



International Academy, Research, and Industry Association

EXPERT PANEL Valencia, 2009

e-Infrastructure Security versus Anonymity and Privacy

ICNS 2009 ICAS 2009
INTENSIVE 2009



My Guests

- **Moderator:**

Petre Dini, Cisco Systems, Inc. USA /Concordia University, Canada

- **Expert Guests:**

Michael A Bauer, University of Western Ontario, Canada

Omar Cherkaoui, UQAM, Canada

Bruno Dillenseger, Orange Labs, France

Wolfgang Gentzsch, DEISA, EU

Latha Kant, Telcordia Technologies, USA

Octavio Nieto-Taladriz García, Universidad Politécnica de Madrid, Spain

Helmut Reiser, MNM-Team, Leibniz Supercomputing Centre, Germany



e-?

- e-Jacking /clickjacking!, keyjacking!
- e-Anonymity
- e-(Large Scale) Infrastructure
- e-Protection
- e-Education
- e-Trust
- e-Confidence
- e-Government and e-Citizen

Motto:

Protecting against piracy difficulty in vast area

<http://www.cnn.com/>

Sun April 12, 2009

Capt. Richard Phillips

Maersk Alabama



Security: the most recent news

Malware:

Human error led Google's malware warning system to mark all search results as bad

Patches:

Only 26 % of a survey respondents said their companies apply patch updates as soon as they are released.

Adobe:

A flaw in Adobe PDF viewing is much more dangerous...than previously thought

Worm:

A new variant of the Conflicker worm is making the rounds /to evade industry attempts to eradicate it/

Privacy: the most recent news

California DMV:

Consumer rights groups raised questions about CA DMV plan to establish fingerprint and facial-recognition systems for issuing driver's licenses

Social networks /Facebook, MySpace/:

Social networking sites agreed to a EU pact to guard against cyberbullying and online abuse /pact is voluntary/

Google:

Google released its privacy policy for its Latitude program /mobile phone users broadcasting their locations to friends/

Policy: the most recent rules

Massachusetts:

State-based revisions in data-privacy regulations; "all data and records be encrypted when possible"

e-Verify:

US stimulus bill, provision to verify workers' employment status has been stripped

California:

Online mapping tools /Google maps/ to blur images of schools, religious buildings, government offices, and medical facilities

Qs: what is the most appropriate response?

- Social response
 - Accessibility
 - User education
- Technical response
 - Security enforcement
 - Communication inspection
 - Cryptography
 - Large-scale update/pruning
- Legal response
 - Anonymity and laws
 - Trust enforcement
 - Defamation/false allegations



InfoSys 2009
Valencia, April 20 – 25, 2009



Panel Contribution

A Model for Sustainability

(and security, anonymity, and privacy are definitely part of it)

Wolfgang Gentsch

The DEISA Project & Board of Directors of OGF
gentsch at rzg.mpg.de

A Model for Sustainability (a checklist)

Reduce or eliminate the barriers in all the different areas such technology, culture, legal, economics and politics !

Especially, incorporate existing sustainability already achieved with individual components !

Therefore, the DEISA sustainability model is based on ensuring sustainability of every *individual* component:

- » Technology and infrastructure
- » Operations and services
- » Expertise
- » Communities
- » Collaborations

The DEISA Model for Sustainability

- **Technology and Infrastructure:**

- DEISA infrastructure is built on existing, proven, sustainable technology components,
- GEANT2, NRENs, Supercomputers, HPC services, global sw environment
- deliver and operate a European supercomputing infrastructure and related services

- **Operations and Services**

- benefit from the many-years operations of the individual European supercomputers centres
- orchestrated by the partners after the end of the funded project
- activities relevant for applications enabling, operation, and technologies have been developed

- **Expertise**

- tight collaboration of the expert groups in the different HPC centres
- provided in the future to the wider European HPC communities.

The DEISA Model for Sustainability



• Communities

- annual DEISA Extreme Computing Initiative (DECI)
- supporting single projects, Virtual European Communities, and international science communities across existing political boundaries

• Collaboration

- Distributed Common Production Environment (DCPE)
- Collaboration with new European and other international initiatives.
- contacts to research infrastructure projects established by the ESFRI, and the European HPC and Grid projects such as PRACE and EGEE
- European & international HPC centres; initiatives in Australia, China, Japan, Russia, US, and leading HPC projects worldwide
- Participate in evaluation and implementation of interoperability standards

• Eco-Political Landscape

- ESFRI European Strategy Forum on Research Infrastructure
- PRACE: preparing installation of a limited number of leadership-class Tier-0 supercomputers in Europe.





Thank You!
GRACIAS POR SU ATENCIÓN

Gentzsch@rzg.mpg.de



Security in embedded systems – The new challenge



Octavio Nieto-Taladriz García - nieto@die.upm.es
Universidad Politécnica de Madrid

IARIA_2009 – Valencia – April 2009



Generals,, officers, ladies and gentlemen

Thanks to the General Director of the Cátedra Alfredo Kindelán for the invitation

Embedded Systems

- **Future (and present) points to an extensive usage of Embedded Systems**
- **In embedded systems the security problems arise earlier than other equipment:**
 - o **Reduced processing capability**
 - o **Strong limitation in available resources (batteries, small memories, etc.)**
 - o **Usually working in non secure environments**
 - o **Strong activity in security breaking technologies**

Prof. Nieto-Taladriz

Universidad Politécnica de Madrid

IARIA – Valencia - April 2009



Taxonomy of security attacks

- **Functional objectives:**
 - o Privacy attacks
 - o Integrity attacks
 - o Availability attacks
- **Agents (Actives and passives):**
 - o Software attacks
 - o Physical attacks
 - o Lateral attacks – Execution time, power consumption and failure behavior

Prof. Nieto-Taladriz
Universidad Politécnica de Madrid

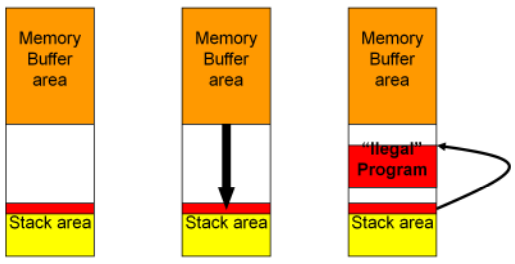
IARIA – Valencia - April 2009



Let´s present a couple of attacks to security systems

Logical attacks

- **Objective:**
 - Execute a program in the system
- **Way:**
 - Exploit the system weaknesses
- **Example:**
 - Buffer overflow



Example PSP

Countermeasures - logical attack

- **Solution: Make the programs in the correct way:**
 - o Engineering instead of art
 - o Formal techniques (verification and synthesis)

Prof. Nieto-Taladriz
Universidad Politécnica de Madrid

IARIA – Valencia - April 2009



A good programmer is a good programmer and the actual trend is to subcontract

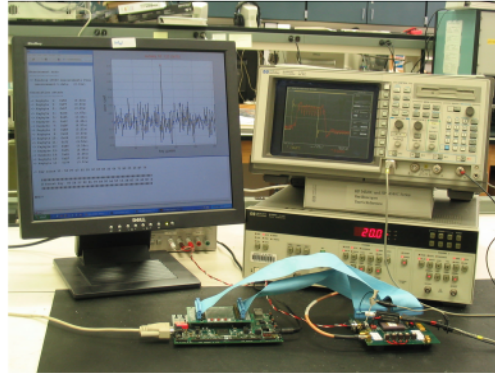
Timing analysis

- **Objective:**
 - Discover the cipher key
- **Way:**
 - Cipher algorithm execution time depends on the data
- **Variation source:**
 - Algorithm
 - Processor instruction set (ie. modular exponentiation uses processor multiplications and divisions that are in time data dependent)
 - Compiler optimization (i.e. Chinese Rest Theorem)



Differential power analysis (DPA)

- Performs an statistical analysis
- Hypothesis are confirmed by statistical correlation
- Robust against measurement inaccuracy
- Good results with high noise



i.e. 8.000 ciphers to discover a 128 bit AES key

Prof. Nieto-Taladriz
Universidad Politécnica de Madrid

IARIA – Valencia - April 2009



Countermeasures – Timing attack

- **Solution:**
 - o Timing balance
 - o Balanced technologies for Hardware
 - o Introduction of random delays

Prof. Nieto-Taladriz

Universidad Politécnica de Madrid

IARIA – Valencia - April 2009



New approaches in hardware design

Musts for security

- **The attacks look for asymmetries:**
 - SW architecture, algorithm, compiler, HW architecture, logical design , chip routing, behavior in abnormal conditions
 - Remove asymmetries implies the mixture of different knowledge domains
- **Security: A new dimension in the design process**
 - Cost, features (performances), power consumption, and security have to be considered from the beginning
- **Need to define a design flow tolerant to security attacks**

Prof. Nieto-Taladriz

Universidad Politécnica de Madrid

IARIA – Valencia - April 2009



New approaches: Confidence model

- **Trust** – Confidence degree in future behaviour, subjective and based on previous experiences
- **Reputation** – Global perception of an entity behaviour based on perceptions of other entities, basically objective
- **Data consistence test**, data is valid if:
 - **Spacial consistence** – Each node has a confidence level and an evaluation function is defined
 - **Temporal consistence**– Each node stores an historic and the evolution is checked
- **Combined trust mechanisms** (other nodes and servers on secure network)
- **Multiple agents** running over the network with various habilities and missions (node supervision, data coherence, attack detection, information elaboration, etc.)

Prof. Nieto-Taladriz

Universidad Politécnica de Madrid

IARIA – Valencia - April 2009



Example: What time is it?

The world is this room

Each one has its own time

Maybe someone has not changed the local time

Maybe someone is trying to mistake me

Complot theories?



MNM
TEAM



Fifth International Conference on Networking and Services (ICNS 09)

e-Infrastructure Security versus Anonymity and Privacy

Helmut Reiser
Leibniz Supercomputing Centre (LRZ)
Garching near Munich
Germany

Leibniz-Supercomputing Centre (LRZ)



© 2007 Foto: Christoph Rehbach



- **Computing centre for Munich Universities, Bavarian Academy of Science and other research institutes**
- **Nationwide supercomputing centre**
- **Service provider and outsourcing partner for our customers**
- **Operation of the Munich Scientific Network (MWN)**
 - ~ 120.000 customers
 - ~ 65.000 connected systems

e-Infrastructure: Grid-Projects

- D-Grid: German Initiative for e-Science Infrastructure
- Distributed European Infrastructure for Supercomputing Applications (DEISA)
- Large Hadron Collider Computing Grid (LCG)
- European Grid Initiative (EGI): Construction of EGI Organization (EGI.org)

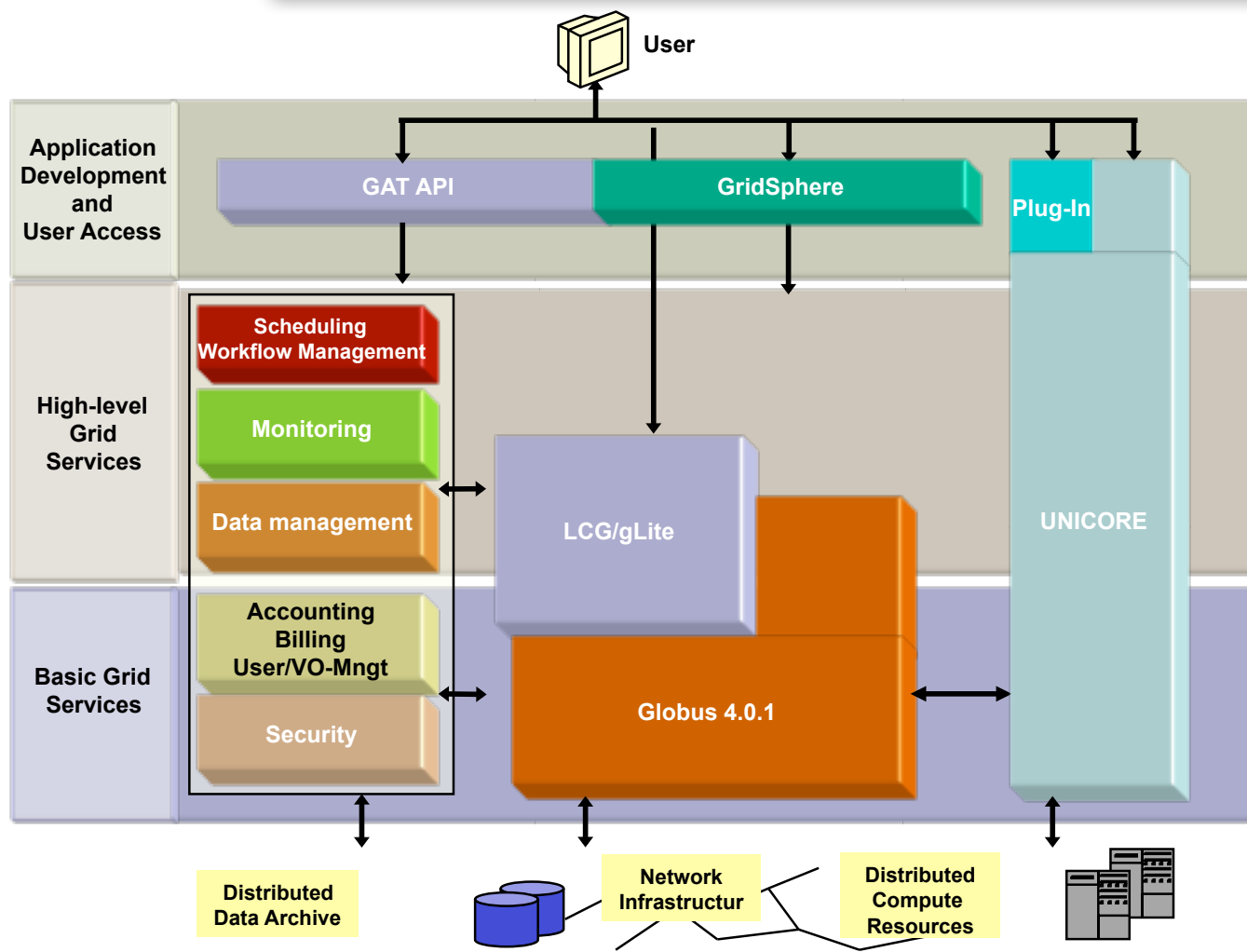




Example: D-Grid e-Infrastructure

- Building a national e-Infrastructure for research and industry
 - 2005: **D-Grid-1**: early adopters, „Services for Science“
 - 2007: **D-Grid-2**: new communities, „Service Grids“
 - 2008: **D-Grid-3**: industry cooperation, „Service Grids for research and industry“
- Funded by the German Federal Ministry of Science and Education (BMBF)
 - **D-Grid-1**: 25 MEuro > 100 Orgs. > 200 researchers
 - **D-Grid-2**: 30 MEuro > 100 addl. Orgs > 200 addl. researchers and industry
 - **D-Grid-3**: 20 MEuro > 40 addl. Orgs > 30 new industrial partners
- Aim: Sustainable production grid infrastructure after end of funding
- Integration of new communities
- Evaluating business models for grid services

D-Grid: Multi-Middleware





D-Grid Resource Providers: Locations



- Core Sites (8)
- Federal Groups (8)
- Community Groups (6)
- further Resource Providers (20)

Science Projects



German **Astronomy** Community Grid



Collaborative **Climate** Community Grid



High Energy Physics



Medical Science



Engineering

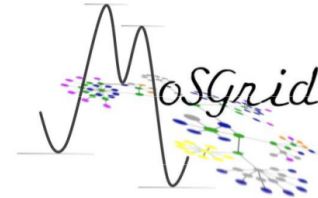


Humanities

Industrial/Commercial Projects



Aviation



Molecular Simulation



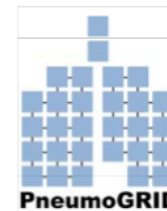
Building



Metal Processing



Automotive



Medicine



Financial Business



Geo Data (GIS)



Product Development



Medicine



Photovoltaics

Logistics

Media Tech.

Plasma Tech.

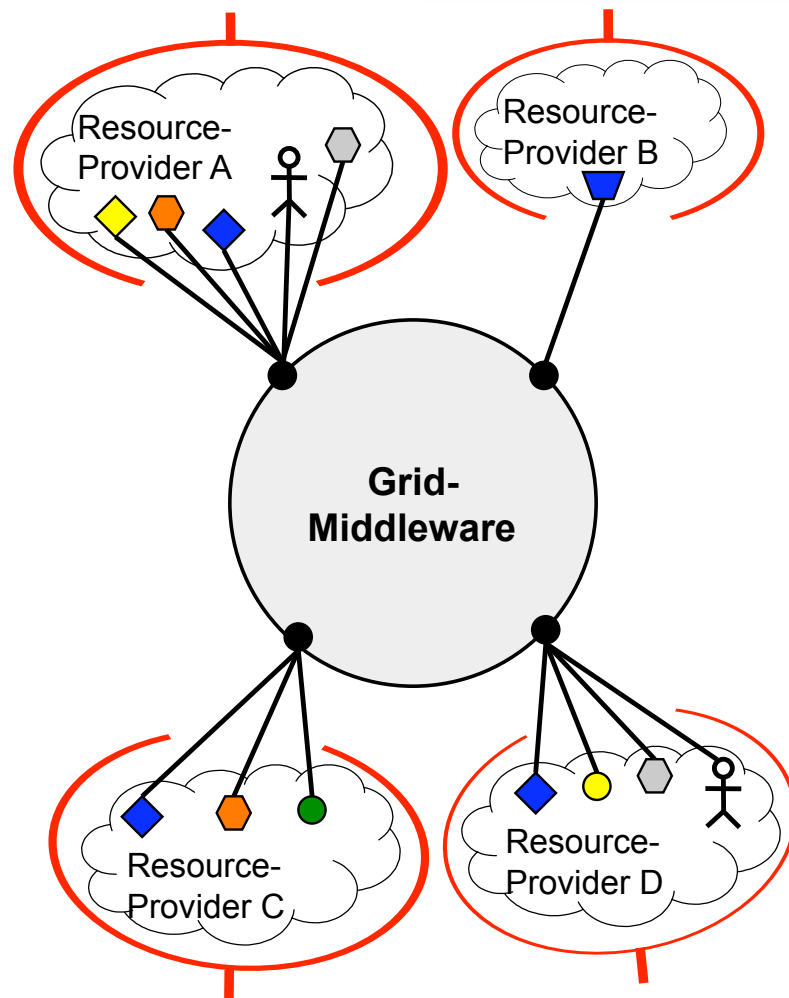
.....

Security, Anonymity, Privacy: Open Questions coming out of Praxis



- Security:
Federated cooperative Grid intrusion detection system
- Anonymity:
Data regulation laws for medical surveys
- Privacy:
Automotive and engineering: Privacy during resource usage

Federated cooperative Grid IDS



- Independent islands of security and IDS tools
 - Security focus solely on local organization
 - Attacks on single organization spread easily the whole Grid
 - Idea: Federated cooperative use of data to establish a Grid IDS
 - Overlapping different organizations
 - Autonomy of partners
 - User/VO specific views
 - Data privacy concept needed
- ➔ New D-Grid Project



Anonymity: Data regulation laws for medical surveys



- Strong privacy protection laws for multi-center surveys
 - Patient can exercise rights:
 - Data usage only with patients explicit consent
 - Consent is revokable at any time
 - Consent is partly revokable, regarding:
 - Restrict amount of data
 - Persons or institutions allowed / disallowed to use data
 - Deletion of data with documented and objective evidence
 - Objective evidence about systems which stored or operated data, persons which had access to data and when and how did they use it
- ➔ None of these requirements is satisfiable in today's Grids




Privacy during Resource Usage

- Competing automotive companies work on grid resources
 - Information about resource usage must be hidden
 - Who is using?
 - Which jobs are executed?
 - How many resources (CPU,memory, visualization,...) are used?
 - Total privacy is hard to achieve
 - Resource or OS information is hard to hide
 - e.g. Process list (ps)
 - Small number of large jobs may indicate crash test simulation (late production phase)
 - Lots of small jobs may indicate design study (early production phase)
- ➔Virtualization as a solution?

EXPERT PANEL

Valencia, 2009



e-Infrastructure Security versus Anonymity and Privacy

**Dr. Latha Kant
Telcordia Technologies
Director & Senior Scientist
Mobile Networking Research
1 Telcordia Drive, Piscataway, NJ 08854
lkant@research.telcordia.com**

April 20, 2009

■ ■ ■ Thoughts on E-Transactions, Security, Anonymity & Privacy

- E-Transactions – have almost become a ‘norm’
 - E.g., payments (gas, electricity, water, credit-card, ...), tuition payments, on-line reservations,
 - Immigration in many countries have initiated an ‘e-verify’ system to expedite processing, E-Z pass (at airports) that cuts down on time!
- Question next becomes how much are people willing to pay for convenience?
- How much “Privacy” does one actually have?
 - E.g., Fingerprint info already in database (for permanent residency and citizenship purposes); – so what extra ‘privacy break’ does it have when associated with e-Security
 - Credit card bureaus (with fingerprinting) and customers’ credit history – have tons of information which may even surprise the individual itself!
- Can one have different levels of privacy and anonymity for web-transactions?
 - E.g., The web “Avatar” concept (i.e., 2nd Life!)

■ ■ ■ Thoughts on E-Transactions, Security, Anonymity & Privacy - continued

Security –

- Can have varying levels of security – but canonical tradeoffs exist
- A very important problem is
 - Identity Theft

Should focus our effort on risk mitigation in the presence of e-transactions (and invariably in the presence of security and anonymity threats)

Bottom line: “Where there is a will (to break in), there is a way!”

- Look at this whole problem in holistic sense of ‘birth-death’ processes
 - As people want more convenience and more security and anonymity all simultaneously, there is the need for more work, more unsolved problems!

Round table about security in the e-infrastructure

What about autonomics?

Bruno Dillenseger, Orange Labs

ICAS round table, 20th April 2009

bruno.dillenseger@orange-ftgroup.com



Autonomics and the e-infrastructure

- Autonomics approach consists of taking advantage on computing and network power to enable the self-management of the e-infrastructure.
 - autonomic computing, networking, communications
 - self-configuration, self-repair, self-protection, self-optimization
- The autonomics vision starts from the consideration that the complexity of the e-infrastructure is such that its management is now reaching (overwhelming?) administrators capabilities.



What about the safe usage of the e-infrastructure?

→ Up to now, autonomics' works in the field of security/safety typically address the security of the e-infrastructure itself

- self-protection
- self-healing

→ But what about enforcing a safe usage?

- are laws sufficient and practically applicable?
 - ◆ technologies and their bad usage are always (at least one) step forward laws
 - ◆ laws may be hard to be fairly enforced for technical and ethical reasons
- is the autonomic approach relevant?



Autonomics and the safe usage of the e-infrastructure

- Why an “autonomics” approach to enforce safe usage?
 - the full understanding and control/ruling of the e-infrastructure usage is
 - ◆ not possible (complex, open, large scale, human non determinism)
 - ◆ and possibly not desirable (to invent new usages, to avoid threats to privacy and democracy)
 - a typical “autonomics” approach would consist in having a self-managed e-infrastructure detecting bad usages and reacting

- Big challenges to invent a new self-* property
 - observing and detecting suspicious usages/contents
 - analyze to confirm bad usages/contents detection
 - react in a fair but efficient manner