Cyber Security Research Roadmap, 
Decision Support System for addressing 
Privacy Concerns, & Maritime Border Protection

Stelios C. A. Thomopoulos, PhD - scat@iit.demokritos.gr

Director of Institute of Informatics & Telecommunications - NCSRD 
Director of Research & Head of Integrated Systems Laboratory

http://isl.iit.demokritos.gr

in collaboration with ISL Research Associates:

Olga E. Segou, PhD - osegou@iit.demokritos.gr
Dimitris M. Kyriazanos, PhD - dkyri@iit.demokritos.gr
Sotirios Kanellopoulos, PhD - skanellopoulos@iit.demokritos.gr
Dionysis Motos, Vassilis Lampropoulos, Chris Margonis, 
Kostantinos Dimitros, and Anastassios Bravakis
Identifying areas of **Cyber Security & Privacy Research**
and potential impact and potential for adoption

- Presenting findings and experiences from our research experience on Digital Security, Privacy, and Maritime Surveillance

1. Risk assessment methodology for ranking of research topics
   - CyberROAD project FP7-2013-607642
   - Why Cyber Security Matters
   - Compiling a Cyber Security Research Roadmap

2. Public Perception of Security and Privacy and its effect on adoption of security technologies
   - PACT project FP7-2012-285635
   - Citizen Perception of Security and Privacy
   - Privacy Impact Assessments and their use on Decision Support

3. Maritime Boarder Surveillance
   - OCULUS Sea™ I2C2 System developed within PERSEUS by NCSRD

scat@iit.demokritos.gr
Identifying research topics in a massive and ever-changing field – Cyber Security

- Cyber Security research is a top EU priority
  - New threats emerge every day

- CyberROAD is a 24-month project funded by the European Commission
  - Coordinated by the U of Cagliari (IT) with participation of 20 partners across Europe

- CyberROAD presents a risk assessment methodology for ranking cyber security research topics taking into account:
  - cyber crime and cyber terrorism, targeting organizations, the public or critical infrastructures
  - Emerging, cutting-edge technologies and commercial trends
  - Ethical and Legal implications and gaps in current regulations
  - Currently set EU policies on the development of Transport, Security etc.

- CyberROAD will deliver a Roadmap for Cyber Security research
Research topic ranking methodology

- **Research topics** are associated with threats, assets to protect and a general area of research.

- Stakeholder and expert input leads to **different ranking based on risk types** (e.g. financial, health & safety etc.)

- This is an on-going research effort, find out more at: [http://www.cyberroad-project.eu/en/](http://www.cyberroad-project.eu/en/)
Example: topics for a Transport-based scenario

- **RESEARCH TOPIC 1**: ICT tools to protect from intrusion in railway command and control systems to interrupt circulation

- **RESEARCH TOPIC 2**: ICT tools to protect from intrusion into social media to generate panic in railway stations with false information

- The threat associated to RT1 is the intrusion in the command and control system affecting the following main assets: the quality of service.

- The threat associated to RT2 is the intrusion in social media affecting the following main asset to protect: the railway passengers.

- Example risk categories: financial risk, health & safety
Adoption of a security technology - PRIVACY

- Multiple security solutions are available on the market and new solutions designed every day, in order to address current research gaps.

- Many factors affect the adoption of a security technology, e.g. cost effectiveness.

- Profound lack of research on the effects of Trust and Privacy affecting the adoption of a security technology:
  - How can we improve adoption of new technologies based on a good understanding of public perception of privacy, trust and security?
  - How can we optimize financial investment on current security technologies and supporting the decision making process?
Studying Public Perception of Privacy and Security

- **PACT project (FP7-2012-285635)**: The PACT DSS aims to support decision process for *security technologies investments* and assessment of impact in terms of *privacy, ethics, social acceptance and public perception*, assisting the decision process of experts through efficient visualisation and user-DSS interaction based on PACT’s *theoretical and empirical findings*.

- Decision Support and not Decision Making

- Required context data is retrieved from the **System Knowledge Base**, fed into the **decision support and decision-tree process** and presented accordingly to the user through multiple visualisation modes as rational arguments towards supporting the user’s decision process.

- System Knowledge **Base is constructed by an EU-wide survey, across 27 EU member states with approximately 27,000 participants**
A brief technical overview

- PACT DSS is an Online Software Tool
- Application Logic offering personalised decision support (user-specified use case scenario) and assistance through multiple modes
- An extensible data model, easily encapsulating empirical and theoretical data
Example: Transport Scenario

- Security measures assessed by PACT
  - Use of CCTV (recording, storage, processing of data, access by Law enforcement etc.)
  - Security Personnel (private contractor or law enforcement etc.)
  - Security Screening (random searches or body scanning etc.)

- Data and related analysis can be found on PACT reports 4.1 and 4.2. For more information, visit:
  - [http://www.projectpact.eu](http://www.projectpact.eu)
Respondents’ preferences for the types of CCTV presented are in the following order: advanced CCTVs that can detect faces are most preferred, followed by CCTV that can detect abandoned bags, CCTV that can recognise suspicious movements of people, and standard CCTVs which work as television.

However the preferences for the CCTV cameras differ in eleven countries. While all types of CCTV cameras are still preferred over no cameras in these countries, the magnitude of preference changes for each of them.
Respondents are averse to going through physical security checks.

Respondents are more averse to physical searches which include a bag search than going through a full body scanner or metal detector.

However, the disinclination towards the physical check involving metal detector/full body scanner compared to no physical checks becomes statistically insignificant after controlling for country and socio-economic variables.

Respondents in more than half the EU27 countries exhibit significantly different preferences for security checks.
In most EU27 countries, respondents prefer having security personnel at the stations relative to the reference level of “No security personnel”.

Unarmed police are the most preferred, followed by unarmed security personnel employed by a private company and armed police; armed security personnel employed by a private company are least preferred.

Thus, in general, unarmed security personnel are preferred over the armed personnel and police are preferred over the security personnel employed by a private company.
Tangible and Personalized Outputs

- Selected Context and use case elements
- Selected technologies under investigation
  - Consolidated selected privacy risks and corresponding threat metrics
  - Prioritization and assessment of applicable privacy controls
  - Comparison of decision paths and quantitative metrics
- Selection of relevant empirical inferences and societal impact references

The PACT Impact Assessment Report
Look and Feel

https://pact.atosresearch.eu/gs-rest-service-0.2.0/

scat@iit.demokritos.gr
Oculus Sea™ : An Integrated Maritime Surveillance Platform

Dr. Stelios C. A. Thomopoulos, Institute Director & Director of Research, Head of Integrated Systems Laboratory

Dr. Sotirios Kanellopoulos, Senior Research Associate, and

Dionysis Motos, Vassilis Lampropoulos, Chris Margonis, Kostantinos Dimitros, Research Associates

Research supported by:
the European Commission under the FP-7 funded research project

and the General Secretariat of Research in Greece
Overview

- **OCULUS Sea™ animated video**
- CC Node reference Architecture & Major components
- Interoperability with 3rd systems
- System configuration
- Way ahead
- References-Acknowledgements
- Contacts


scat@iit.demokritos.gr
Conclusions

- Multiple research topics and security technologies available

- It is possible to extend current knowledge to provide a roadmap for cyber security research and also provide a methodology for assessing privacy impact and potential for adaption by the public

- For additional information, we would be happy to discuss with you and demonstrate the PACT DSS tool for you:
  - Additional use case scenarios: Internet-based surveillance and eHealth data management

- A full scale demonstration of PERSEUS is available by contacting Dr. Thomopoulos by emailing to: scat@iit.demokritos.gr
THANK YOU FOR YOUR ATTENTION

Stelios C. A. Thomopoulos, PhD

in collaboration with:

Olga E. Segou, PhD
Dimitris M. Kyriaizanos, PhD
Anastassios Bravakis

National Center for Scientific Research “Demokritos”

E-mail: {scat, dkyri,osegou,abravakis}@iit.demokritos.gr

Research supported by:
APPENDIX

- Additional explanatory slides
Privacy, Ethics and Social Impact Assessment (i)

- PACT DSS guides the user through assessing the privacy, ethics and social impact of selected technologies within the specific context.

- Select and assess privacy risks through a provided selection according to Privacy Type: Privacy of Personal Information, Privacy of the Person, Privacy of Personal Behaviour, Privacy of Personal Communications (UK’s Information Commissioner Officer PIA Handbook).

- Assess contribution to Privacy Targets according to European Data Protection Directive.

- Assess Privacy risks connected with Privacy Targets.
  - Create the consolidated Privacy Threat Index (PTI).
Privacy, Ethics and Social Impact Assessment (ii)

- Assess relevant empirical results and inferences related to the societal perception and acceptance
  - An empirical knowledge database including survey results from EU-27 on the perception of privacy and security in Health, Internet and Transport context
  - As per the combined Context and personalised/customizable parameters

- Calculate Privacy Threat Index Metrics and explore extracted alternative technologies decision paths in corresponding Decision Trees

- Assess how the case conforms to the 8 basic privacy services identified by the OASIS Privacy Management Reference Model (PMRM), by (i) marking controls as Mandatory, (ii) providing ratings: Sufficient Controls, Partially Sufficient Controls, Missing/Insufficient Controls, and (iii) assessment comments including a prioritisation flag for each control
DSS Success criteria, Evaluation and Validation

- PACT DSS aims at the following user-perspective success criteria:
  - Reduction on average decision process time (including collaboration with other users)
  - Improving decision specific context visibility & access to necessary knowledge for related security technologies decision making
  - Reduction on average time for compiling a privacy impact assessment report
  - Convenience and acceptance of the produced PACT impact assessment report
  - Usability & User friendliness
  - Cost effectiveness (value for money)
Which of the following options would you prefer for your train or underground journey?

<table>
<thead>
<tr>
<th>Description</th>
<th>Option A</th>
<th>Option B</th>
<th>Option C</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCTV cameras</td>
<td>Advanced CCTV that can recognise faces</td>
<td>Advanced CCTV that can detect abandoned bags</td>
<td>None of these. I would prefer not to make this journey by train or underground</td>
</tr>
<tr>
<td>Type of CCTV Camera</td>
<td>CCTV information stored for 7 days</td>
<td>CCTV information stored for 15 days</td>
<td></td>
</tr>
<tr>
<td>How long CCTV Camera information is stored</td>
<td>All European police departments have access to the camera information</td>
<td>All European police departments have access to the camera information</td>
<td></td>
</tr>
<tr>
<td>Who can access CCTV Camera information</td>
<td>Unarmed security personnel employed by a private company</td>
<td>Unarmed police</td>
<td></td>
</tr>
<tr>
<td>Security personnel at the station</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security checks at the station</td>
<td>People randomly selected for physical search and bag check</td>
<td>No physical security checks</td>
<td></td>
</tr>
<tr>
<td>Type of security checks</td>
<td>10 seconds</td>
<td>No delay</td>
<td></td>
</tr>
<tr>
<td>Time to go through security checks</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security surcharge on top of ticket cost</td>
<td>Security surcharge of £ 0.43</td>
<td>Security surcharge of £ 0.04</td>
<td></td>
</tr>
<tr>
<td>Number</td>
<td>Research hypotheses</td>
<td>Findings</td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>---------------------</td>
<td>----------</td>
<td></td>
</tr>
<tr>
<td>H1.1</td>
<td>Respondents prefer having CCTV cameras when travelling by metro/train.</td>
<td>Accept: all</td>
<td></td>
</tr>
</tbody>
</table>
| H1.2   | When CCTV is present, respondents prefer cameras with additional capabilities (e.g. abandoned bag detection and face recognition). | Reject: Sweden  
Accept: others |
| H1.3   | When CCTV is present, respondents prefer settings with CCTV footage only used in real time versus those in which the footage is stored for a specific number of days (3, 7, 15, 45 days). | Accept: Greece  
Reject: others |
| H1.4   | When CCTV is present, respondents prefer settings in which only the police departments in their country have access to CCTV footage compared to those in which European or worldwide police departments can access the CCTV footage. | Accept: all |
| H1.5   | Respondents prefer having security personnel at the stations. | Reject: Germany,  
Hungary,  
Czech Republic,  
Poland,  
UK  
Accept: Others |
| H1.6   | Respondents prefer police compared to private security forces. | Accept: Unarmed Police, all  
Reject: Armed Police, all |
| H1.7   | Respondents prefer unarmed personnel (police or private) over armed personnel. | Accept: all |
| H1.8   | Respondents prefer travel options with no physical security checks (pat-down, bag search, metal detector and full body scanner). | Reject: Bulgaria, UK  
France,  
Italy,  
Spain  
Accept: others |
| H1.9   | Respondents prefer options with metal detector or full body scanners compared to those involving pat-down and bag checks. | Reject: Luxembourg  
Accept: others |
| H1.10  | Respondents prefer travel options which involve no delay due to physical security checks. | Accept: all |
| H1.11  | Respondents prefer travel options which involve no additional cost related to security and surveillance measures. | Reject: WTP for some security and surveillance measures |
Privacy concern

- Misuse of travel data for tracking a person's whereabouts
- Misuse of CCTV camera images by the authorities
- Sharing travel data and CCTV images across and outside the EU
- Misuse of security measures for sexual or racial harassment
- (Dis)trust in government
- Distrust in voting process
- Distrust in technology
- (Dis)trust in businesses

Distrust

- Public security surveillance systems are not designed to provide acceptable privacy
- Often security is used as an excuse to impose stricter surveillance and control over the population
- Increasing surveillance increases the risk of discrimination
- Investments in security are not being particularly effective in reducing crimes

Surveillance concern

- Male
- Frequency of travel
- Income
- Age

Measurement Model

Structural Model