertions from IP to SP.
- E.g. using SOAP, web redirection.
- Possible problems, as with any scheme using web redirection, if man-in-the-middle attacks.

WS Federation

- Part of Web Services Security.
- Covers federation of identifiers, and also allowed ‘brokering’ of identity/authentication services.
- Would appear that it can be used as the basis of an SSO scheme.

TC-based single sign-on

- SSO typically requires an external TTP to act as the Identity Provider (IP).
- Why not use TC component to act as the IP, which authenticates the user once, and then asserts that user is present to other devices?
- Why should other devices believe assertions – well, by checking out the TC component, and knowing that the program making the assertion is not compromised.

Contents

- What is trusted computing?
- The need for trusted computing
- A multiplicity of specifications …
- Application I: Single Sign-On
- Application II: DRM for broadcast
- Application III: Privacy of Personal Information
- Application IV: Co-operation enforcement

Acknowledgement

- This is based on work done by Eimear Gallery and Allan Tomlinson within the Mobile VCE Core III programme.

Protection of Broadcast Content

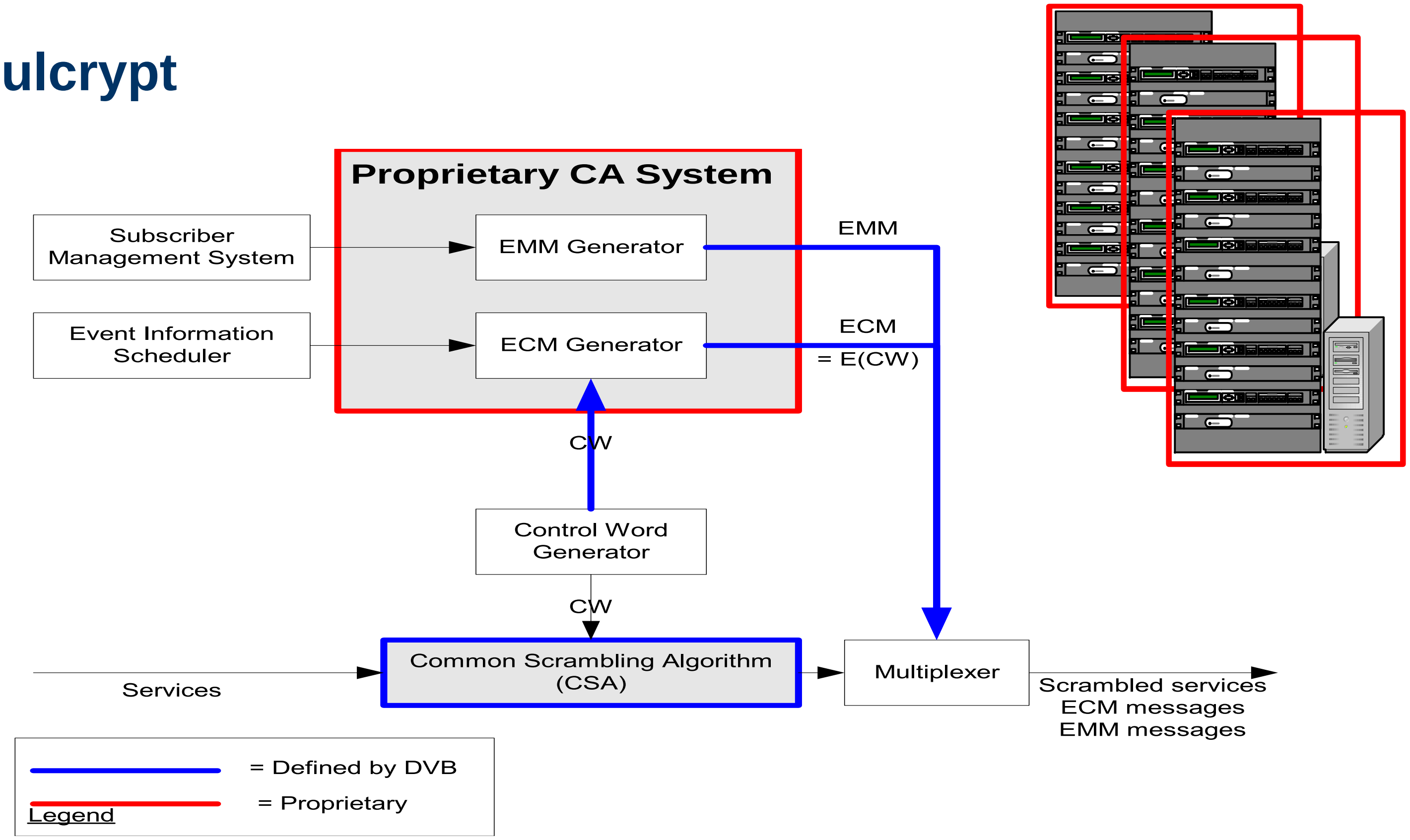
- Broadcast content is currently protected by
  - Conditional Access (CA) systems that:
    - Scramble video
    - Manage keys and viewing rights, using proprietary security mechanisms
  - DVB standards
    - Provide an interface to proprietary systems

Protection of Broadcast Content

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

Protection of Broadcast Content

Simulcrypt



Proprietary CA System

Subscriber Management System

Event Information Scheduler

EMM Generator

ECM Generator

EMM

ECM = E(CW)

CW

Control Word Generator

CW

Services

Common Scrambling Algorithm (CSA)

Multiplexer

Scrambled services
ECM messages
EMM messages

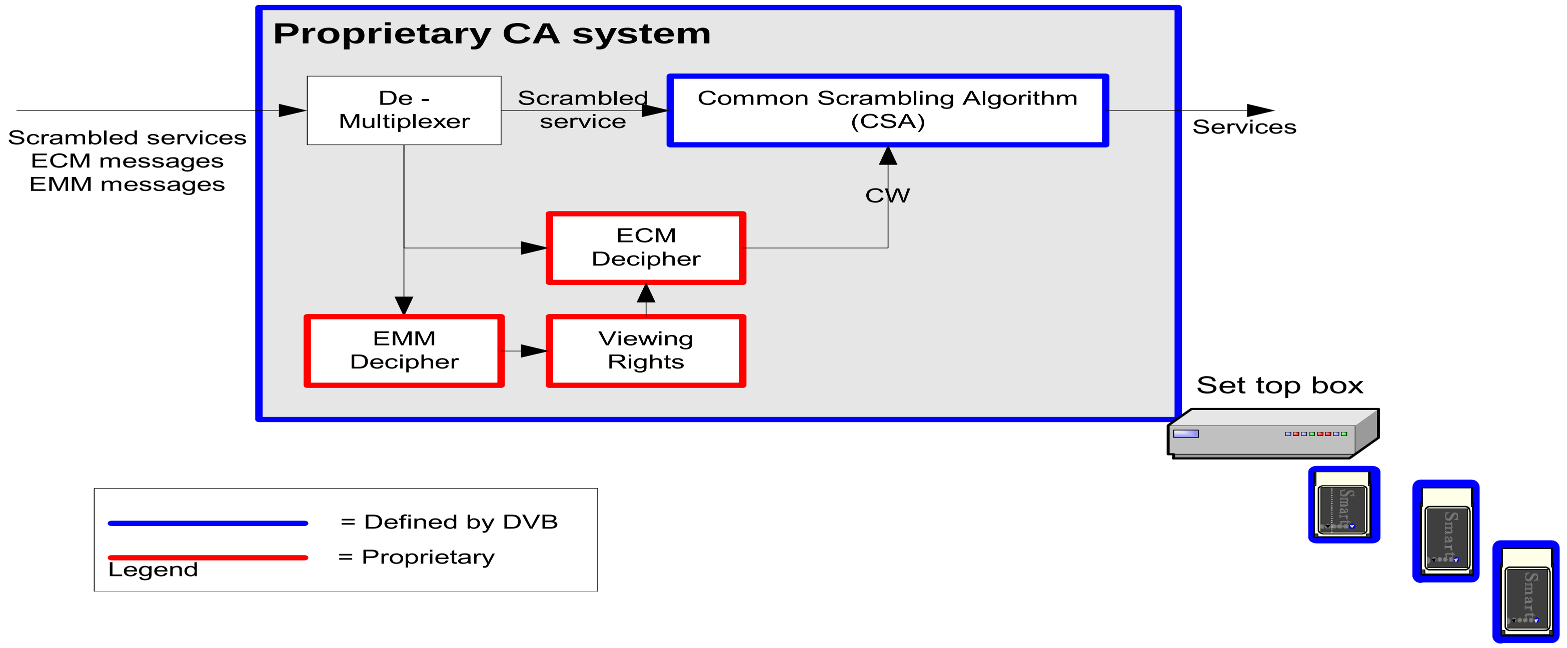
Legend

🟦 = Defined by DVB

🟥 = Proprietary

Protection of Broadcast Content

Common Interface



Proprietary CA system

Scrambled services
ECM messages
EMM messages

De - Multiplexer

Scrambled service

Common Scrambling Algorithm (CSA)

Services

CW

ECM Decipher

EMM Decipher

Viewing Rights

Set top box

Legend

= Defined by DVB

= Proprietary

Protection of Broadcast Content

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

Protection of Broadcast Content

- DVB Compliant Conditional Access (CA) systems

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

Limits of current protection mechanisms

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

Requirements

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

Application of TCG Trusted Platform technology

- Demonstration of trustworthiness
  - Integrity metrics
    - Authenticated boot – CRTM (Core Root of Trust for Measurement);
    - Configuration measurements – PCR (Platform Configuration Register);
    - Attestation – TPM (Trusted Platform Module)
      - current platform configuration
- Application protection
  - Secure *delivery* mechanism
    - Key generation and exchange
  - Secure *execution* environment
    - Sealed storage

Other security and trusted platform technology

- Demonstration of trustworthiness
  - Integrity *verification* mechanism
    - Certificates and Certification Authorities
- Application protection
  - Secure *delivery* mechanism
    - Encryption, Message Authentication Codes
  - Secure *execution* environment
    - Physical separation of trusted and untrusted processes
      - Curtained memory – NGSCB, LaGrande
      - Compartmentalised OS – NGSCB Nexus

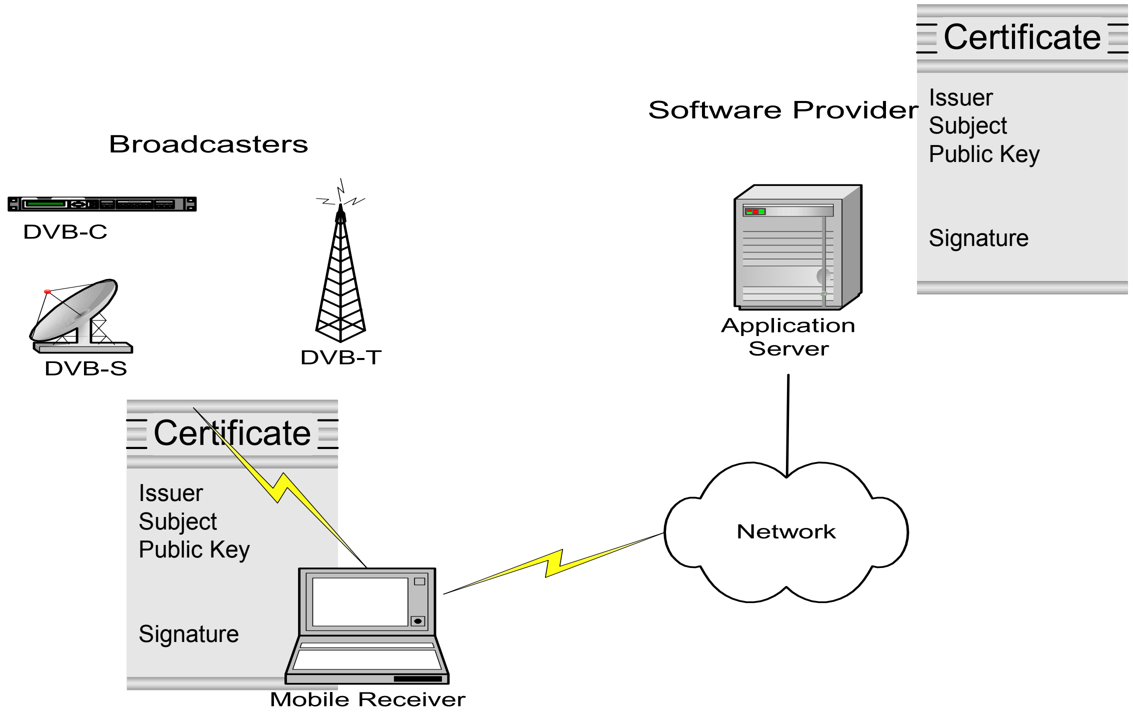
General Approach to trusted download

- 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 exchange;
  - Keys in sealed storage to ensure consistent configuration;
  - Message Authentication Codes and Encryption;
  - Isolation of applications.

Protocol requirements

- The protocol must protect against:
  - Replay
    - A malicious host could replay attestation information from before the system was compromised
  - Tampering
    - A malicious host could tamper with the integrity metrics before transmission to the challenger
  - Masquerading
    - A malicious host could replace the original integrity metrics with data from another system
  - Revealing the application
    - A malicious host could reveal the application and keys

Model



Software Provider

Certificate

Issuer
Subject
Public Key

Signature

Broadcasters

DVB-C

DVB-S

DVB-T

Application Server

Certificate

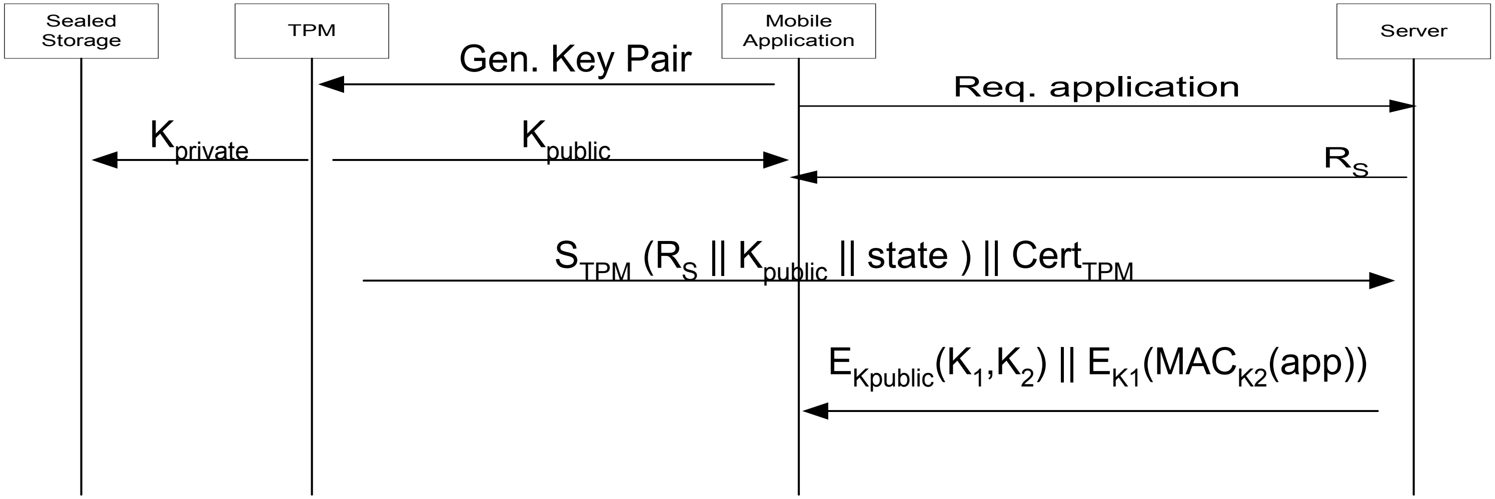
Issuer
Subject
Public Key

Signature

Network

Mobile Receiver

Protocol 1



Sealed Storage

TPM

Mobile Application

Server

Gen. Key Pair

Req. application

$K_{private}$

K_{public}

R_S

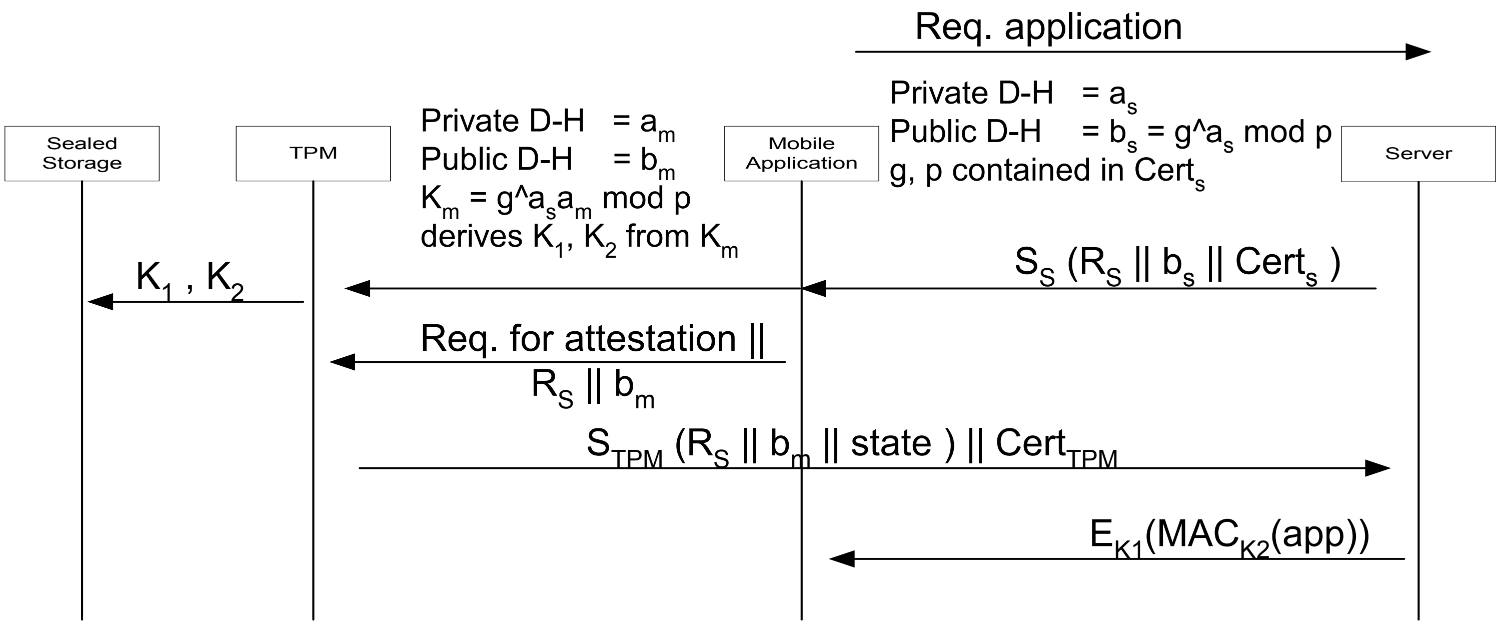
$S_{TPM}\ (R_S \,||\, K_{public} \,||\, \text{state}\ ) \,||\, Cert_{TPM}$

$E_{Kpublic}(K_1,K_2) \,||\, E_{K1}(MAC_{K2}(app))$

Protocol provisions

- The protocol protects against
  - Replay
    - The nonce, R_S, protects against replay
  - Tampering
    - The TPM signature protects the integrity metrics
  - Masquerading
    - The Certificate of the TPM protects against masquerading
  - Revealing the application
    - K_1, K_2, protect the application during transmission
    - Sealed storage and isolation protect during execution

Protocol 2



Sealed Storage

TPM

Mobile Application

Server

Req. application

Private D-H = a_s
Public D-H = b_s = g^a_s mod p
g, p contained in $Cert_s$

Private D-H = a_m
Public D-H = b_m
K_m = g^a_sa_m mod p
derives K_1, K_2 from K_m

S_S (R_S || b_s || $Cert_s$)

K_1 , K_2

Req. for attestation ||
R_S || b_m

S_{TPM} (R_S || b_m || state) || $Cert_{TPM}$

$E_{K1}(MAC_{K2}(app))$

Summary

- Using Trusted Platform 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

Contents

- What is trusted computing?
- The need for trusted computing
- A multiplicity of specifications …
- Application I: Single Sign-On
- Application II: DRM for broadcast
- Application III: Privacy of Personal Information
- Application IV: Co-operation enforcement

TC-based personal information control

- One partial solution to the problem of controlling personal information (PI) e.g. location information, is by attaching policy information.
- However, such a system needs enforcement.
- Of course, part of that is regulation.
- However, TC can help – that is, if the intended destination for PI is a TC-platform, the holder of PI can potentially verify the software to which it may be passing PI (indeed, it might be obliged to!).
- Currently being studied by Anand Gajparia.

Contents

- What is trusted computing?
- The need for trusted computing
- A multiplicity of specifications …
- Application I: Single Sign-On
- Application II: DRM for broadcast
- Application III: Privacy of Personal Information
- Application IV: Co-operation enforcement

TC-based co-operation enforcement

- The support of MANETs typically requires co-operation by the nodes, e.g. to support routing.
- As commonly discussed, malicious users may replace their network software with a ‘selfish’ version, e.g. to save battery power.
- TC could help guarantee that a network element is running the ‘correct’ software, and hence will not behave selfishly.
- (Of course, this requires the communications hardware to be part of the TC subsystem.)