Securing agents using Secure Docking Module

Zoltán Balogh[1], Emil Gatial[1], Daniel Hein[2], Ladislav Hluchý[1]

[1]Institute of Informatics, Slovak Academy of Sciences (II SAS) Bratislava, Department of Parallel and Distributed Computing, Bratislava, Slovakia

[2]Institute for Applied Information Processing and Communications (IAIK), Graz University of Technology, Graz, Austria

SECRICOM FINAL CONFERENCE 2012,

April 26th, Warsaw, Poland

Európska únia
Európsky fond regionálneho rozvoja

Introduction

Objective

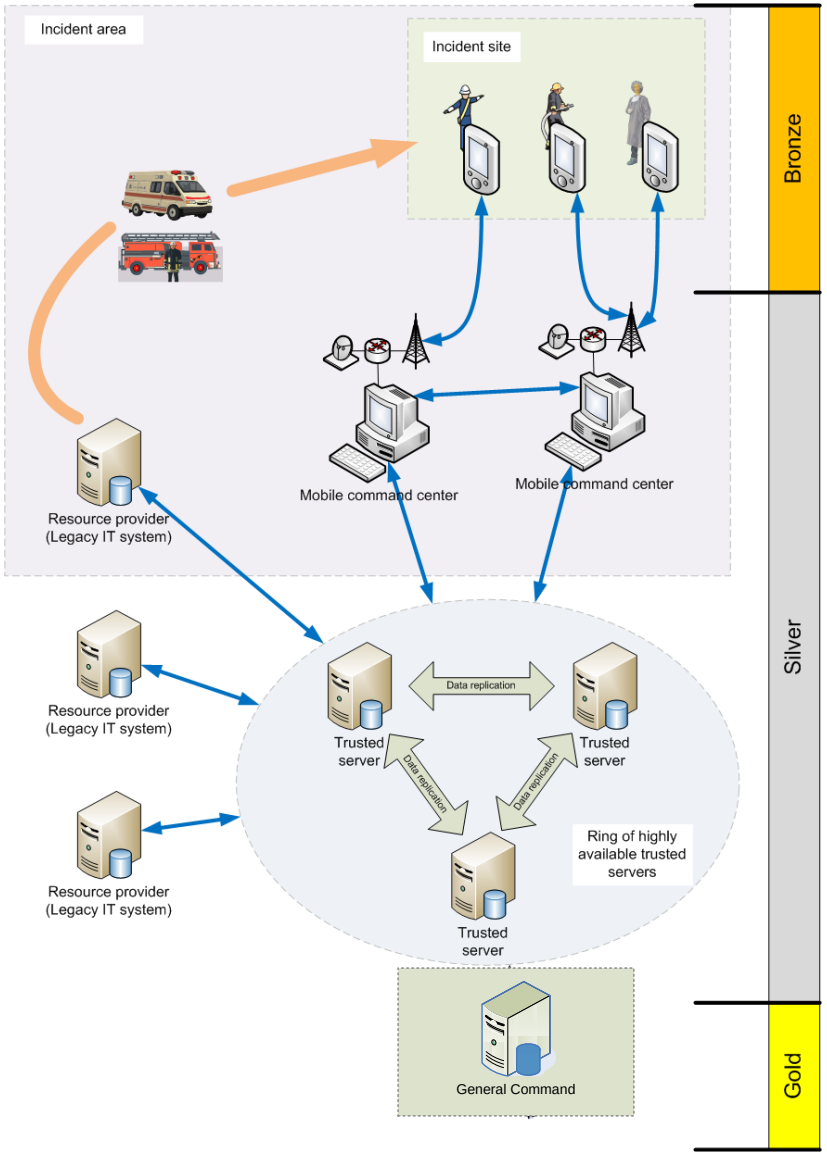
"Add *new smart functions* to existing services which will make the *communication more effective and helpful* for users. Smart functions will be provided by distributed IT systems based on an agents' infrastructure."

Thus we should *allow creating a pervasive and trusted communication infrastructure* fulfilling requirements of *crisis management* users and ready for immediate application.

Requirements for Secure Agent Infrastructure (SAI)

- Provision of a *distributed agent paradigm* to achieve ***confidentiality and access to resources***.
- Should be designed as a *collection of software services* with agent-like features (mobility, pro-activity) which would ***execute in a secure manner***.
- Enable ***access legacy IT systems*** whilst keeping information confidential.
- The *security should be provided* by a specialized component called "***Secure docking module***" (SDM).

SAI Deployment Diagram



Operational Level

Tactical Level

Strategic Level

Security Requirements

- ***Host Platform Providers*** (HPP) - in general any organization which wishes to join the designed system and to provide information from his legacy systems or users must introduce a host platform for agents.
- The following HPPs were identified so far:
  - ***Resource Providers*** – emergency responders (hospitals, fire brigade, police, warehouses) or any other entities which can play a role in the mitigation of crisis
  - ***Command Centers*** – mobile centers which coordinate locally the incident site
  - ***General Command Center*** and ***Operators***
- Security concerns of HPPs:
  1. HPPs do not want/like to install and execute any external application on their systems in line with their strategic legacy applications.
  2. HPPs prefer to have a dedicated and isolated system which would connect to their legacy system in a secure predefined way.
  3. HPPs want to be able to control **what** (data), when and **by who** (traceability) is provided to the system.
  4. HPPs want to be able to configure set of applications executable on their side. Agents must be therefore audited and verified thus mediate trust to executable agent code.

Security Requirements for Agent Platform

The agent platform has the following security requirements in respect to agents:

- *Isolated execution environment* for agent execution - agents must be executed in isolated environment (isolated hardware preferred), so an agent can not harm legacy systems
- Means to *monitor and trace agents activity*
- Means to *configure the set of agents executable on the host platform*

Agents are audited and signed before their deployment. Only agents signed with trusted authority and assigned to selected category will be trusted by a host system.

Threats in general

- Agent platform attacking an agent,
- Agent attacking an agent platform (HPPs concern)
- Agent attacking another agent on the agent platform,
- Other entities attacking the agent system.

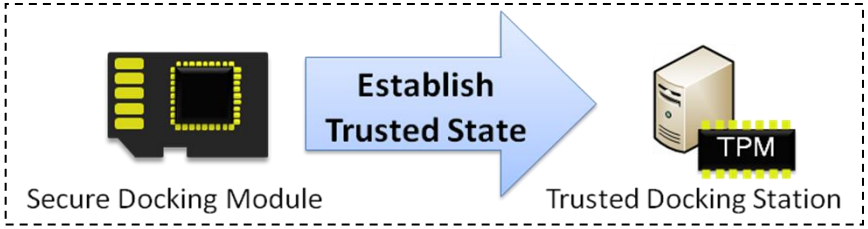
In order to overcome these threats, ***agents require***

1. Safe secured place to store cryptographic credentials (PKI secret keys) and provide interfaces to retrieve these keys
2. Attested platform – a hosted platform which is in a trusted state
3. Provide interface to safely communicate with hosted platform (legacy system).

Hardware Security

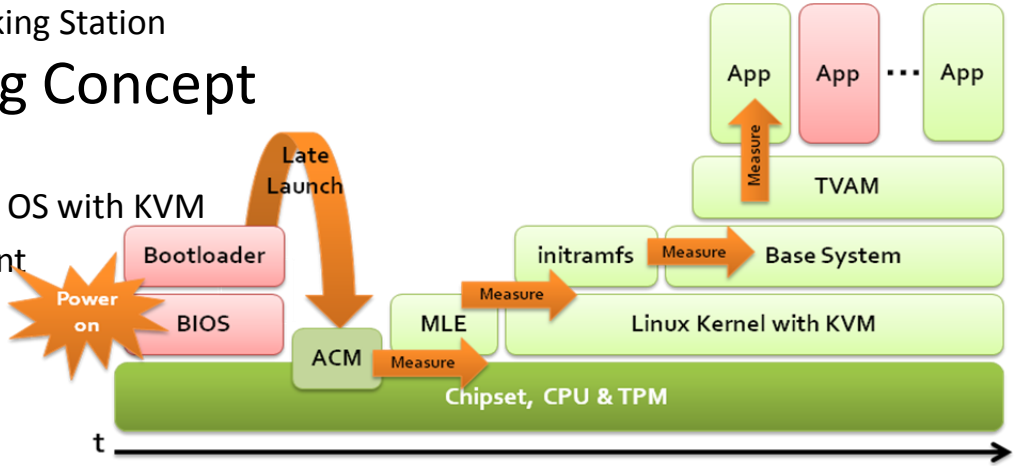
- Core element of the SAI is the *Secure Docking Station* (SDS)
- Realized by two complementary devices called the *Secure Docking Module (SDM)* and the *Trusted Docking Station (TDS)*

SDS = TDS + SDM



Secure Docking Station

- Using Trusted Computing Concept
  - Trust measurements are performed
  - Secure boot loads customized Linux OS with KVM
  - TVAM - virtual partition management



Design and development of SDM and TDS is being done by

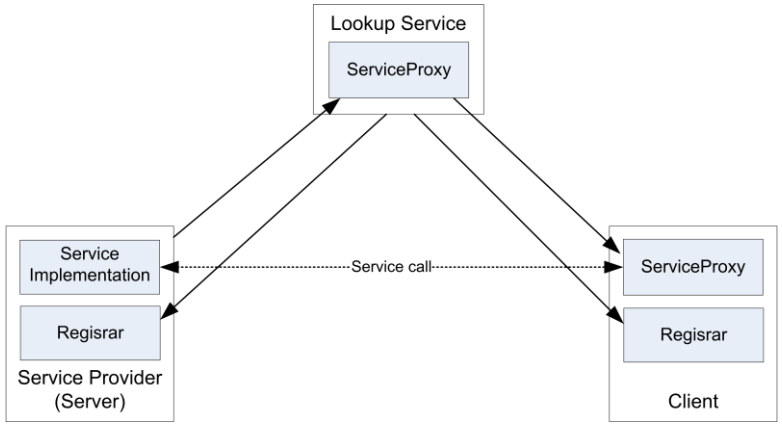
Technical University Graz

Hardware Security

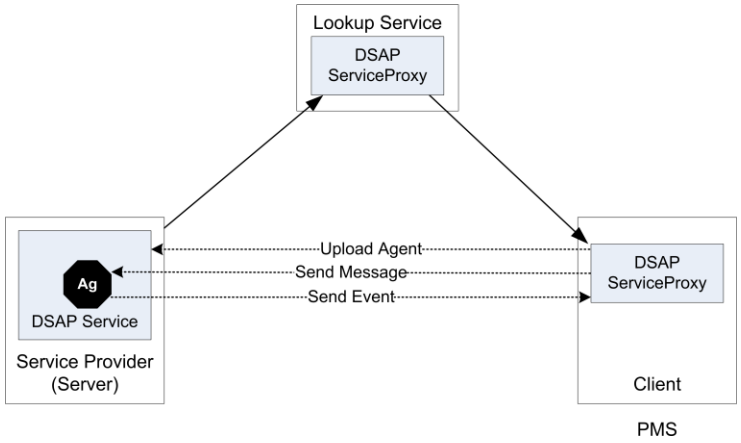
- Secure Docking Module
  - Key storage device with local/remote attestation verification capabilities
  - Protects a small set of key pairs for asymmetric cryptography
  - Releases the keys to a host device if and only if this host device is in a *trusted state*.
- Trusted Docking Station
  - Is a "regular" computer that is attested to be in a *trusted state* – specific software configuration
  - Software configuration is measured by using a *Trusted Platform Module (TPM)*
  - Hosts the Secure Docking Module
- If the TDS is in a *trusted state*, it can be trusted to adhere to a specific *policy*.

Distributed Secure Agent Platform (DSAP)

- Implementation framework
  - Java language
    - "write once run anywhere" – important for easy support of different devices
  - Jini
    - Loading of the service object into client's virtual machine and running it there
    - Requires Java RMI support on the device and ability to load Jini libraries



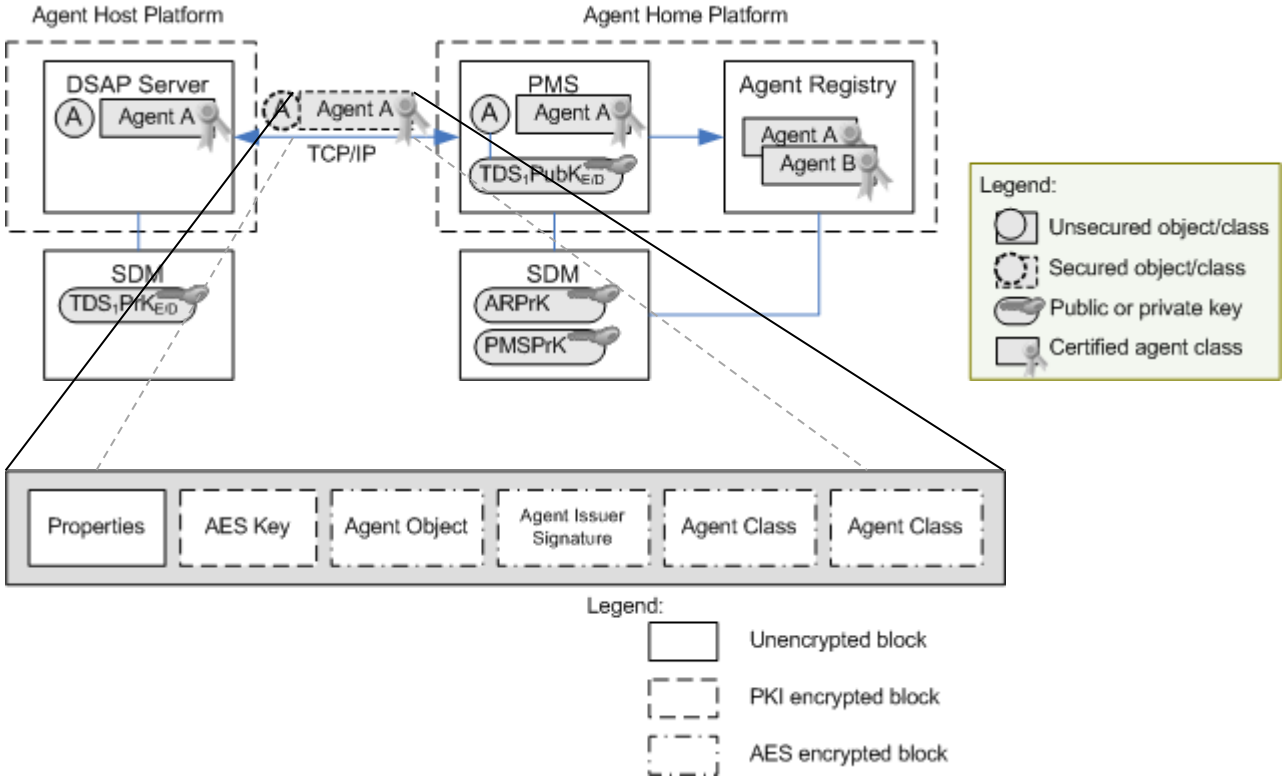
Jini service invocation mechanism



Using SAI service for agent relocation and communication

Securing Agents

- Agent code is transferred encrypted by AES (AES is encapsulated by PubK of destination agent host platform) and transferred to agent host platform
- In the agent host platform the PrivK can be accessed only in case the platform is in the trusted state (well known software and hardware conf.) and it is used to extract AES key and decrypt agen
- Then, AES key is used for communication between agent and client code (PMS)



Testbed Infrastructure

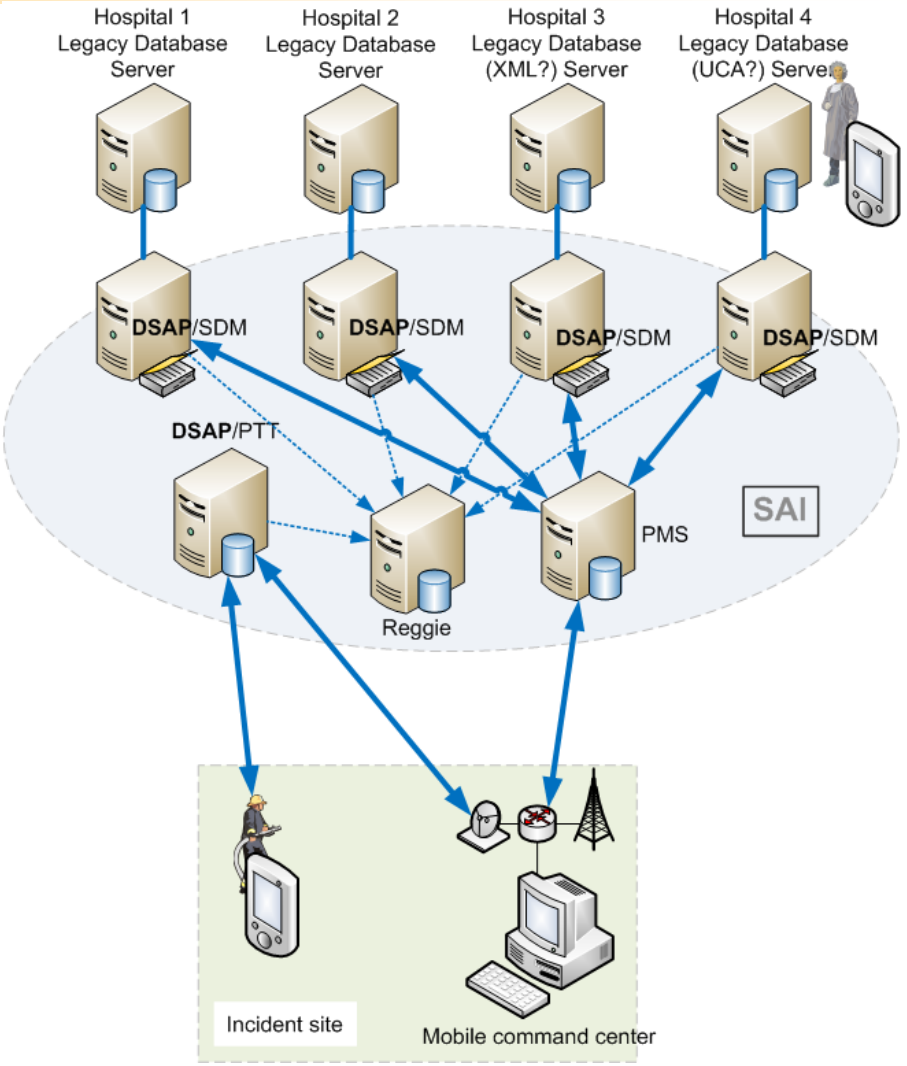
For the Review Testbed 3 workstations (WS) was used (network connection through MBR):

- **WS1** – 4 virtual machines (VMs): simulating 4 isolated Hospital Legacy DB with connected DSAP/SDM
- **WS2** – 2 VMs: Reggie + PMS
- **WS3** – Mobile Command Center

- PTT will be installed on a dedicated server
- DSAP/PTT Client will be on WS3 or on a separate (optional) WS4

Abbreviations:

- **DSAP** – Distributed Secure Agent Platform
- **PTT** – Push To Talk
- **PMS** – Process Management Subsystem
- **SDM** – Secure Docking Module
- **Reggie** – DSAP Service register



Conclusion

- Presented concepts of SAI: DSAP, PMS, RIS for distributed agent execution in trusted environment (SDS=TDS+SDM)
- Agent mobility
  - Trusted server (TS) being in the centre and mobile devices or SDMs connected to other machines being the endpoints.
  - Possible deployment in mesh topology (peer-to-peer)
    - Considered for of increased failure resilience
- Security
  - Data and code privacy and integrity
  - Encryption of all the code/data transfers
  - Agent code is signed
    - Signatures are checked before execution
  - Deployment of agent in the trusted environment using SDM
- Evaluation in model scenario on drug distribution

Thank You for Attention.

Zoltán Balogh, Emil Gatial

zoltan.balogh@savba , emil.gatial@savba.sk

Institute of Informatics
Slovak Academy of Sciences, Bratislava
(UI SAV)

This work is supported by projects SECRICOM FP7-218123, CRISIS ITMS 26240220060.

Európska únia
Európsky fond regionálneho rozvoja