UNIVERSIDAD DE MÁLAGA

Secure Software Execution with the Protected Computing Paradigm

Antonio Maña and Antonio Muñoz

gisum Research Group

Computer Science Department

E.T.S. de Ingenieros en Informática

University of Málaga

e mail: amg@lcc.uma.es

UNIVERSIDAD DE MÁLAGA

Agenda

- New Computing Models
- Protection Goals
- Protection Approaches
  - Trusted Computing
  - Protected Computing
  - Example: Agent computing
- Conclusions

UNIVERSIDAD DE MÁLAGA

General Trend

- Service Oriented Computing, Grids, Global Computing, Ubiquitous Computing, Autonomic Computing, Ambient Intelligence, ..
- From systems and applications to ecosystems
  - New computing ecosystems will offer highly distributed dynamic services in environments that will be heterogeneous, large scale and nomadic, where computing nodes will be omnipresent and communications infrastructures will be dynamically assembled.
- Providing security and trust for these ecosystems will be increasingly difficult to achieve with existing security solutions, engineering approaches and tools because of
  - heterogeneity,
  - dynamism,
  - lack of control,
  - unpredictability,
  - along with the growing demands for dependability and security.

UNIVERSIDAD DE MÁLAGA

Key Problem: lack of control

- The concepts of ***system*** and ***application*** as we know them nowadays will **disappear**,
  - evolving from static architectures with well-defined pieces of hardware, software, communication links, limits and owners,
  - to open architectures that will be sensitive, adaptive, context-aware and responsive to users' needs and habits that we will refer to as ***computing ecosystems***.
- We will be faced with pieces of software, communication infrastructures and hardware devices not under our control.
  - Thus, approaches based only on application-level or infrastructure-level security will not be sufficient

UNIVERSIDAD DE MÁLAGA

Protection goals

- Avoid reverse engineering
  - IP Protection
  - Contributes to use control
  - Contributes to integrity
- Avoid unauthorized use
- Ensure integrity
  - Detect integrity failures (modifications, …)
- Protect data and results

- In the end, TRUSTING the correct execution of the software

UNIVERSIDAD DE MÁLAGA

Protection approaches

- Well covered this morning by Mikhail Atallah
  - Encryption,
  - Obfuscation,
  - Splitting,
  - Evolvable Sw,
  - Computing with encrypted functions
  - PUFs, …
- We'll focus on
  - Trusted Computing
  - Protected Computing (a.k.a. Program splitting,…)

UNIVERSIDAD DE MÁLAGA

TC: Some public information

"For years, Bill Gates has dreamed of finding a way to make the Chinese pay for software: TC looks like being the answer to his prayer".

Ross Anderson

"A 'trusted' computer does not mean a computer that is *trustworthy*".

Bruce Schneier

" '*Treacherous computing*' is a more appropriate name, because the plan is designed to make sure your computer will systematically disobey you. In fact, it is designed to stop your computer from functioning as a general-purpose computer. Every operation may require explicit permission".

Richard M. Stallman. FSF

UNIVERSIDAD DE MÁLAGA

TC: Some public information

- **WIKIPEDIA:**
  - **Trusted computing** refers to a family of specifications from the TCG with a stated goal of making computers more secure through the use of dedicated hardware.
  - Critics, including academics, security experts, members of the free and open source software community, contend that **the overall effect** (and perhaps intent) **of trusted computing is to impose unreasonable restrictions on how people can use their computers**.

UNIVERSIDAD DE MÁLAGA

TC: Some public information

- The *Best Practices Committee* of the TCG published a document entitled *"Design, Implementation, and Usage Principles for TPM-Based Platforms"*. On page 13, the document states:

Remember Murphy's law:
if something **can** happen, it **will** happen

"TCG realizes that market forces, coercive behavior, and poor implementations can do much to weaken these principles and that **there is little the TCG organization can do to prevent a manufacturer or system designer from subverting the goals of privacy and control, if they are determined to do so**".

UNIVERSIDAD DE MÁLAGA

Protection approaches: Trusted Computing

- **Origin**

  Bill Arbaugh, Dave Farber and Jonathan Smith,

  "***A Secure and Reliable Bootstrap Architecture***"

  IEEE Symposium on Security and Privacy (1997)

- **Current Status**

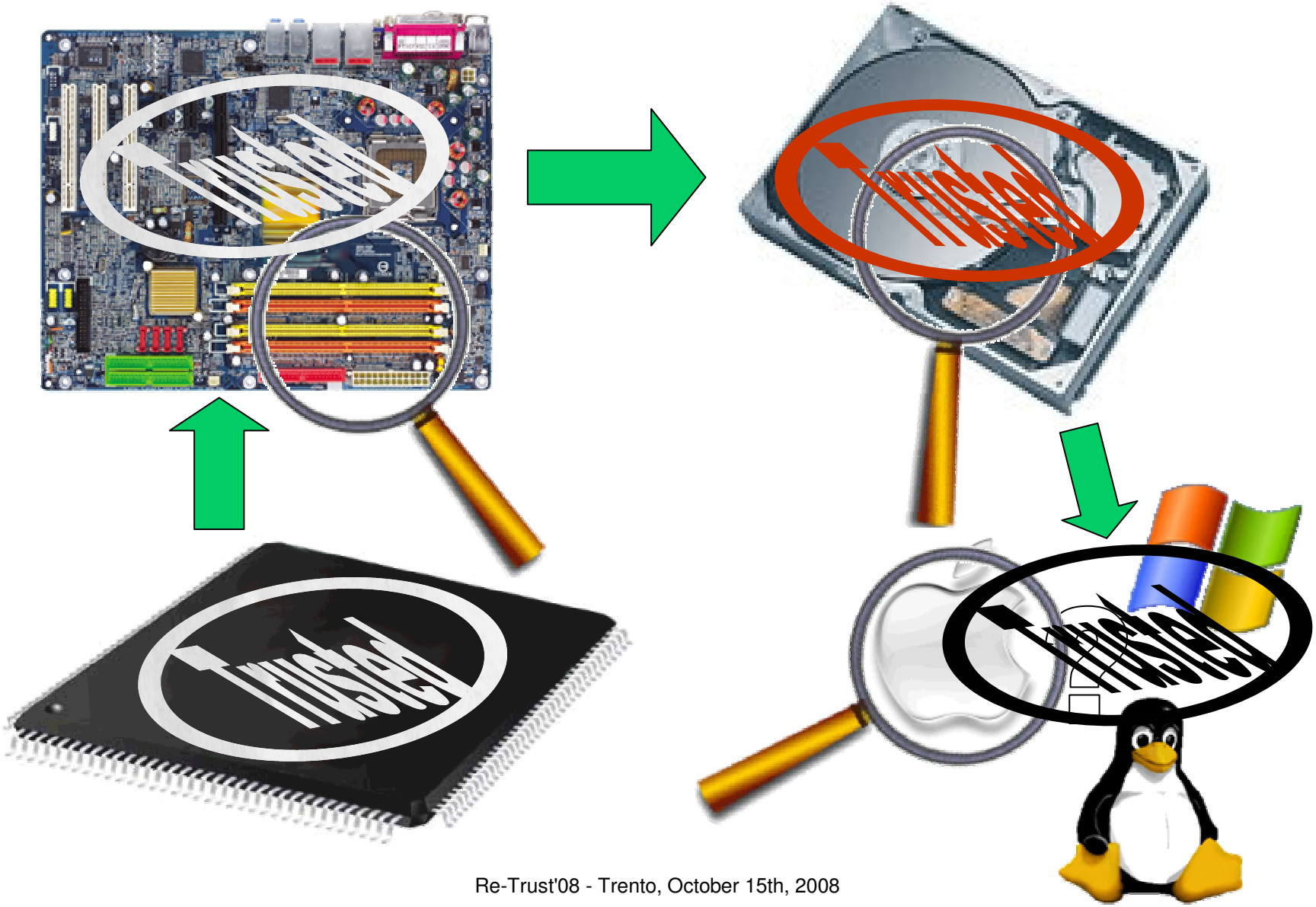
  Trusted Computing Group Specifications, Available from https://www.trustedcomputinggroup.org/specs/

UNIVERSIDAD DE MÁLAGA

Protection approaches: Trusted Computing

- Basis
  - A tamperproof hardware device is user to build a fully secured system **bottom-up**
  - The basic idea is to create a chain of **trust** between all elements in the computing system.
  - In a Trusted Computing scenario a trusted application runs exclusively on top of trusted supporting software.
  - A tamperproof hardware device analyses the BIOS of the computer and, in case it is recognized as trusted, passes control to it.
    - This process is repeated for the boot sector, the OS and the applications...

Protection approaches: Trusted Computing



Protection approaches: Trusted Computing

- More formally

QuickTime™ and a
decompressor
are needed to see this picture.

UNIVERSIDAD DE MÁLAGA

Protection approaches: Trusted Computing

- **Main Advantages:**
  - **The necessary trusted hardware is integrated in the heart of the computing system**
  - **Fully *secure* systems are possible…**
    - **well, … provided everything is perfect !**

UNIVERSIDAD DE MÁLAGA

Protection approaches: Trusted Computing

- **Main Problems:**
  - **Any failure is likely to affect the whole system**
  - **Lack of flexibility**
  - **Lack of user control**
  - **Lack of dynamism**
  - **What is a *secure* system?**
    - **Depends on the point of view !**
    - **What about conflicts of interests ?**
    - **What about tradeoffs ?**

UNIVERSIDAD DE MÁLAGA

Protection approaches: Trusted Computing

- **Other Problems:**
  - **Automated trust relationships…**
    - **Without enough control by users**
  - **Anti-competitive and anti-consumer behavior**
  - **Incorrect and malicious implementations: Impossibility of verification of the correctness of the implementation**
    - Not feasible
    - Not so desirable (by manufacturers)
      - Risk for the IPR over their designs
      - Usually marketing departments are more **trusted** than engineering departments!!

Protection approaches: Protected Computing

- **A.k.a. Program splitting…**

- **Origin**

  Schaumüller-Bichl, I. and Piller, E.

  "A Method of Software Protection Based on the Use of Smart Cards and Cryptographic Techniques" *Eurocrypt'84. 1984.*

- **Current status**

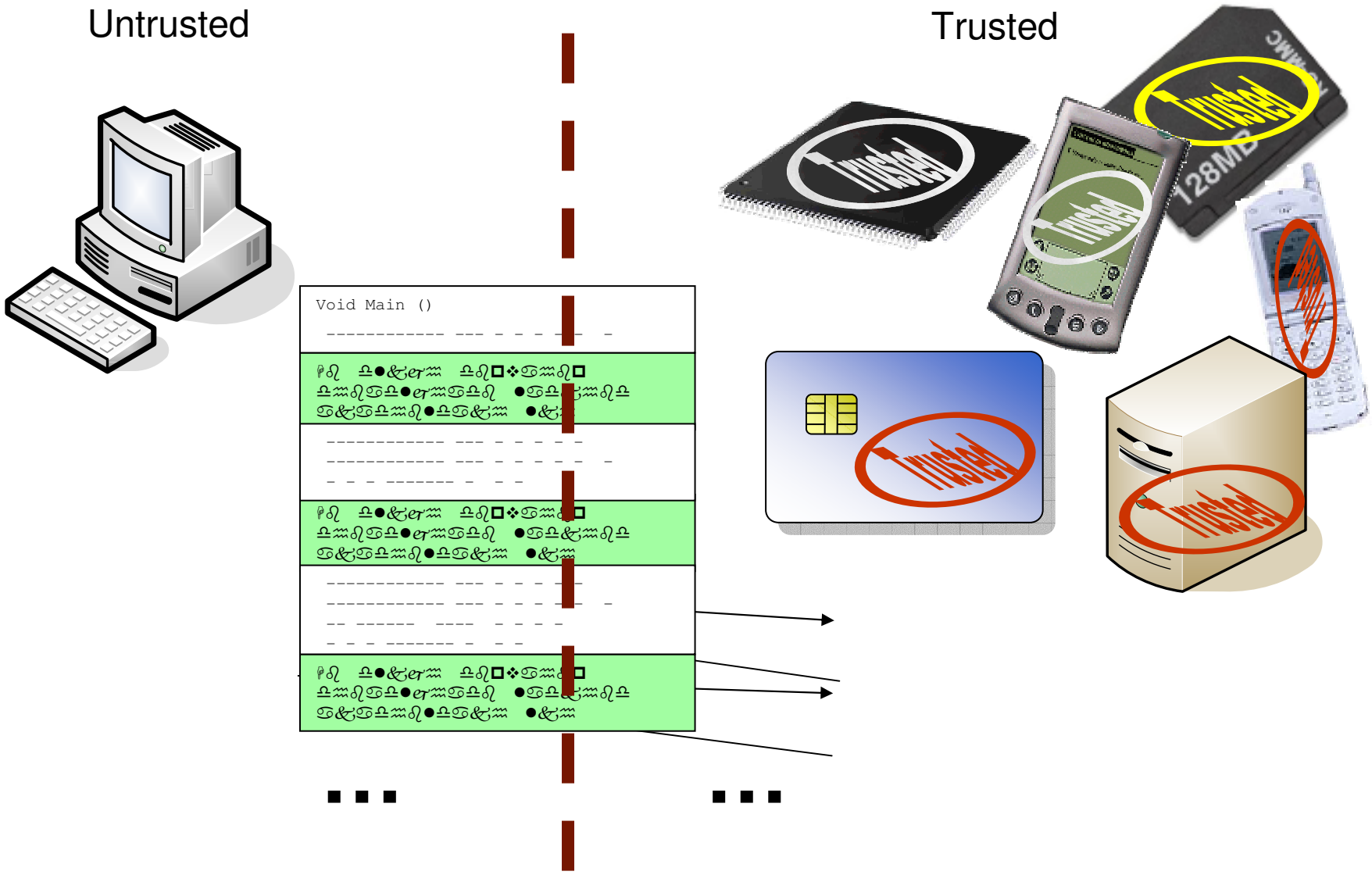
  Dvir et al, Ceccatto et al, Maña et al, Chaumette…

UNIVERSIDAD DE MÁLAGA

Protection approaches: Protected Computing

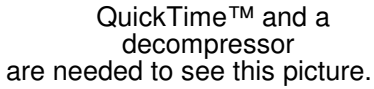
- Basis
  - Partitioning of the software elements into two or more parts. Some of the parts are executed in a secure processor, while others are executed in a normal (non-trusted) processor
  - A secure tamperproof coprocessor (not necessarily hardware) capable of executing code “on the fly” is required
  - The basic idea is to divide the application code into two mutually dependent parts.
    - The **public part** cannot be used to obtain the **protected part**
    - The **communication trace** between the parts cannot be used to obtain the protected part

Protection approaches: Protected Computing



Protection approaches: Protected Computing

- More formally



UNIVERSIDAD DE MÁLAGA

Application Example: Agent Computing

- Mobile agents: software entities with the ability to migrate from node to node in a network acting autonomously and in cooperation with other agents in order to accomplish a variety of tasks.
- Multi-agent systems (MAS) represent a promising architectural approach for building distributed Internet-based applications.
  - They can bring important benefits especially in application scenarios where highly distributed, autonomous, intelligent, self organizing and robust systems are required.
  - The high levels of autonomy and self-organization of agent systems provide excellent support for the development of systems in which dependability is essential.

UNIVERSIDAD DE MÁLAGA

Application Example: Agent Computing

- Despite the attention given to the field by the research community, the agent technology has failed to gain a wide acceptance and has been applied only in a few specific real world scenarios.
  - Security is the main issue to solve before agent technology is ready to be widely used outside the research community.
- Not enough that the agent platform provides a set of standard security mechanisms such as sandboxing, encryption and digital signatures.
- In fact, mobile agents introduce most of the security challenges of other open, distributed computing models.

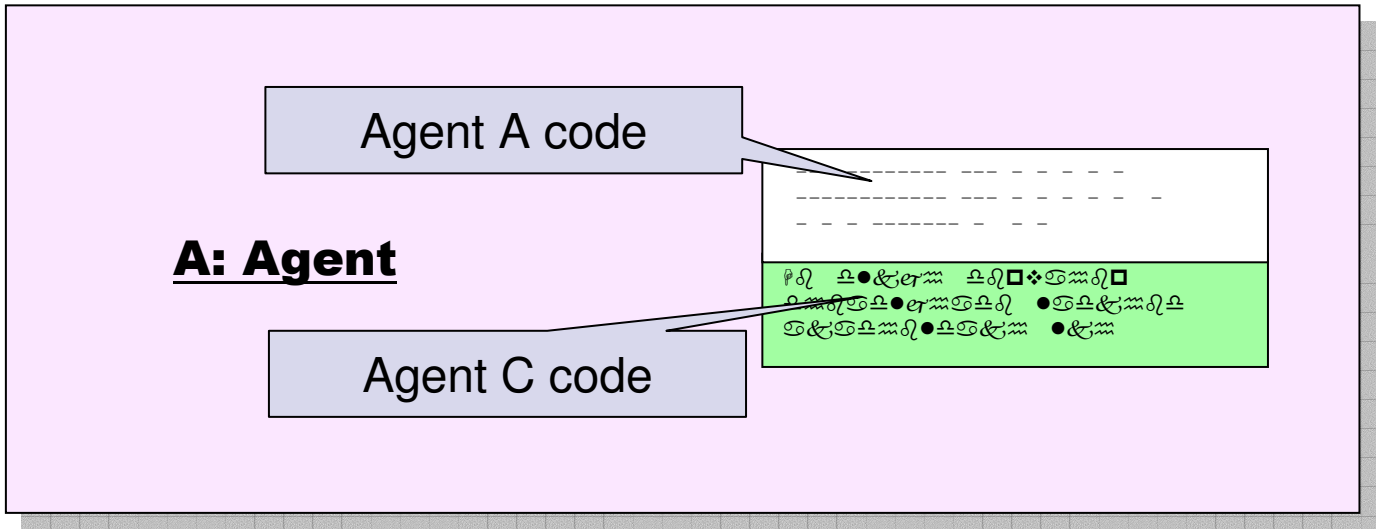
Protection approaches: Protected Computing

- Possible application without trusted hardware

QuickTime™ and a
decompressor
are needed to see this picture.

Protection approaches: Protected Computing

- Possible application without trusted hardware



Protection approaches: Protected Computing

- Possible application without trusted hardware

QuickTime™ and a
decompressor
are needed to see this picture.

Protection approaches: Protected Computing

QuickTime™ and a
decompressor
are needed to see this picture.

Protection approaches: Protected Computing

- Possible application without trusted hardware

QuickTime™ and a
decompressor
are needed to see this picture.

UNIVERSIDAD DE MÁLAGA

Protection approaches: Protected Computing

- **Main Advantages:**
  - Independent *secure* applications are possible
  - Both applications and computer owners can control their security settings
  - Different secure coprocessors can be used (even simultaneously)
    - Solutions without secure coprocessor are also possible
  - Mobile and replaceable devices such as Smart Cards can be used (*allowing different levels of protection*)
  - Low complexity and inexpensive solution
  - O.S. and HW platform agnostic
  - Applicable to open distributed computing environments

UNIVERSIDAD DE MÁLAGA

Protection approaches: Protected Computing

- **Main Problems:**
  - **Coprocessors must be fast and secure enough**
  - **Not well-suited for some applications (alone)**
  - **Coprocessors must be accessible to computing devices (may require HW modifications in some cases). Network connection is required in other cases.**
  - **Latency in communication between parts might be a problem**

UNIVERSIDAD DE MÁLAGA

Conclusions

- A trusted element is necessary in order to achieve software protection
- Current TC problems make this approach unacceptable as it is now
  - interoperability, limit to free competition, lack of owner control, lack of “assurance”, etc.
  - The general view (which we support) is that none of these problems is impossible to solve
- Protected Computing has a high potential in the new computing scenarios
- Protected Computing can be easily combined with other approaches
  - TC, Obfuscation, Computing with encrypted functions, PUFs, etc.

UNIVERSIDAD
DE MÁLAGA

Secure Software Execution with the Protected Computing Paradigm

Thanks for your attention

Questions?

Antonio Maña and Antonio Muñoz
gisum *Research Group*
Computer Science Department
E.T.S. de Ingenieros en Informática
University of Málaga
e mail: amg@lcc.uma.es