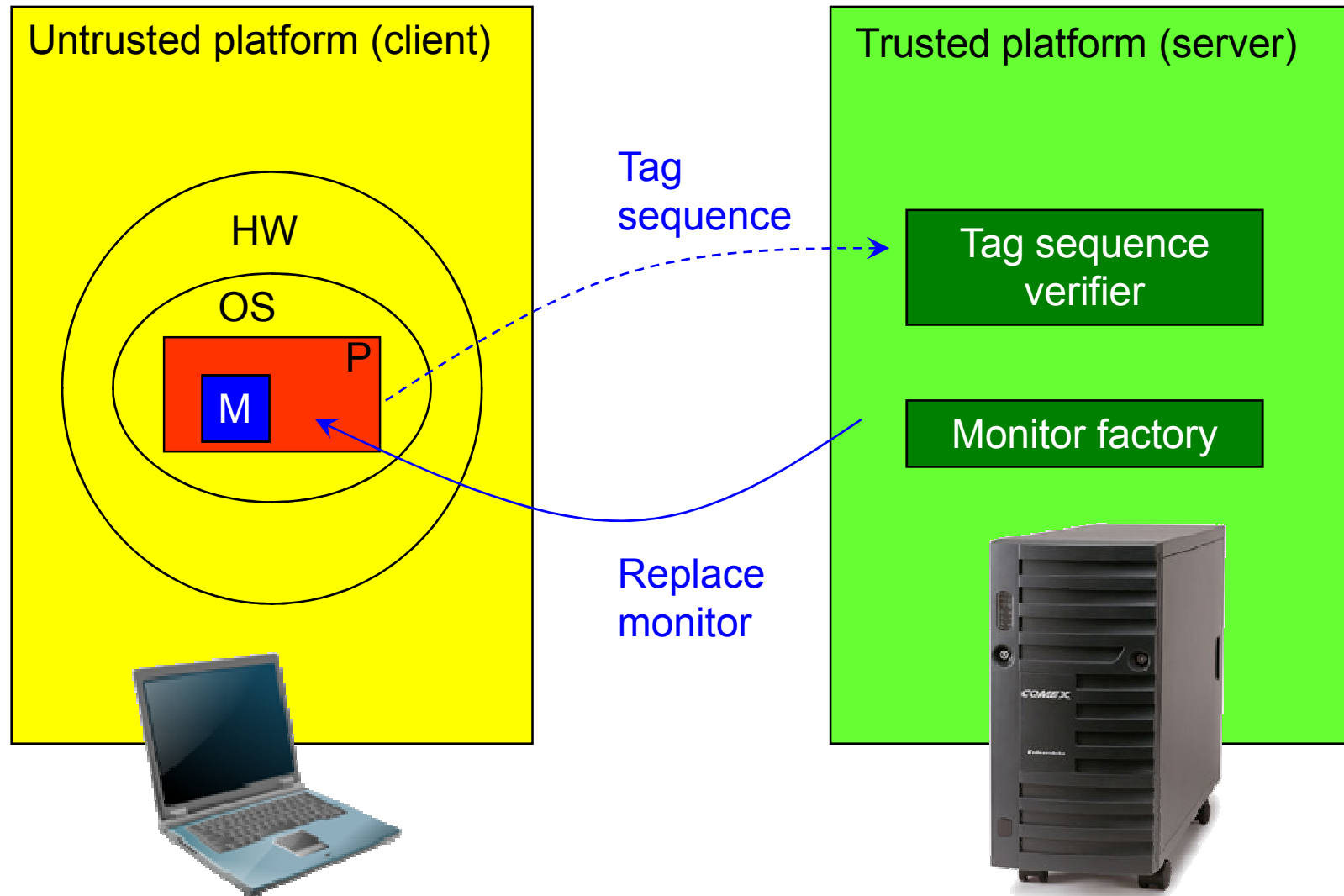


D1.1 Analysis of generic classes of applications

Ceccato Mariano

Fondazione Bruno Kessler-IRST, Trento, Italy

Reference architecture



Client-server

- Instant messaging:
 - Free services may what the client to show advertisements;
 - Attack: bypass advertisement displaying features.
- VoIP:
 - Bypass the payment method;
 - Avoiding the possibility to become a super-node.

Network gaming

- Multi-player games:
 - Because of performances, many critical tasks are performed on the client;
 - Attack: tamper with the client and gain unfair advantages.
- Online gambling:
 - It requires to have an human that plays;
 - Attack: tamper to gain unfair advantages, make a robot plays instead of a human (e.g., in poker).

Protect information management

- Digital content distribution:
 - Protecting the content after the media has been distributed;
 - Attack: distribute the media, play more times than permitted.
- Private information retrieval:
 - Search in a data base, without letting the DBA know what has been searched;
 - Attack: DBA obtains sensitive information by correlating queries with BD entries.
- Healthcare:
 - Medical records are made available to third parties for an eternal consult;
 - Attack: information become public and go to unauthorized parties.

Peer-to-peer

- File sharing:
 - Peers share information according to predefined rules (keep sharing, bigger bandwidth to who shares more)
 - Tamper with the application and bypass rule enforcement

Distributed computing

- Greed computing:
 - The server must correctly apply the scheduling/management policies;
 - The client must correctly access and use the resources;
 - Attack: tamper to bypass the policies.

Mobile code

- Mobile agents:
 - Code that move among several nodes (e.g., hosts) to achieve a goal;
 - Attack: the malicious host could compromise the agent or steal secret keys;
 - Note: protecting the agent from the host is out of the scope of the project.

E-commerce

- Electronic auctions
 - Attack: computer program participate to the auction on behalf of the user (better response time).
- Electronic banking
 - Policies could be enforced by the client, it should behave in a predefined way.
- Privacy friendly shopping chart
 - Shopping cart content is stored on the client (e.g., cookie);
 - Attack: purchase item at a reduced cost.

Application Analysis

<i>Application</i>	<i>Correct execution</i>	<i>Complete execution</i>	<i>Limited execution</i>	<i>Timely execution</i>	<i>Correct number of exec.</i>	<i>Conf. of the program</i>	<i>Conf. of crypto keys</i>
Client-server	X	X	X		X	X	X
Network gaming	X	X	X	X	X	X	X
Protected information management	X	X			X	X	X
Peer-to-peer file sharing		X					
Distributed computing	X	X	X		X	X	
Mobile code	X			X		X	X
E-commerce	X	X	X	X			X

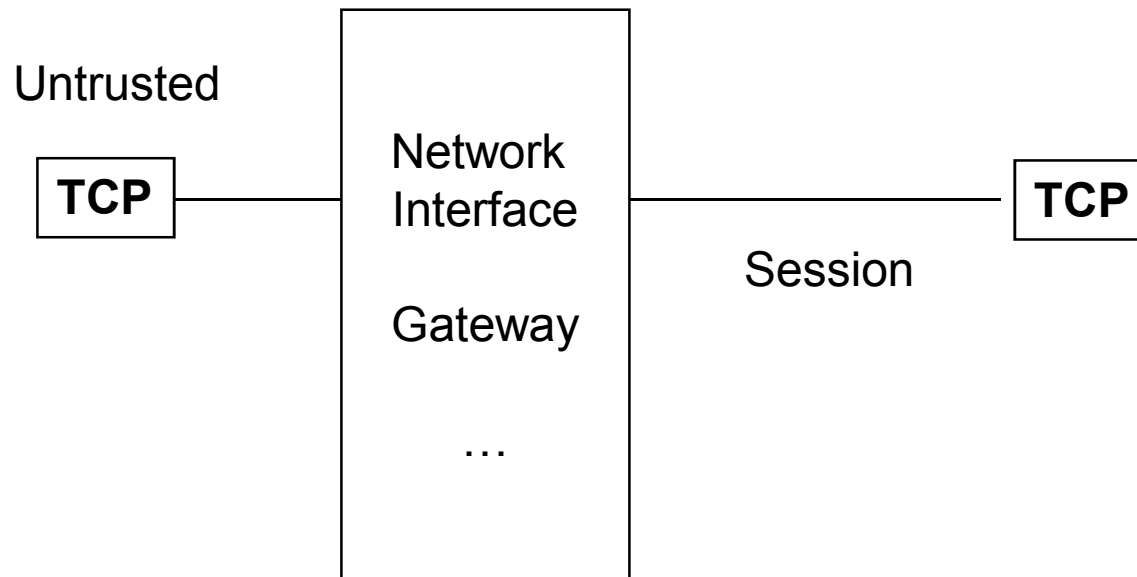
Protect fields (t)

Subset of the application data that must be protected against **tampering**.

- Changes are allowed as long as they do not affect the values of those fields.
- Barrier slicing address this problem by moving the code that updates sensitive field values.
- Examples:
 - Multi-player games.

Protect Protocol

- Two parties
 - Chat
- Three parties



Protect/private data

Subset of the application data that must be protected against **stealing**.

- Data can be tampered but not read in clear.
- This is challenging, maybe hardware is mandatory here.
- Examples:
 - DRM;
 - Digital content distribution;
 - Healthcare;
 - Private information retrieval;
 - Mobile agents.

Protect code

Subset of the application code must be protected against **tampering**.

- The servers relies on a client run a relevant part of the application.
- Examples:
 - Instant messaging;
 - VoIP;
 - Multi-player games;
 - Online gambling;
 - File sharing;
 - Greed computing;
 - Mobile agents.

Protect code

Subset of the application code must be protected against **stealing**.

- Intellectual property protection on the client code (=DRM ?).
- Examples:
 - Multi-player games;
 - Greed computing;
 - Mobile agents.

Discussion

- Other classes to propose/discuss;
- Orthogonal dimensions/views for considering the same applications;
- Other important applications that have been forgotten;
- Purpose of the classification?

	Source code	Data
Tampering		
Stealing		