Trustworthy & Secure
Future Internet

Fabio Martinelli
Outline

• Past
  • The Evolution
• Present
  • The Context
  • The Vision
  • The Activities
• Future
  • The Prospective
Our History
Ten years of life

Formal institution of the research group

Separation of the Web technologies group
The initial research themes

• Digital signature
• Certification authority
• Model Checking
• Biometry
• ……. 
The evolution

- Significant cultural and numerical growth
- Widening of the research areas and expertise
- Increment of scientific production and technological one as well as of the capability of funding acquisition
- Balance among foundational research, innovation and technology development
- Very good international visibility
The Present
Security research: The context

• New scientific and technological problems
  • From complex distributed service systems to Future Internet Services

• Technology changes
  • Security needs to evolve with technology

• Possibly new horizons
  • Cyber Security plans for national security (e.g. see US)
  • From ICT security to ICT for security
  • Since FP7, new research theme called Security (1000 ME)
### People (13)

<table>
<thead>
<tr>
<th>Category</th>
<th>Permanent staff (2)</th>
<th>Temporary staff (3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Researchers and technologists</td>
<td>Fabio Martinelli, Anna Vaccarelli</td>
<td>Ilaria Matteucci, Paolo Mori, Marinella Petrocchi</td>
</tr>
<tr>
<td>1 Post Doc</td>
<td>Artsiom Yautsiukhin</td>
<td></td>
</tr>
<tr>
<td>3 Ph.D. Students</td>
<td>Gabriele Costa, Leanid Krautsevich, Alexander Lazouski</td>
<td></td>
</tr>
<tr>
<td>2 SW Eng.</td>
<td>Maurizio Colombo, Francesco Latorre</td>
<td></td>
</tr>
<tr>
<td>1 Research Associate</td>
<td>Stefano Bistarelli</td>
<td></td>
</tr>
<tr>
<td>1 Administration EU projects</td>
<td>Lucia Ghelardi</td>
<td></td>
</tr>
</tbody>
</table>
Group Features

• Active research group with well motivated people

• Balance among:
  • Fundamental/applied research (i)
  • Software Products (ii)
  • Service provision (iii)

• Very good capability of funding acquisition
Three Pillars

- KNOWLEDGE
- PROJECTS
- VISIBILITY
Research Areas

- **Formal methods** for the design and analysis of security systems for ICT and critical infrastructures
- **Access and usage control** in distributed systems (GRID – Web Services)
- **Secure communication** and applications for pervasive computing
- **Mobile phones and applications security**
  - Including parental control
- **Identity and trust management** for dynamic coalitions and social networks
- **Security for e-goverment**
  - Including e-voting protocols
- **Document security and digital signatures**
- **Strong authentication mechanisms and biometry**
- …
Software produced

- Software for the analysis of security protocols and architectures
- Middleware for access and usage control in (GRID/Web services)
- Biometry and strong authentication methods
- Mobile devices and applications security (smart phones, PDAs)
  - Including software for parental control on mobile devices
- Digital signature, certification authorities
  - SignIT software sold to INFOCAMERE
- ...
Events organized

- ... 

2008
- 1st International Symposium on Information Governance (ISGI-G08)
- 6th International research school on Foundations of Security Analysis and Design (FOSAD08)
- 4th International Workshop In Security and Trust management (STM08)
- 5th International Workshop on Formal Aspects in Security and trust (FAST 2008)
- EC-ERCIM Strategic Seminar on Secure Software Engineering
- NSS (since 2002)

2009
- EuroCAT 2009 - Combining Context-Awareness with Trust, Security, and Privacy
- In Bio We Trust 2009 - Bio-inspired Trust Management for Information Systems
- 9th International research school on Foundations of Security Analysis and Design (FOSAD09)
- 6th European PKI Workshop (EUROPKI 2009)
- 12th Information Security Conference (ISC 2009)

2010
- 10th International research school on Foundations of Security Analysis and Design (FOSAD10)
- International Symposium on Engineering Secure Software and Systems ESSoS 10
- ...
WG and Associations

- ERCIM Security and Trust Management
  - (Fabio Martinelli: Chair)
- IFIP WG on Trust Management
  - (Fabio Martinelli: Member of the Executive Board)
- NESSI TSD WG
- Think-Trust EU Coordinated action
- INCO-Trust EU Coordinated action
- IMG-S (FP 7 Security Theme)
- Assosecurity
  - (Anna Vaccarelli – Vicepresident)
- …
Consultancy for EU and European Countries

- Experts in consultation meetings, road mapping activities, project reviewing for
  - Future and Emerging Technologies
  - ICT Security
    - FIA Trust and security
- Evaluators of project and research programs for:
  - Czech Republic, France, Germany, Iceland, Norway, Netherlands.
Focus on ERCIM

• The European Research Consortium in Informatics and Mathematics (ERCIM) has a member organization in each country
  • CNR is member for Italy
• ERCIM has several technical WGs
• IIT Security group promoted and manage the Security e Trust Management WG (STM)
  • 60 european researchers
  • Major corporates in ICT have a rappresentative in the WG
    • Microsoft, HP, IBM, SAP, Siemens, ATOS, BT, …
External funding
(2007-2012)
Provisional results for 2009

<table>
<thead>
<tr>
<th>Risultati</th>
<th>Numero</th>
</tr>
</thead>
<tbody>
<tr>
<td>Books</td>
<td>2</td>
</tr>
<tr>
<td>Articles on Journals</td>
<td>5</td>
</tr>
<tr>
<td>Papers in Conference/ workshop proc.</td>
<td>10</td>
</tr>
<tr>
<td>Book chapters</td>
<td>2</td>
</tr>
<tr>
<td>Guest editor for special journal issues</td>
<td>1</td>
</tr>
<tr>
<td>Patents</td>
<td>0</td>
</tr>
<tr>
<td>Memberships in Int. Journal Boards</td>
<td>2</td>
</tr>
<tr>
<td>Relevant duties/ memberships in Int. WGs</td>
<td>7</td>
</tr>
<tr>
<td>Conference/ Workshop organization</td>
<td>5</td>
</tr>
<tr>
<td>Program Committee membership</td>
<td>28</td>
</tr>
<tr>
<td>Software packages</td>
<td>3</td>
</tr>
<tr>
<td>Ph.D. Students</td>
<td>3</td>
</tr>
</tbody>
</table>
International Projects

1. EU Project FP7-ICT-FET CONNECT (Emergent Connector for Eternal Software Intensive Networked Systems)
2. EU project FP7-ICT CONSEQUENCE Context-aware data-centric information sharing
3. EU project FP6-FET BIONETS: "BIOlogically-inspired autonomic NETworks and Services"
4. EU project FP6-FET SENSORIA: “Software Engineering for Service-Oriented Overlay Computers"
6. EU project FP6-IST-27004 S3MS: “Secure Software and Services for Mobile Systems”
7. DOCOMO “Run-time enforcement mechanisms for smart phones”
National Projects

1. MIUR: Progetto Sybilla “Formal Methods System Biology”
2. Progettazione e realizzazione di soluzioni di autenticazione forte - TAI
3. Access control for DDS - SSI
4. Mobile security "EAP SIM" - VPTech/TIM
5. Distributed systems security - Omnitech
6. Azione 1.7.1 DOCUP Regione Toscana TEC-MOB
7. Azione 1.7.1 DOCUP Regione Toscana EMOTION
8. Comune di Livorno: Consultancy on information security
9. "Secure electronic transactions" - EURID (Registro ".eu") e Registro .it
10. Trust and security in mobile devices (XML digital signature) – Infocamere
11. Visual Support to cultural heritage Interactive access in Tuscany (VISITO) – newly funded by the Tuscany Region
Focus on the EU projects
EU projects/ Research Areas

- Bionets
- S3MS
- GRIDTrust
- Consequence
- Connect
- Sensoria

- ID and TRUST
- Usage Control
- Secure communication
- Data Protection
- Formal methods for modelling, analysis, and synthesis

- Sensors
- Mobile Devices
- PC
- ... Grid / Web
EU Project FP7-FET CONNECT

• Emergent Connector for Eternal Software Intensive Networked Systems
  • Focus on software evolution
• AS IIT, we cover the security aspects:
  • Automated synthesis of security connectors
  • Usage of security contracts
  • Privacy policies for connectors
EU project FP6-FET BIONETS

- BIOlogically-inspired autonomic NETworks and Services
- We work on bio-inspired models of computation
  - Formal semantics for bio-inspired programming models
  - Self-protection mechanisms
  - Trust as a social control mechanism
EU project FP6-FET SENSORIA

• Software Engineering for Service-Oriented Overlay Computers

• We focus on formal aspects of security and trust for services
  • We develop techniques by using formal methods as temporal logic, process algebras
  • Inclusion of trust features in languages for the specification of IT-services
EU project FP6-IST S3MS

S3MS Security of Software and Service for Mobile Systems

- Secure Software and Service for Mobile Systems
- The idea is to allow the secure download of third party Java applications on mobile devices
  - Security contracts
  - Local user policies
- As IIT, we work on the synthesis of monitors for run-time security policy enforcement
Bilateral project with DOCOMO

• Follow up S3MS

• On the right side the “Japanese” description of the project
EU project FP7-ICT CONSEQUENCE

• Context-aware data-centric information sharing
  • Focus on protection of disseminated information regulated by data sharing agreements:
  • Define an architecture within a framework
    ▪ to enable dynamic management policies
    ▪ based on agreements that
    ▪ ensure end-to-end secure protection
    ▪ of data-centric information.

• We work on the formal specification and verification of the agreements
EU project FP6-1ST GRIDtrust

• Trust and Security for Next Generation Grids
  • Focus on model-based techniques for security policy enforcement in distributed systems

• We work on usage control mechanism
  • The concept is an extension of the usual notion of access control
  • We integrate trust and reputation mechanisms into the control phases
An example of research path on mobile device security

- Expertise on mobile devices
- Development of a real application for TIM
- Extension of the ideas for the EU project S3MS
- Successful completion and follow up project funded by DOCOMO
- Application of the framework for parental control. Further scientific publications and interest from the media, e.g. TV and national newspapers
The Future: Prospective
Mid Term (2-4 years)

• Scientific: Good
• Funding: Good
  • Till 2012 same level without even corrective actions (just with current projects!)
  • It is however reasonable to immagine even increasing project income
Long Term (4-8 years)

• We aim at a significant **growth**
  • the international context (research areas and funding possibilities) would allow it

• It is necessary an extension of the research areas
  • Adherence to the mutation of current research areas
  • Opening of research lines in new areas (and thus visibility)
Some of the Necessary Steps
Things under our control

- **Strengthening**
  - Increase the competence in the current research areas and investigate others (e.g. global security) where synergies are possible
  - Formation activities (Master/Ph.D. students)
  - Continue regular funding acquisition
  - Foster contacts with public and local administrations
  - Research divulgation (also on media)
Things that are NOT under our control

• Need for permanent staff
  • At least 3
    • Currently, we have 3 temporary researchers with at least 5 years in the group (one 9!)
  • The issue could be solved (for the moment) if:
    • stabilization process is completed
    • additional resources as planned are effectively distributed

Remind our director slides!
Conclusion

• An active and solid research group with wide R&D competencies in security

• Significant growth and results achieved since its creation

• Very good prospectives for the future