ICT 01

PRESENTER	FILE NAME
Georgios Gardikis	ggar@space.gr
Seldeslachts Ulrich	ulrich@lsec.eu
Mauro Pezzè	mauro.pezze@usi.ch
Andreas Zalonis	azalonis@iit.demokritos.gr
Uli Siebold	uli.siebold@ic-information.com
Christian Derler	christian.derler@joanneum.at
Tuomas Tammilehto	Tuomas.tammilehto@laurea.fi

Building an open ecosystem for cybersecurity services

- *Georgios Gardikis, PhD*
- *ggar@space.gr*
- *SPACEHellas SA*
- *Proposal coordinator*

- *Proposal activity: SU-ICT-01-2018: Dynamic countering of cyber-attacks*
  - ***Sub-topic 2: Cyber-attacks management - advanced assurance and protection***

Proposal idea/content

Problem

- *diversity of development contexts and of levels of maturity*
- *increase of encrypted flows over the Internet*
- *detection of suspicious cyber activities and traffic patterns, and for classification of flows, while keeping privacy and confidentiality*
- ***Closed, proprietary and monolithic cybersecurity solutions***

Impact

- Enhanced protection against novel (incl. 0-day) threats
- Promote openness of cybersecurity technologies and facilitate cooperation among stakeholders
- Novel business models
- Promotion of cost-efficient cybersecurity solutions, esp. for SMEs

Solution

- *Adopt an open, community-based approach to detection of cyber-attacks*
- *Build on open-source Network Big Data and Virtualisation platforms*
- *Mobilise a community of stakeholders to develop open-source cybersecurity services on top of these platforms, including:*
  - *Machine Learning components, also extending to Deep Learning for zero-day threats*
  - *Virtual Security Appliances (VNFs)*
- *Assure privacy and security to the maximum possible extent*
- *Real-life use cases, possibly involving vertical industries*

Georgios Gardikis | ggar@space.gr

Project participants

- *Proposed coordinator: SPACEHellas (GR - SME), large ICT system integrator, expertise on data integration, cybersecurity and big data analytics*
  - *Coordinator of the EUSHIELD project on cybersecurity and big data*
- *Partners/Other participants:*
  - *3 SMEs, 2 Research Institutes (TBC)*
- *Looking for partners with the following expertise/technology/ application field:*
  - *Advanced ML techniques for cybersecurity, incl. Deep Learning*
  - *End-users / Vertical industries*

Georgios Gardikis | ggar@space.gr

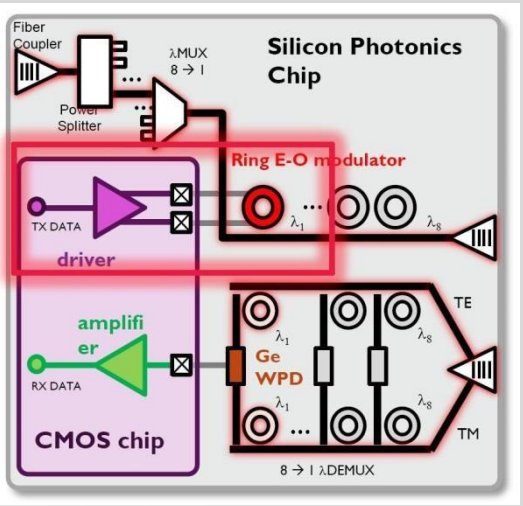
DYNAMO

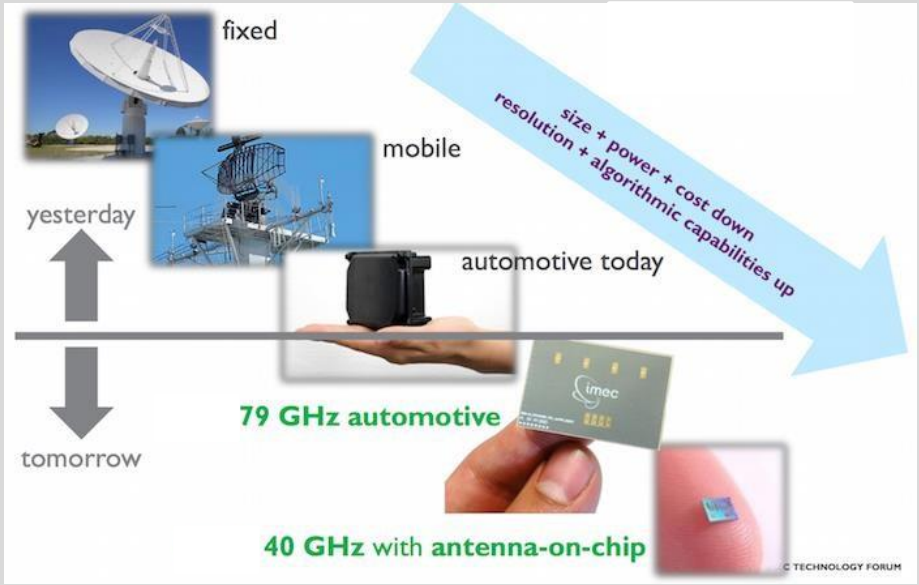
- *Seldeslachts Ulrich*
- *ulrich@lsec.eu*
- LSEC- Leaders In Security : a non-profit European (vzw) industry association (300+), cluster and user community (3500+ end users) supporting innovation & development of cyber security. ECSO Member and Global EPIC partner.
- Role: *Proposal coordinator, Requirements definition and validation*

- Proposal activity: *SU-ICT01-2018 Innovation Action,*
  - *A) cyber-attacks management – advanced assurance and protection*

Proposal idea/content

- *Use of high performance computing power capabilities to preload current and future security monitoring and reaction capabilities. Using:*
  - *High Performance Security Processing Power*
  - *Security on Silicon*





Example : using A/D converters DSP for high performance wireless signals, utilizing for security dynamics, on chip

Richard Chisnall, richard.chisnall@leadersinsecurity.org

Project participants

Have

- *Nano/Micro Electronics research & development facility*
- *Micro-Electronics Consumer Applications*
- *Security Information and Cyber Threat Intelligence actors*

Seeking

- Partners with the following expertise/ technology/ application field:
  - *HSM or other high performance security device manufacturers*
  - *Advanced High Performance Security Analytics requiring mass processing power*
  - *Deep learning methods for advanced analytics*
  - *OTA& other software update mechanics for high performance upgrading*

Richard Chisnall, richard.chisnall@leadersinsecurity.org

Security **P**latform for Cyber-**A**ttacks **M**anagement (SPAM)

Mauro Pezzè

mauro.pezze@usi.ch

Università della Svizzera italiana USI – campus Lugano

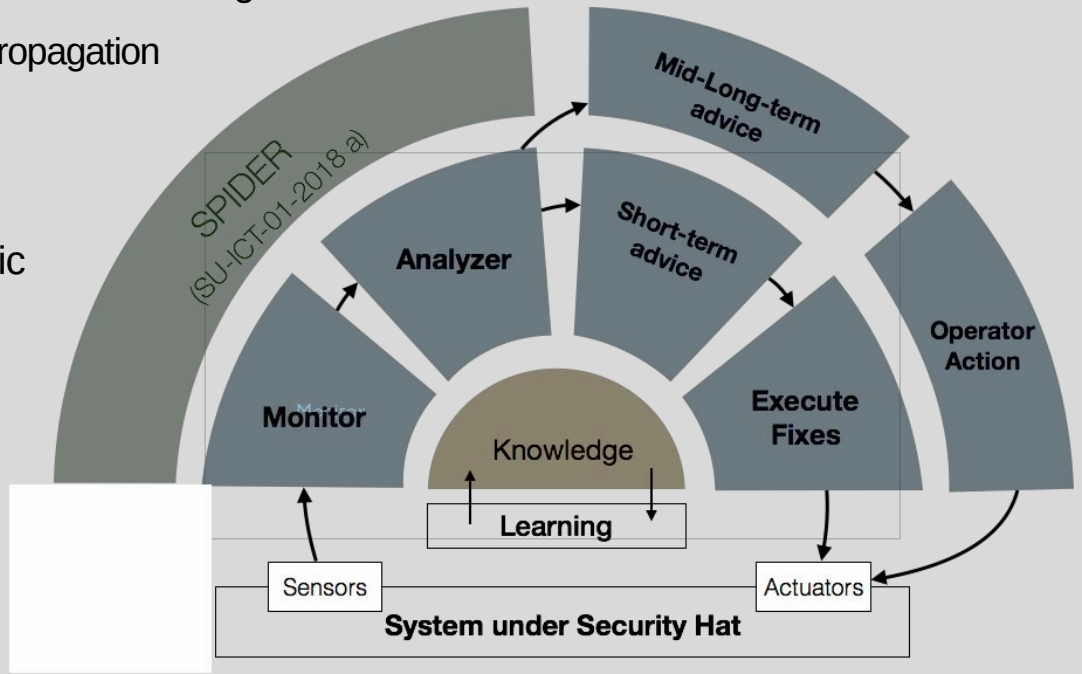
Role: *Coordinator or Work-Package leader*

Proposal activity: *ICT-01-2018 b.*

Paired with
Security **P**latform for **i**ntelligent
Data Analysis of cyber **R**esilience (SPiDeR)

Proposal idea/content

- **Vision:** Platform for dynamic, automatic, responsive recovery actions and security advices
  - Incrementally learning security vulnerability models
  - Runtime analyzing dynamically collected KPIs (metrics) to early predict security vulnerabilities
  - Runtime short term healing actions and long term security repairs
- **Techniques:** network theory, machine learning
  - Dynamic analysis of attack propagation
  - Automatic modelling
- Runtime **recovery actions**
  - Rapid, cheap and automatic
  - Partially automated
  - Complete removal
- **Feedback** mechanism
- Simple plugin of monitoring and predictive tools **(SPiDeR)**



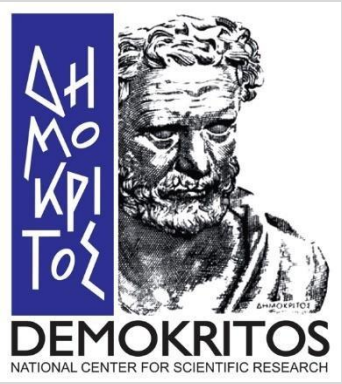
Presenter: Cristina Monni cristina.monni@usi.ch

Project participants

- Proposed coordinator:
  - *USI - Università della Svizzera italiana (CH)*
    - *Technology provider: dynamic analysis, self healing, autonomic cloud systems*
- Partners / Other participants:
  - *IC information company AG (CH), SME*
    - *Technology provider, developer, market study, exploitation*
  - *IMDEA Software institute (ES) [contact in progress]*
    - *Technology provider: security*

- Partner requirements:
  - *End-user: Banking, Assurance, Transportation, Energy,…*
  - *Developer, Exploiter: Critical infrastructure provider*
  - *Government agencies: society and ethical issues*
  - *Technology provider: ethical analysis, machine learning, network theory*

Presenter: Cristina Monni cristina.monni@usi.ch



Dynamic countering of cyber-attacks

- *Andreas Zalonis*
- *azalonis@iit.demokritos.gr*
- *NCSR DEMOKRITOS*
- Role: *WP leader and S/T provider*
- Proposal activity: *SU-ICT-01-2018, Dynamic countering of cyber-attacks*
  - *Subtopic a) Cyber-attacks management – advanced assurance and protection*

Dr. Andreas Zalonis
Research Associate at the Integrated Systems Laboratory
Email: azalonis@iit.demokritos.gr
Phone number: (+30) 210 650 3189

Dr. Stelios C.A. Thomopoulos
Institute Director and Head of Integrated Systems Laboratory
Email: scat@iit.demokritos.gr
Phone number: (+30) 210 650 3154
Mobile: (+30) 6944 986699

Proposal focus

- **Behavioral, social and human interaction modeling** for the design of efficient and effective trusted and verifiable computation systems and environments
  - Psychological data about human social engineering vulnerabilities
  - Behavioral models (AI, statistical or deterministic) based on experts theoretical use cases and log datasets
  - Cognition and Perception models
  - Historical data about past cyber-security violations and cyber-attack incidents
  - Partial behavioral modelling allowing integration with diverse behavioral models in different implementations
- Testing and validation in a controlled virtual environment
- Support of security mechanisms in the virtual environment

Andreas Zalonis – azalonis@iit.demokritos.gr

Project participants

Existing expertise and assets:

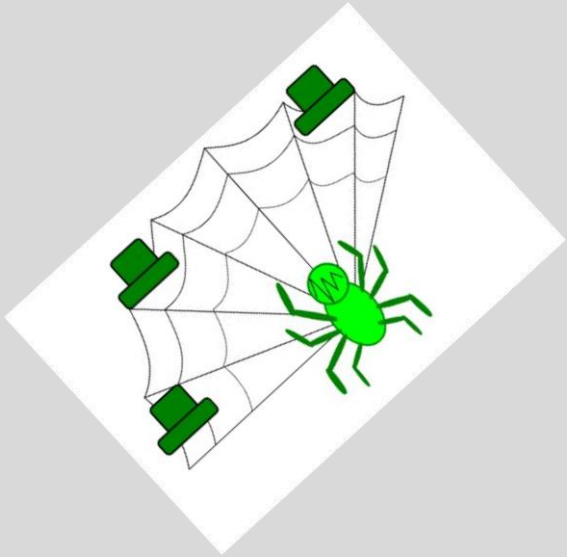
- Cyber security and network Threat Analysis, Pen-Testing methodologies, Distributed Ledger Technologies
- Agent–based simulation engine and federated simulation platform for the creation of a controlled virtual environment
- SoA behavioral modeling

Consortium – looking for partners:

- Coordinator
- End-users (public organizations – industry)
- Experts in Information Systems security
- Assets and tools based on machine learning and analytics for cybersecurity
- Assets and tools on advanced Security mechanisms (authentication/access control mechanisms, etc.)

Andreas Zalonis – azalonis@iit.demokritos.gr

Security Platform for intelligent Data Analysis of cyber Resilience (SPiDeR)



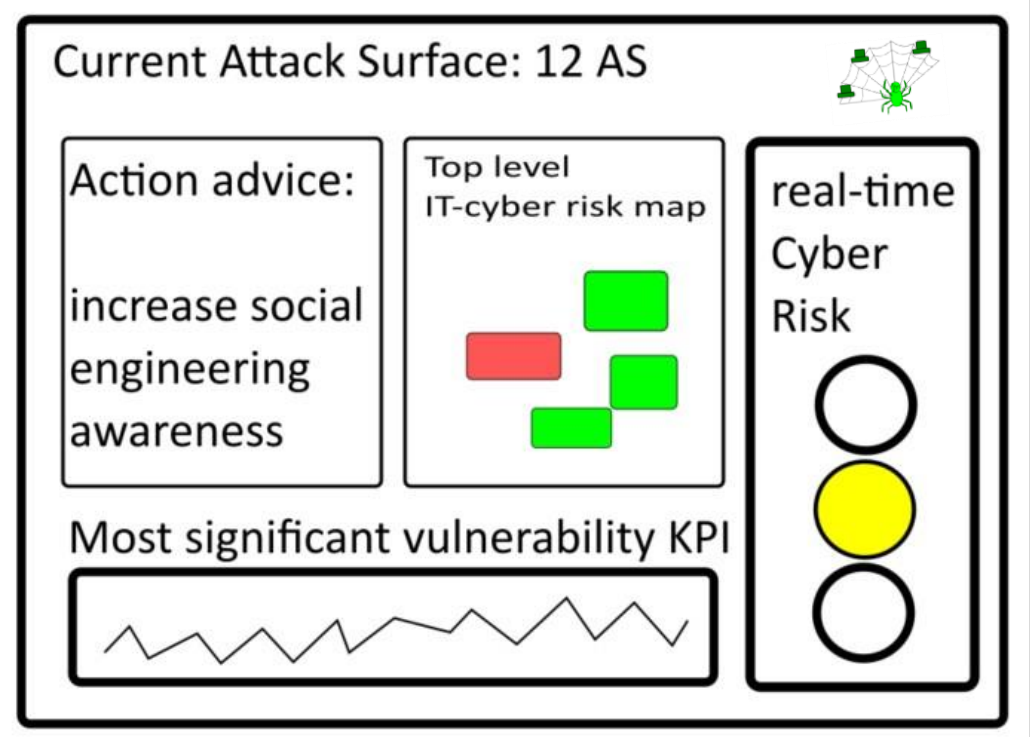
- *Uli Siebold*
- *uli.siebold@ic-information.com*
- *IC information company AG*
- Role: *Work-Package leader*

- Proposal activity: *ICT-01-2018*
  (Subtopic a Cyber-attacks management - advanced assurance and protection)

- *Paired with Proposal Security Platform for Cyber-Attacks Management SPAM (ICT-01-2018 b.)*

Proposal idea/content (end-user perspective)

- ***Vision:*** *Platform that analyses real time cyber security status of IT system and provides user friendly information*
- *Extension of measures, eg. «Relative Attack Surface Quotient» to generic systems (model based)*
- *AI - Analysis of runtime KPIs*
- *Real-time*
  - *risk analyis*
  - *advices*
- *Connects to existing security tools*



Uli Siebold uli.siebold@ic-information.com

Project participants

- Proposed coordinator: not confirmed, yet
- Partners / Other participants:
  - *Università della Svizzera italiana USI – campus Lugano*
  - *IC information company AG*

- Looking for partners with the following expertise/technology/application field:
  - *End-user: Banking, Assurance, critical infrastructure provider, ...*
  - *Security expert (ethical hacking, vulnerabilities analysis, etc.)*
  - *Busines service experts/analysts*
  - *Ethical analysis, governmental organizations*

Uli Siebold uli.siebold@ic-information.com

ESENTC: Enhanced Security Estimation through Network Topologic Classification

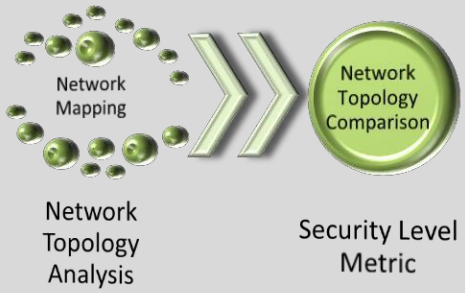
- *Christian Derler*
- *christian.derler@joanneum.at*
- *JOANNEUM RESEARCH*

- Role: *WP leader, R&D*

- Proposal activity: *SU-ICT-01-2018*
  - *Subtopic a) Cyber-attacks management - advanced assurance and protection*

Enhanced Security Estimation through **Network Topology Classification**

- Objectives
  - to achieve an estimation of a network's security status based on its topological characteristics obtained from black box scanning
- Expected results
  - First assessment of a network's overall security
  - Identification of hotspots to increase the efficiency of more thorough security analyses
  - Structural approach supplementing security measure proposals with topological (network architectural) ones



Christian Derler, christian.derler@joanneum.at

Project participants

- Looking for partners with the following expertise/ technology/ application field:
  - *Industry partner, Co-ordination ?*
    - *Commercial Exploitation*
  - *User partner*
    - *ISP, multinational cooperation with subsidiaries*
      - *Large network, many networks*

Christian Derler, christian.derler@joanneum.at

Dynamic approach to cyber-attacks management

- *Tuomas Tammilehto*
- *Tuomas.tammilehto@laurea.fi*
- *Laurea University of Applied Sciences, Finland*

- Role: *WP leader/partner*

- SU-ICT-01-2018: **Cyber-attacks management - advanced response and recovery**

Proposed role in the project

- *WP leader on* **Behavioural, social and human aspects in security/privacy**
  - User behavior
  - Trust building strategies
  - Collaboration with end-users, requirements, service design

- *WP leader on* **Exploitation and Dissemination**
  - Multi-stakeholder engagement and information sharing strategies
  - Policy dialogs
  - Business models and sustainability of the project results
    - Laurea is a member of e.g. EOS, ECSO, ESDC

Tuomas Tammilehto, tuomas.tammilehto@laurea.fi

Project participants

- Partners / Other participants:
- 1 – Laurea UAS, Finland – HEI/RD
- 2 – Cyber Services, Hungary - SME

- Looking for partners with the following expertise/ technology/ application field:
  - *Coordinator*
  - *Industry cooperation groups*
  - *Research organizations*
  - *CSIRTs*
  - *Critical infrastructure as end user (healthcare, finance, etc)*
  - *Incident/crisis management expert*
  - *AI/deep learning expert*

Tuomas Tammilehto, tuomas.tammilehto@laurea.fi