

Killer Applications in Pervasive Computing Nanodatacenters - EU FP7 funded Project

Nicolai Kuntze¹

¹Fraunhofer Institute for Secure Information Technology

December 2, 2008

Outline

- 1 Use Case
 - Roles and Trust
 - Interaction
- 2 Threat Analysis
 - authenticity and integrity
 - content security
 - distribution mechanisms
- 3 Architecture
 - Attestation
 - Platform
 - Communication
 - Media Protection
 - Time

Use Case

- Distribution of **Virtual Goods** based on a distributed environment may be one of the first applications for pervasive environments
- Strong acceptance from Network Providers, Content Providers, and also some request by the users
- Usage of available bandwidth by utilising locality effects

Pervasive Application

- ubiquitous
- means that it is operated in a hostile environment

Use Case

- Distribution of **Virtual Goods** based on a distributed environment may be one of the first applications for pervasive environments
- Strong acceptance from Network Providers, Content Providers, and also some request by the users
- Usage of available bandwidth by utilising locality effects

Pervasive Application

- ubiquitous
- means that it is operated in a hostile environment

Use Case from a Security Perspective

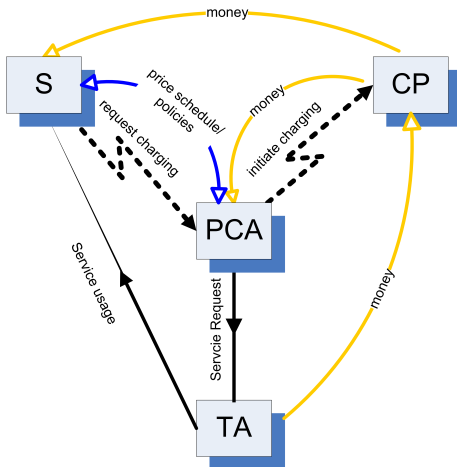
NaDa security discusses full business process security to allow for all stakeholders to put trust into the platform

- Content provider expects that content is secure during transfer, storage, and delivery
- Security policies are defined by each stakeholder (mostly by the network operator) and enforced by the platform
- **Node manages** IDs (MID) for stakeholders

Outline

- 1 Use Case
 - Roles and Trust
 - Interaction
- 2 Threat Analysis
 - authenticity and integrity
 - content security
 - distribution mechanisms
- 3 Architecture
 - Attestation
 - Platform
 - Communication
 - Media Protection
 - Time

Roles in the model 1/2



Roles in the model 2/2

Most business cases are composed of the following roles.

- Trusted Agent (TA) who is for example the customer
- Service (S) who offers a certain service or access to services
- Privacy Certification Authority (PCA) providing TA a certain identity
- Charging Provider (CP) managing all money transfers between the involved parties

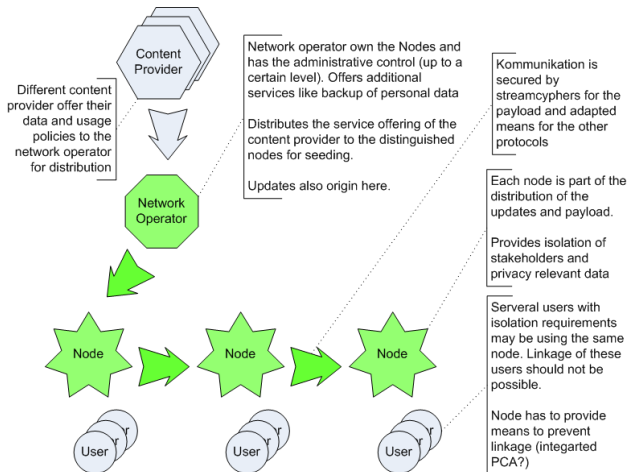
Trust in Systems

- Trust on a technical level just says that a system will always behave in an expected manner
- This trust definition does not include any judgement on the behaviour of the system e.g. in terms of good or bad behaviour. If there is a failure in the System Trust only says that we expect this failure.

Outline

- 1 Use Case
 - Roles and Trust
 - **Interaction**
- 2 Threat Analysis
 - authenticity and integrity
 - content security
 - distribution mechanisms
- 3 Architecture
 - Attestation
 - Platform
 - Communication
 - Media Protection
 - Time

Player interaction



Identified Threats

The trust in the overall system depends on the security of each node.
Therefore the prioritisation on the top level can be as follows:

- 1 Authenticity and Integrity for the nodes are primary aims
- 2 Content protection is build upon these basic requirements
- 3 Protection of the distribution mechanisms

In this context Manageable IDs (MID) encompass (for simplicity)

- User Keys
- User data
- Other user Credentials related to its identity

Identified Threats to authenticity and integrity

- Emulation of a legitimate Box to obtain MIDs
- Attacks on the MID provision process
- Malicious software at the Box to access MIDs
- Physical attacks on the Box to obtain MIDs and keys
- Modification of functions of the Box
- Attacking and changing the permissions associated with an MID
- One stakeholder access the MIDs of another
- Access to the Box by masquerading as a legitimate user
- User loses access due to malfunction of MIDs
- False registration to obtain MIDs

Identified Threats to content security

- Eavesdropping on stored content
- Unauthorised changes to the content consumption licence
- Unauthorised changes to the content distribution license
- Content manipulation (e.g downgrading)
- Illigieal use of content after delivery (e.g. redistribution)

Identified Threats to distribution mechanisms

- Premature removal of content from the cache
- Unauthorised injection of content
- Changes to distribution tables (e.g. DHT)
- Modifications to the caching of content

Outline

- 1 Use Case
 - Roles and Trust
 - Interaction
- 2 Threat Analysis
 - **authenticity and integrity**
 - content security
 - distribution mechanisms
- 3 Architecture
 - Attestation
 - Platform
 - Communication
 - Media Protection
 - Time

Emulation of a legitimate Box to obtain MIDs

An attacker emulates the functions of a legitimate Box (this needs an extraction of appropriate credentials and MIDs first) and gains service access based on these duplicates.

- This allows for service access that is billed for by the original user
- Impact on the overall distribution network is also possible

Attacks on the MID provision process

An attacker penetrates the MID provision process to access and use them. This can be done e.g. by eavesdropping, Man-in-the-middle, or spoofing attacks.

- This allows for service access that is billed for by the original user
- Jeopardises the content distribution process by allowing to eavesdrop on the data

Malicious software at the Box to access MIDs (Logical attacks)

An attacker gains access to MIDs using malicious software and is later on able to use the identity credential in other environments.

- Extraction allows for service access that is billed for by the original user
- Could lead to eavesdropping on the protected data (e.g. content)
- Privacy implications

Physical attacks to obtain MIDs and keys

Use of physical attacks (e.g. timing attacks) to reveal the Identity secrets and used other credentials.

- Extraction allows for service access that is billed for by the original user
- Could lead to eavesdropping on the protected data (e.g. content)
- Privacy implications

Modification of functions of the Box

Changes to the behaviour of the box without accessing the secrets it is keeping. This could e.g. to DoS attacks or mischarging.

- Impact of the changes on the overall systems depends on the system that is affected
- Could lead to severe problems on the overall system stability
- Privacy issues may arise
- Eavesdropping on the protected data may be possible

Attacking and changing the permissions associated with an MID

Each MID has associated rights on the level of the operations that are allowed for the associated stakeholder.

- Attacker may gain administrative control on the box
- Could lead to problems on the system stability

One stakeholder access the MIDs of another

Cross taking between stakeholders that leads to security breaches and by this exposure of the protected secrets.

- One stakeholder may gain insights on secrets of another
- Could lead to service access in the name of another person
- Privacy breach

Access to the Box by masquerading as a legitimate user

Without knowledge of Identity secrets the attacker masquerades himself as a legitimate user. A possible reason for this may be due to insufficient authentication methods or that an attacker can interfere with the system and issue command under the name of a legitimate user.

- Could lead to service access in the name of another person or unpayed service access
- Privacy breach

User loses access due to malfunction of MIDs

The legitimate user loses the possibility to access his subscribed services.

- Reasons for this may hardware malfunctions, software failures, or deliberate attacks
- Result is a Denial of Service
- Leads to support costs

False registration to obtain MIDs

- **Weak Identity** leads to false registrations
- Attackers receive by this a mean to conceal their attacks behind many accounts
- Weak Identities are a major tool for attacks on incentive and P2P schemes

Correlation of data

A fraudulent stakeholder or third party gains access to other stakeholder information and is able to link these.

- Profiling of user (stakeholder) actions is the result and a possible privacy leakage.
- The process of data linking can be performed either at the nodes or on the infrastructure side.
- Linkage at the side of the box would require another unallowed behaviour already covered by other threats.
- Infrastructure attacks on privacy are more likely.

Outline

- 1 Use Case
 - Roles and Trust
 - Interaction
- 2 Threat Analysis
 - authenticity and integrity
 - **content security**
 - distribution mechanisms
- 3 Architecture
 - Attestation
 - Platform
 - Communication
 - Media Protection
 - Time

Eavesdropping on stored content

Content is stored according to the caching algorithms on each node in advance of the consumption until the cache is flushed. During this time the content stored on the node without personalisation. In case of active content (e.g. games) maps and user specific data are also endangered.

- Leakage of data leads to a loss of value of these data
- Content provider are less confident in the platform
- May also result in contractual penalties

Unauthorised changes to the content consumption licence

Each content contains explicit or implicit licences defining the consumption of the content. These rules can for example define the frequency of viewing, the place, time, or quality of the equipment.

- Changes may degrade the QuE

Unauthorised changes to the content distribution license

Redistribution of content may be part of use cases in the focus of the project. Distribution licenses define the distribution and the interaction between the entities.

- Changes may lead to unpayed or misspayed content transfer e.g. by paying to another entity as originally intended.
- Loss of trust by the content provider

Content manipulation (e.g downgrading)

Manipulation to the content by e.g. downgrading it or by adding new features to avatars in a game by an attacker.

- Loss of trust in the system by the content provider
- Loss of trust by the customers

Illegal use of content after delivery

the underlying cot e.g. layed down in the content distribution or content consumption license. Examples are unlawfull distribution or modification.

- Loss of income due to unauthorised distribution
- Bad mouthing by producing low quality examples of the offered content

Outline

- 1 Use Case
 - Roles and Trust
 - Interaction
- 2 Threat Analysis
 - authenticity and integrity
 - content security
 - **distribution mechanisms**
- 3 Architecture
 - Attestation
 - Platform
 - Communication
 - Media Protection
 - Time

Premature removal of content from the cache

Content is cached by the node. QoE is dependend on the quality of the cache and its filling. Attackes may use the node to force the removal of content on its node and the local nodes by interferring with the protocol.

- QoE reduction in terms of service availability and latencies recognised by the user

Unauthorised injection of content

An attacker injects content that is not authorised by the network provider

- Depending on the content (e.g. violence, pornography) severe penalties are imaginable for the network operator
- Malicious content may effect the public opinion on the system
- Unpayed content in the network available (lack of revenue stream)

Changes to distribution tables (e.g. DHT)

Attacking the tables used to distribute the content in the network (e.g. DHT tables) leads to unavailable content for a certain number of users. It is also possible that an attacker creates a subnet where he controls the content.

- Degraded service quality

Modifications to the caching of content

An attacker creates by e.g. automatic usage of the node malicious usage profiles resulting in changes to the caching strategy and cached content.

- Leads to changed availability of content

Outline

- 1 Use Case
 - Roles and Trust
 - Interaction
- 2 Threat Analysis
 - authenticity and integrity
 - content security
 - distribution mechanisms
- 3 **Architecture**
 - **Attestation**
 - Platform
 - Communication
 - Media Protection
 - Time

Attestation as a basic mean

Authenticity and Integrity of the platform is the basic requirement that is required to build up security and trustworthiness of the distribution process on it

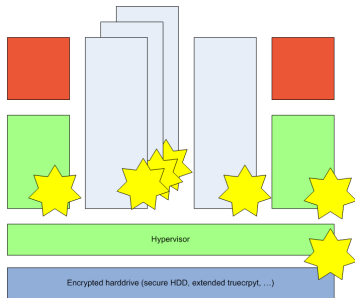
- Trusted Computing establishes a strong base providing a protected platform identity
- Before a device is accepted in the P2P network it has to provide proof of its integrity and authenticity
- This has to be incorporated in the P2P protocols between the devices in the field
- Offers secure storage and processing in the user domain

Attestation and virtualised systems

Reporting the trustworthiness of a virtualised system requires

- Providing proof on the DOM running the system. Each DOM requires therefore its own trust anchor.
- Providing proof on the integrity and authenticity of the underlying layer N-1.
- This recursion stops if an appropriate anchor is found that is considered trusted (e.g. TPM)
- Open issue here is how the appropriate protocol looks satisfying the security and trust requirements.

Security Anchor in Virtual System



- Each DOM owns **his own Security Anchor** that is implemented e.g. in software (level N)
- These are protected by the hypervisor (level N-1)
- **level 0** relies on a hardware device e.g. TPM

General Virtualisation remarks

- Virtualisation introduces **horizontal isolation** between processes or other logical entities (e.g. called DOMs, compartments, ...)
- The stakeholder controlling the underlying system (e.g. the hypervisor, microkernel, ...) is also able to interfere with all running entities ontop
- Stakeholders have to establish complete trust in the owner of the underlying system as they are not able to prove the correct operation other then reviwing the system by source code checks
- If it is reviewed Trusted Computing provides means to testify that the reviewed system is running below the virtualized systems (as the operation of the virtualised systems is not reliable these checks can only be made outside)

Virtualisation and Attestation Challenges

- N-1 attestation is still a research topic as it is not clear what the best solution here is
- Attestation of multiple layers also requires significant computational overhead (once)

Outline

- 1 Use Case
 - Roles and Trust
 - Interaction
- 2 Threat Analysis
 - authenticity and integrity
 - content security
 - distribution mechanisms
- 3 **Architecture**
 - Attestation
 - **Platform**
 - Communication
 - Media Protection
 - Time

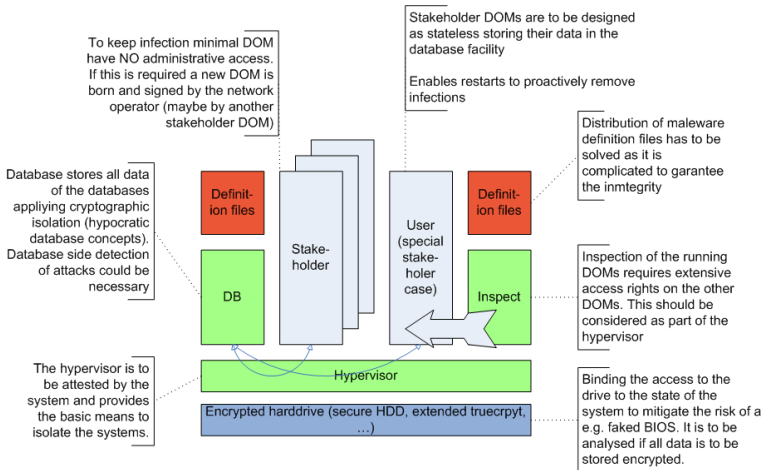
A secure and attestable environment

Several schemes are possible and should be combined to fulfill the requirements to the platform discussed before.

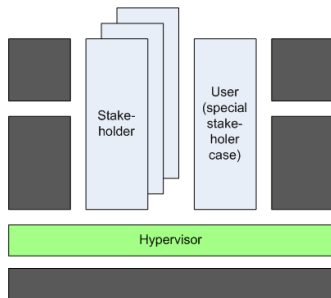
- Shape of the environment
- Meta level evaluation
- OS creation certificates
- Read only software portions
- Separation of Code and Data

Attestation allow to testify the existence of these measures to the remote systems.

System design overview

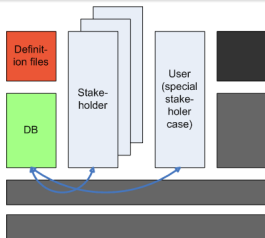


Shape of the environment



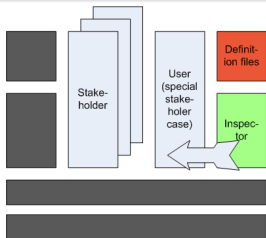
- Definition and enforcement of the environment of each DOM
- Enforcement is done by the hypervisor based on policies given for each DOM
- Policies have to be defined by the DOM producer and signed. The hypervisor then has to decide if the issuer is trusted.

Seperation of Code and Data



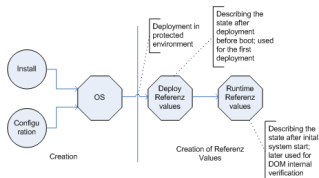
- Stateless DOMs allow for restarts of the DOM at random points in the execution
- Statelessness can be enabled by DB storing the actual state. During recovery only a smart amount of work is lost
- Aim is to be able to restart the DOM at arbitrary points without relying on additional communication with the DOM OS
- After a successful attack max. time until it is clean can be guaranteed

Meta level evaluation



- Ensuring the integrity during runtime by inspection. Known technologies like virus scanner can be incorporated later
- Problems arise in the transfer and acceptance of updates and definition files used to scan the system
- Scanning a running DOM would require large scale changes to the security model of the hypervisor
- Usefull in combination with stateless aproaches scanning only deactivates system to report possible attacks to the owner

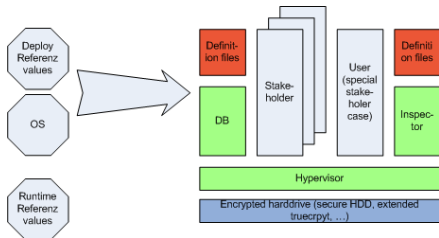
OS creation certificates - creation



Each DOM used by the device is created by the operator and requires credentials stating the origin and integrity.

- Origin is stated by the signature on the referenz values for deployment and runtime
- As the image may change due to the changes during operation also appropriate referenz values for the runtime are required
- After deployment only the Runtime values are of importance for the attestation of the system state

OS creation certificates - deployment (static)



On initial deployment the deployment referenz values and the authenticity is verified by checking the respective certificate OS is bound to platform status to prevent eavesdropping on the DOM image. Junking requires that each junk is bound to the target platform. By this only the target can access the data.

OS creation certificates - runtime (dynamic)

Due to changes during the lifecycle of the DOM e.g. caused by updates or by local adaptations to the platform hosting it the static certificate is later not necessarily applicable

- Changes to the executables require delivery of new images by the operator
- As the image may change due to the changes during operation also appropriate referenz values for the runtime are required
- After deployment only the Runtime values are of importance for the attestation of the system state

Read only software portions

- Readonly software is already in use like the BIOS
- Offers a stable and attested core to rely on that is available after boot
- Integrity can (and should) be verified by cryptographic means by integrating the measurement in the attestation

Outline

- 1 Use Case
 - Roles and Trust
 - Interaction
- 2 Threat Analysis
 - authenticity and integrity
 - content security
 - distribution mechanisms
- 3 **Architecture**
 - Attestation
 - Platform
 - **Communication**
 - Media Protection
 - Time

Communication

- Communication protocols have to provide for authenticity and content protection in the communication between the nodes
- Statements of integrity based upon attestation have to be included where necessary
- From the security perspective update and software distribution towards the nodes are of special interest
- Content protection can be based upon stream ciphers using keys that are bound to the inbound node. Therefore all communication can only be deciphered by a node in the required state.

Outline

- 1 Use Case
 - Roles and Trust
 - Interaction
- 2 Threat Analysis
 - authenticity and integrity
 - content security
 - distribution mechanisms
- 3 **Architecture**
 - Attestation
 - Platform
 - Communication
 - **Media Protection**
 - Time

Content Protection

- On the **node** data is stored protected and bound to the state and identity of the node
- Media consumed by the user can be according to the policies of the provider protected by **DRM** or **watermarks**
- Please note that due to the P2P approach it is not possible to apply user specific protection before the content is delivered by the node
- **Trustworthiness** relies upon the security of the node

P2P Aspects in Content Protection

- As said P2P communication does not allow for user based protection like DRM or Watermarks at the side of the content provider
- Content is distributed in data chunks between the involved nodes, so that the file arrives from different nodes at the target node
- Communication has to assure that **only reliable nodes** are part of the data distribution as malicious nodes may alter or leak content
- Data on the nodes needs to be **cryptographically linked** to the platform and its state to assure that data is only accessible if the box is in a well state

Outline

- 1 Use Case
 - Roles and Trust
 - Interaction
- 2 Threat Analysis
 - authenticity and integrity
 - content security
 - distribution mechanisms
- 3 Architecture
 - Attestation
 - Platform
 - Communication
 - Media Protection
 - Time

Trustworthy Time

- In many business models a reliable time is required underlying certain parts of the contracts and usage regulations
- Time should be build up on a hardware protected capability allowing for offline processes where no centralised authority is available
- Protocoll requires initial synchronisation with a trusted party