NIS WG3 meeting, October 8th 2014

WG3 Secure ICT Research & Innovation

NIS Platform WG3 Secure ICT Research & Innovation

NIS WG3 Meeting

Secure ICT Landscape Deliverable

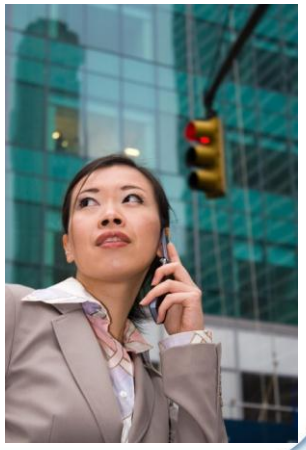
Mari Kert, Javier Lopez
Evangelos Markatos, Bart Preneel

NIS Platform WG3 Secure ICT Research & Innovation

SECURE ICT LANDSCAPE DELIVERABLE

What is it?

- Describe State of the Art
  - In Cyber Security
- What are the Treats?
  - What are the Existing Defenses for each threat?
  - What are the Research Challenges?
  - What are the Existing Tools?



How did we do it?

- Created 4 Groups:
  - **@steering**
  - **@contributors**
  - **@wg3**
  - **@stakeholders**

How did we do it?

- @**steering** created a Table of Contents
  - Asked for feedback from @**wg3** and @**stakeholders**
  - In parallel,
    - those who gave feedback (and wanted)
      - became part of @**contributors**

Contributors

Magnus Almgren, *Chalmers University of Technology*
Elias Athanasopoulos, *FORTH*
Christoph Bier *Fraunhofer*
Gabriela Bodea *TNO*
Henk Birkholz, *Fraunhofer SIT*
Hugh Boyes, *University of Warwick*
Sabrina de Capitani di Vimercati, *Università degli Studi di Milano*
Hervé Debar, *Télécom SudParis*
Bruno Empatz *European Defence Agency*
Sotiris Ioannidis, *FORTH, Greece*
Roy Isbell, *University of Warwick*
Nicola Jentzsch, *DIW*
Rieks Joosten *TNO*
Florent Kirchner *CEA LIST*
Wouter Leibbrandt, *NXP Semiconductors*
Fabio Martinelli *CNR*
Emmanuel Miconnet *Thales Services*
Nina Olesen *EOS*
Bert Jan te Paske *TNO*
Thanasis Petsas, *FORTH, Greece*
Joachim Posegga, *University of Passau*
Michalis Polychronakis, *Columbia University*
Vassilis Prevelakis, *Technical University, Braunschweig*
Ali Rezaki, *TUBITAK - BILGEM, Turkey*
Rodrigo Roman, *University of Malaga*
Carsten Rudolph, *Fraunhofer SIT*
Pierangela Samarati, *Università degli Studi di Milano*
Michael Sieber *European Defence Agency*
Bjornar Solhaug, *SINTEF*
Christophe Sprenger, *ETH Zurich*
Theo Tryfonas, *University of Bristol*
Paulo Verissimo, *University of Lisbon*
Claire Vishik, *Intel*
Tim Watson, *University of Warwick*

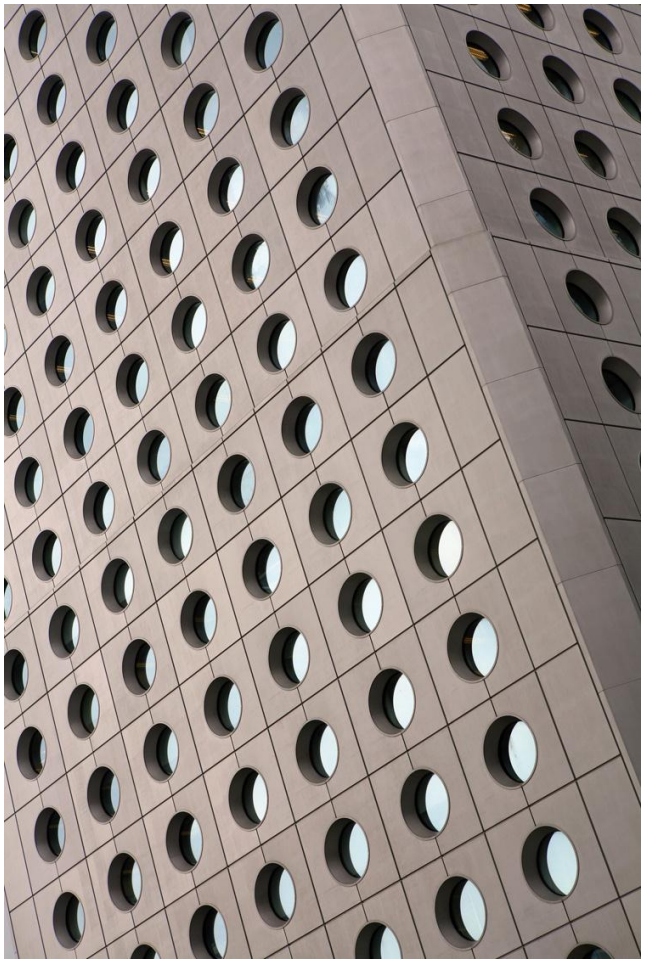
The procedure

- **@steering**
  - created an “example” section
    - to be used by the rest of the contributors
  - assigned the sections to authors
    - and reviewers as well

- Text has been steadily flowing
  - Some is still trickling

Structure

- Introduction
- Basic Technologies
- Internet of Things - Cloud
- Application Domains
- Conclusions



Structure – Example Section

- Basic Structure of Each section:
  - Introduction
    - *What is it?*
  - Current Status
    - *What has been done?*
  - Research Challenges
    - *What needs to be done?*
  - Existing Tools (if applicable)

Example Section: Intrusion Detection Systems

- Introduction
  - Rule-based, Anomaly-based
- Current Status
- Research Challenges
  - The Changing Security Paradigm
    - No more perimeter security
  - Speed
  - Whole System Image
    - Not only network image
  - New models for attack patterns
    - String matching and automata are not enough

Example Section II: Mobile Security

- Introduction
  - smartphones
- Current Status
- Research Challenges
  - Bring Your Own Device
  - Managing the Lack of Diversity
    - 2-3 systems dominate the market
  - Re-packaged applications
    - Malicious apps masquerading as innocent ones

Example Section III: Social Media

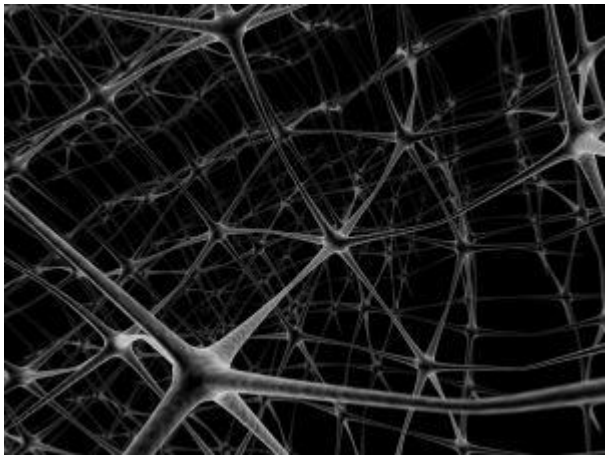
- Introduction
  - evolution
- Current Status
  - Threats?
- Research Challenges
  - Lack of research data
  - Information tracking
    - Who has what for which user?
      - Personal data? Cookies?
      - IP addresses?
      - Web browse fingerprinting?
  - Compromised account identification

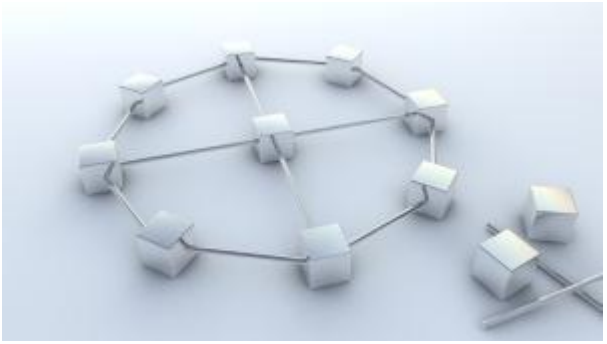
Example Section IV: The cloud

- Introduction
  - deployment
- Current Status
  - Security? Transparency?
- Research Challenges
  - Proprietary cloud implementations
    - Hinder research
  - Increased target vector
    - Lots of assets in the same data center
  - Insider threats
  - Trust erosion
  - Privacy
  - Data Protection

Example Section V: IoT

- Introduction
- Current Status
  - Identity, authentication?
  - Access control
  - Trust
- Research Challenges
  - Large Scale
  - Distribution - ownership
  - Heterogeneity
  - Dynamicity – churn (peers join/leave)





Current Status

- Version 1 has been delivered
  - On-time (July 2014)
  - 33 contributors
  - 69 pages
  - 14 Basic Technologies
  - 11 applications domains
- Version 2 has started
  - TOC to be circulated for additions

What's next?

- Version 1 of the Deliverable
  - Created lots of interest
  - More people would like to contribute
- Plan:
  - Circulated an extended ToC
  - Received more interest
  - Will assign new co-authors for the rest of the sections
  - Will assign new reviewers for the new sections

Summary

- Secure ICT Landscape Deliverable
  - Have mobilized the community
  - At several different levels
    - **@contributors**, **@wg3**, **@stakeholders**
  - Version 1 has been delivered
    - On-time
  - Version 2 is ongoing