Enforcing Trust in Pervasive Computing with Trusted Computing Technology.

Shiqun Li[1,2] Shane Balfe[3] Jianying Zhou[2] Kefei Chen[1]

[1]Shanghai Jiao Tong University

[2]Institute for InfoComm Research

[3]Royal Holloway, University of London

1st International Workshop on Critical Information Infrastructures Security

Outline

Outline

Outline

Outline

Overview

Definition

Trusted Computing Group: A trusted system or component is one that behaves in the expected manner for a particular purpose.

Deployment

- TPM (Trusted Platform Module) market saturation by 2010 - IDC.
- Processor support (Averill) tentatively - 2008.
- OS support - soon?

Overview

Definition

Trusted Computing Group: A trusted system or component is one that behaves in the expected manner for a particular purpose.

Deployment

- TPM (Trusted Platform Module) market saturation by 2010 - IDC.
- Processor support (Averill) tentatively - 2008.
- OS support - soon?

Overview

Definition

Trusted Computing Group: A trusted system or component is one that behaves in the expected manner for a particular purpose.

Deployment

- TPM (Trusted Platform Module) market saturation by 2010 - IDC.
- Processor support (Averill) tentatively - 2008.
- OS support - soon?

Overview

Definition

Trusted Computing Group: A trusted system or component is one that behaves in the expected manner for a particular purpose.

Deployment

- TPM (Trusted Platform Module) market saturation by 2010 - IDC.
- Processor support (Averill) tentatively - 2008.
- OS support - soon?

Overview

Definition

Trusted Computing Group: A trusted system or component is one that behaves in the expected manner for a particular purpose.

Deployment

- TPM (Trusted Platform Module) market saturation by 2010 - IDC.
- Processor support (Averill) tentatively - 2008.
- OS support - soon?

Outline

TPM support

Measuring, Storing and Reporting

- Integrity measurement is the process of obtaining metrics of platform characteristics that affect the integrity (trustworthiness) of a platform; storing those metrics; and putting digests of those metrics in PCRs (Platform Configuration Registers).
- Storage has a double meaning in Trusted Computing. It refers to the intermediate step between measurement and report but also to the protection of keys and data with a TPM
- Integrity reporting is the process of attesting to the contents of integrity storage.

TPM support

Measuring, Storing and Reporting

- Integrity measurement is the process of obtaining metrics of platform characteristics that affect the integrity (trustworthiness) of a platform; storing those metrics; and putting digests of those metrics in PCRs (Platform Configuration Registers).
- Storage has a double meaning in Trusted Computing. It refers to the intermediate step between measurement and report but also to the protection of keys and data with a TPM
- Integrity reporting is the process of attesting to the contents of integrity storage.

TPM support

Measuring, Storing and Reporting

- Integrity measurement is the process of obtaining metrics of platform characteristics that affect the integrity (trustworthiness) of a platform; storing those metrics; and putting digests of those metrics in PCRs (Platform Configuration Registers).
- Storage has a double meaning in Trusted Computing. It refers to the intermediate step between measurement and report but also to the protection of keys and data with a TPM
- Integrity reporting is the process of attesting to the contents of integrity storage.

TPM support
Remote Attestation

- This is the mechanism through which a challenger can inspect a remote platform's state.
- Before a platform can attest to its state it must obtain a credential using either a Privacy CA or DAA based approach
- In either case the end result is the same. The platform obtains a credential (or a means of issuing credential like statements) that will be used to adduce current platform state.

TPM support
Remote Attestation

- This is the mechanism through which a challenger can inspect a remote platform's state.
- Before a platform can attest to its state it must obtain a credential using either a Privacy CA or DAA based approach
- In either case the end result is the same. The platform obtains a credential (or a means of issuing credential like statements) that will be used to adduce current platform state.

TPM support
Remote Attestation

- This is the mechanism through which a challenger can inspect a remote platform's state.
- Before a platform can attest to its state it must obtain a credential using either a Privacy CA or DAA based approach
- In either case the end result is the same. The platform obtains a credential (or a means of issuing credential like statements) that will be used to adduce current platform state.

TPM support
Delegation and Certified Migration

- Delegation enables PCR constraints on delegated rights.
- Certified Migration permits secure transfer of migratory keys from one TCG compliant platform to another. The new platform has full usage of the migrated key.

TPM support
Delegation and Certified Migration

- Delegation enables PCR constraints on delegated rights.
- Certified Migration permits secure transfer of migratory keys from one TCG compliant platform to another. The new platform has full usage of the migrated key.

Outline

Intel's La Grande, AMD's Presidio, ARM's Trustzone

- Protected Execution: Provides applications with the ability to run in isolated protected execution environments.
- Protected Input: Provides a mechanism that protects communication between the keyboard/mouse and applications running in the protected execution environments.
- Protected graphics: Provides a mechanism that enables applications running within the protected execution environment to send display information to the graphics frame buffer
- Protected Launch: Provides for the controlled launch and registration of the critical OS and system software components in a protected execution environment.

Intel's La Grande, AMD's Presidio, ARM's Trustzone

- Protected Execution: Provides applications with the ability to run in isolated protected execution environments.
- Protected Input: Provides a mechanism that protects communication between the keyboard/mouse and applications running in the protected execution environments.
- Protected graphics: Provides a mechanism that enables applications running within the protected execution environment to send display information to the graphics frame buffer
- Protected Launch: Provides for the controlled launch and registration of the critical OS and system software components in a protected execution environment.

Intel's La Grande, AMD's Presidio, ARM's Trustzone

- Protected Execution: Provides applications with the ability to run in isolated protected execution environments.
- Protected Input: Provides a mechanism that protects communication between the keyboard/mouse and applications running in the protected execution environments.
- Protected graphics: Provides a mechanism that enables applications running within the protected execution environment to send display information to the graphics frame buffer
- Protected Launch: Provides for the controlled launch and registration of the critical OS and system software components in a protected execution environment.

Intel's La Grande, AMD's Presidio, ARM's Trustzone

- Protected Execution: Provides applications with the ability to run in isolated protected execution environments.
- Protected Input: Provides a mechanism that protects communication between the keyboard/mouse and applications running in the protected execution environments.
- Protected graphics: Provides a mechanism that enables applications running within the protected execution environment to send display information to the graphics frame buffer
- Protected Launch: Provides for the controlled launch and registration of the critical OS and system software components in a protected execution environment.

Outline

Microsoft's NGSCB, OpenTC project

- Implementation of an isolation kernel that enforces domain separation.
- NGSCB - Microsoft's efforts in the area of Trusted Operating Systems.
- OpenTC - EU project for the development of an open source OS (amongst other things).

Microsoft's NGSCB, OpenTC project

- Implementation of an isolation kernel that enforces domain separation.
- NGSCB - Microsoft's efforts in the area of Trusted Operating Systems.
- OpenTC - EU project for the development of an open source OS (amongst other things).

Outline

Pervasive Computing needs trust

- Pervasive Computing environment is open and dynamic, devices and environment may be unknown to each other.
- Confidentiality, Integrity, Authentication, Authorisation...
- Mutual belief of behaviors as expected?

Pervasive Computing needs trust

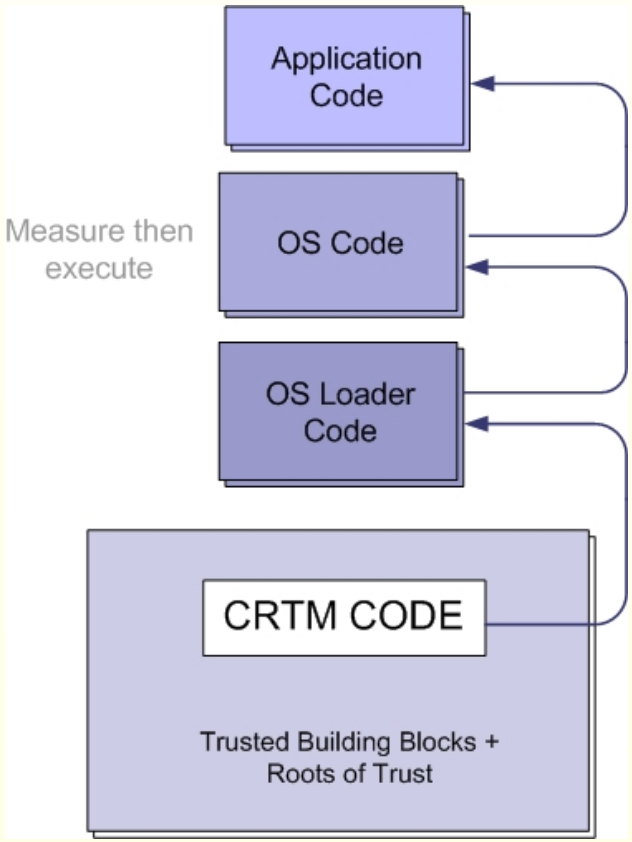
- Pervasive Computing environment is open and dynamic, devices and environment may be unknown to each other.
- Confidentiality, Integrity, Authentication, Authorisation...
- Mutual belief of behaviors as expected?

Pervasive Computing needs trust

- Pervasive Computing environment is open and dynamic, devices and environment may be unknown to each other.
- Confidentiality, Integrity, Authentication, Authorisation...
- Mutual belief of behaviors as expected?

Definition

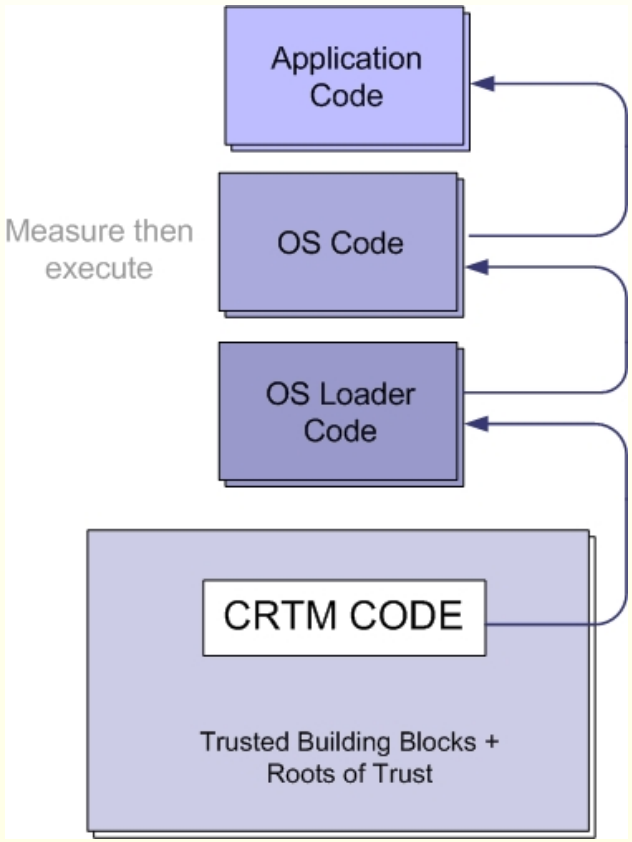
Trusted Computing Group: A trusted system or component is one that behaves in the expected manner for a particular purpose.



- Transitive trust based on manufacturing process.
- Trust is established from code identities.

Definition

Trusted Computing Group: A trusted system or component is one that behaves in the expected manner for a particular purpose.



- Transitive trust based on manufacturing process.
- Trust is established from code identities.

Outline

Controlling Access After Distribution

There may be policies restricting use of confidential data

- Access control - based on proof of possession of a valid credential providing the capabilities.
- Control after distribution - based on proof of correct authentication data to a TPM.

Controlling Access After Distribution

There may be policies restricting use of confidential data

- Access control - based on proof of possession of a valid credential providing the capabilities.
- Control after distribution - based on proof of correct authentication data to a TPM.

Controlling Access After Distribution

Set-Up:Credential acquirement

1. Instructs *TPM* to generate non-migratable keys.
2. *TPM* creates a *TPM_Key* specifying authorisation data and an acceptable platform state for it's usage.
3. Have this key certified by the *TPM*.
4. *TPM* returns the *TPM_Certify_Info* describing the certified key.

Access Control

- Simple Challenge-Response based protocols incorporating credentials.
- *TPM* would unseal the encrypted document at any time provided the authorisation data is valid.

Trusted Printing Service

- Client requests server's attestation.
- Server checks the validation of the Client, responses with running integrity measurement and other necessary information.
- Client checks the response to assure the server's behavior, then send request.

Trusted Printing Service

- Client requests server's attestation.
- Server checks the validation of the Client, responses with running integrity measurement and other necessary information.
- Client checks the response to assure the server's behavior, then send request.

Trusted Printing Service

- Client requests server's attestation.
- Server checks the validation of the Client, responses with running integrity measurement and other necessary information.
- Client checks the response to assure the server's behavior, then send request.

Outline

Concluding points

- Trusted Computing could end up playing an important role in future architectures. Both from a hardware perspective and in establishing communicability infrastructure - Trusted Network Connect.
- Stable force of homogeneity in heterogenous environments. Perhaps not at the minor device level (Ubicomp in its truest sense) but more at the meta-interaction level performing abstract services.

Concluding points

- Trusted Computing could end up playing an important role in future architectures. Both from a hardware perspective and in establishing communicability infrastructure - Trusted Network Connect.
- Stable force of homogeneity in heterogenous environments. Perhaps not at the minor device level (Ubicomp in its truest sense) but more at the meta-interaction level performing abstract services.

Concluding points

- Trusted Computing could end up playing an important role in future architectures. Both from a hardware perspective and in establishing communicability infrastructure - Trusted Network Connect.
- Stable force of homogeneity in heterogenous environments. Perhaps not at the minor device level (Ubicomp in its truest sense) but more at the meta-interaction level performing abstract services.