



www.isg.rhul.ac.uk



www.mobilevce.com

Protecting user privacy using trusted computing

Anand Gajparia

Information Security Group

Royal Holloway

University of London

a.gajparia@rhul.ac.uk

Protecting User Privacy using Trusted Computing

Anand Gajparia

Information Security Group
Royal Holloway
University of London
a.gajparia@rhul.ac.uk

Anand Gajparia is being supported by sponsorship from Toshiba Telecommunications Research Laboratory, UK **TOSHIBA**

Contents

- Introduction
- Privacy
- Constraints
- Trusted Computing
- TCG enabling Privacy
- NGSCB enabling Privacy
- Conclusion

- Introduction
- Privacy
- Constraints
- Trusted Computing
- TCG enabling Privacy
- NGSCB enabling Privacy
- Conclusion

Introduction

- Privacy of personal information is a major issue
- Particular concern is how users can control private data after it has entered the electronic world
- We show how Trusted Platforms (TPs) conforming to the Trusted Computing Groups (TCGs) specifications can be used to help enforce user control

- Introduction
- Privacy
- Constraints
- Trusted Computing
- TCG enabling Privacy
- NGSCB enabling Privacy
- Conclusion

Privacy

- Types of personal information
 - Location Information (LI)
 - Medical records
 - Bank details
 - Phone number
 - Address
- Main focus of this talk is on LI, although similar mechanisms could be used to protect other personal information

Privacy

- Users want personal information to remain private after it has been distributed
 - For example in application forms
- Users also want to retain some control of their personal information even after it has been distributed

7

Privacy

- Range of mechanisms have been proposed which allow users to remain anonymous when using a service
 - This may be impractical for some applications
 - Vendors may require information for billing purposes
 - Contact details may be necessary to provide services at a later date
- We propose a mechanism which allows a user to retain a certain degree of control of personal information after it has been distributed

8

Privacy model

- Private data
 - This is data containing personal information regarding a subject
- Privacy subject
 - the entity regarding which private data is being gathered, managed and used. This entity is most commonly a human user
- Service provider
 - This entity is willing to provide some service requiring personal information from a privacy subject

9

- Introduction
- Privacy
- **Constraints**
- Trusted Computing
- TCG enabling Privacy
- NGSCB enabling Privacy
- Conclusion

10

Constraints

- Simple statements, bound to personal data, which may be used to help control its use, storage and distribution

11

Constraint types

- Use
 - Purpose for which private data may be used
 - Example: Medical use only; Location based services only.
- Validity
 - Length of time private data may be stored
- Redistribution
 - Constraints for further distribution

12

Constraint management

- Envisage that there will exist trusted software which will manage personal data in a manner trusted by the privacy subject
- Aim is to discuss how a user can establish whether or not this software is executing on a target platform, and further ensure that this software is executing when the private data is used in the future

13

- Introduction
- Privacy
- Constraints
- **Trusted Computing**
- TCG enabling Privacy
- NGSCB enabling Privacy
- Conclusion

14

TCG and Trusted Computing

- Discussed in Department of Defense, Trusted Computer System Evaluation Criteria (Orange Book)
 - discusses a trusted computing base as a part of a computer protected by secure perimeter containing the parts of the system responsible for security protection of the system
- Trusted Computing Group specification could be viewed as an implementation of such a specification

15

TCG and Trusted Computing

- We will show one way in which the use of mechanisms provided by the Trusted Computing Group specification can enhance the privacy of private data

16

- Introduction
- Privacy
- Constraints
- Trusted Computing
- TCG enabling Privacy
- NGSCB enabling Privacy
- Conclusion

TCG enabling privacy

- Look at how described mechanisms may enable privacy
 - Consider a privacy subject who wishes to decide whether or not to divulge private data to a service provider with a Trusted Platform
- Using the mechanisms described by the TCG, a user can check to see if trusted management software was running on the platform when the platform booted and also specify that this personal information is only used when the platform is in a trusted state

TCG enabling privacy

- Privacy subject first establishes if trusted software for management of their private data is on a service provider's Trusted Platform
- If trusted management software is found on the platform, the privacy subject then decides on limitations for future use of this private data

19

TCG and Trusted Computing

- We use mechanisms found within the TCG TP which seal, measure, store and report integrity metrics in a trusted manner to ensure the privacy of data
- These mechanisms may be used to determine processes running on a target machine when it boots, and further ensure that data is only accessed in a trusted environment where only specified processes are running

20

TPM Identity (version 1.1b)

- A Trusted Platform Module (TPM) identity is used to attest to aspects of the TP. This is provided by a Privacy CA
- Three certificates attesting to various aspects of the platform are sent to a Privacy CA
- If the certificates are valid for the TPM, the Privacy CA provides the TPM with a TPM identity

21

TPM Identity (version 1.1b)

- TPM Endorsement Credential
 - attests that a Trusted Platform Module (TPM) conforms to the TCG specification
- Platform Credential
 - attests that the platform as a whole is a genuine TCG platform
- Conformance Credential
 - attests that the design and incorporation of the platform conforms to the TCG specification.

22

TPM Identity (version 1.2)

- Uses Direct Anonymous Attestation (DAA)
 - Removes need for Privacy CA

23

TCG measuring, reporting and storing

- The Core Root of Trust for Measurement (CRTM)
 - Responsible for integrity measurement of the first component to execute on a platform
- Root of trust for measurement (RTM)
 - Responsible for the integrity measurement of following components

24

Platform Configuration Registers (PCRs)

- When the platform starts up, the CRTM takes a measurement used to ensure the integrity of the first component to be executed on the TP
 - This is reported to the Platform Configuration Register (PCR)
- The measured component is then responsible for measuring the integrity of the next component to be executed and is called the RTM
 - This is also reported to a Platform Configuration Register (PCR)

25

Challenging the Trusted Platform

- An entity which wishes to challenge the state of a Trusted Platform will receive the values found in the PCR together with some validation data
 - Validation data is data signed by an entity which vouches to an aspect of a platform and shows the values that should result when integrity measurements are made in the platform
- Using this validation data, a challenger recalculates PCR values and compares these to the ones sent by the challenger

26

Sealing Data

- The TCG specification also provides a mechanism which may be used to dictate the state a platform must be in for data encrypted by the TPM to be decrypted
 - Sealing of data may also be without the additional requirement of dictating the state of the platform to decrypt data

27

Sealing Data

- Sealing mechanism relies on three objects
 - the digestAtCreation
 - a hash of the list of PCR numbers and their corresponding PCR values when the sealed data item was created
 - the digestAtRelease
 - a hash of a list of PCR numbers and corresponding PCR values to which data may be released
 - a list of PCRs which must be considered when releasing data.

28

Sealing Data

- When a request is made to unseal this data, the TPM decrypts the sealed item. The information held within this sealed item is only released if, when using the listed PCR values, the recalculation of digestAtRelease corresponds to the one found in the sealed item

29

TCG enabling privacy

- Upon first interaction with the service provider's TP, the privacy subject will typically request proof of the state of the TP
 - The privacy subject will typically send the TP a challenge
- The TP then returns information in the form of a signed version of the challenge and PCR values and also validation data
- The signing key used here is from the TPM identity
 - The use of this key assures the privacy subject that the TP they are interacting with is a valid TP
 - The inclusion of the challenge prevents replay attacks

30

TCG enabling privacy

- Using the validation data, the privacy subject may then recalculate the PCR values found within the scope of the signature, which will then assure them of the state of the service provider's platform
- Also, the user may also verify integrity of software found on the target TP
 - This may allow a user to ensure that target platforms use software which will manage their data in an appropriate manner

31

TCG enabling privacy

- If the target platform is in a satisfactory state the user can then specify the state of the platform for future use of their private data
 - TPM Seals data to a platform state
 - The service provider's platform must be in the specified state for further use of the private data

32

- Introduction
- Privacy
- Constraints
- Trusted Computing
- TCG enabling Privacy
- **NGSCB enabling Privacy**
- Conclusion

Next Generation Secure Computing Base (NGSCB)

- Trusted Computing Platform being developed by Microsoft
- Uses two kernels on the same platform
 - Standard operating system kernel
 - Security kernel
- Kernels and processes are partitioned by a machine monitor
 - Security essential processes run on the secure partition

NGSCB

- NGSCB provides
 - Strong process isolation
 - Separates secure processes from un-trusted processes
 - Sealed storage
 - May be used to indicate platform states for unsealing data
 - Secure paths
 - Ensures existence of a secure path between devices and a platform
 - Attestation

35

NGSCB

- The mechanisms provided in the NGSCB architecture may also be used to provide user privacy of personal information in a similar manner to that described using the TCG specification

36

- Introduction
- Privacy
- Constraints
- Trusted Computing
- TCG enabling Privacy
- NGSCB enabling Privacy
- **Conclusion**

Conclusion

- We have shown how Trusted Computing Platforms may be used to ensure that a user's private data is managed according to the wishes of the user
- Additionally, we have extended this and shown how future use of this data can be dependent on the platform being in a secure state



Thank you!