Novel Approaches to Risk and Security Management for Utility Providers and Critical Infrastructures

Workshop Introduction

Stefan Schauer

HyRiM End User Workshop
Vienna, 02.11.2015

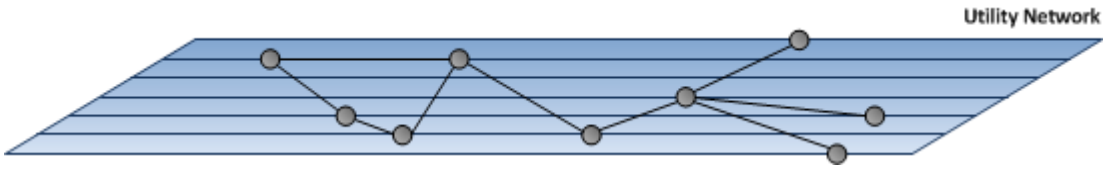
Risk Management

- Risk assessment and risk management is a core duty for utility providers
  - Utility providers operate critical infrastructures
  - Responsible for the supply of large number of people with different goods
  - Incidents within/affecting utility providers might have huge economic and societal impacts

- Numerous risk assessment and risk management tools already exist
  - Based on well-established standards and guidelines (e.g. ISO 31000)
  - Often focusing on a specific field (e.g. IT Security – ISO 27005, Supply Chain Management – ISO 28000, Port Security – ISO 20858)
  - Often designed for businesses and not the special requirements of utility providers or critical infrastructures
  - Mostly a matter of best practices

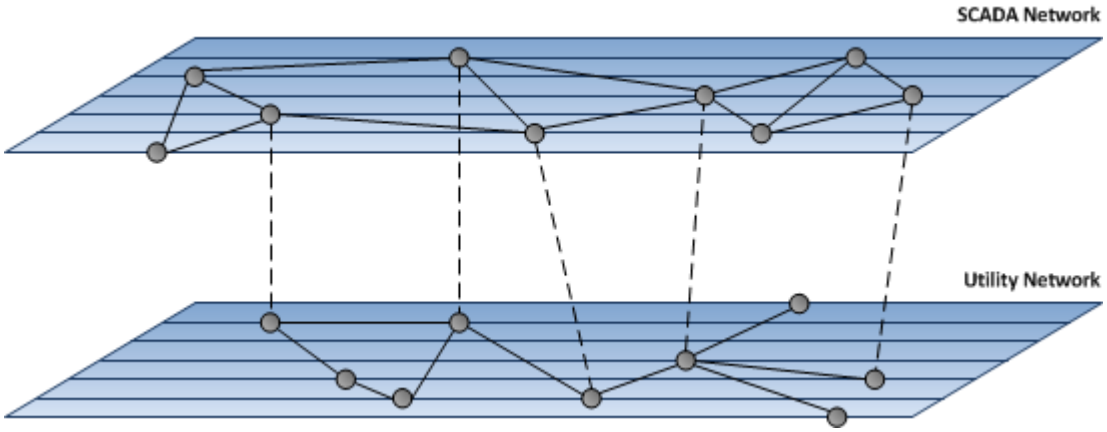
Interconnected Networks

- Networks operated by utility providers become more and more interconnected
  - Utility network (e.g. power lines, water pipes, oil pipelines, etc.)



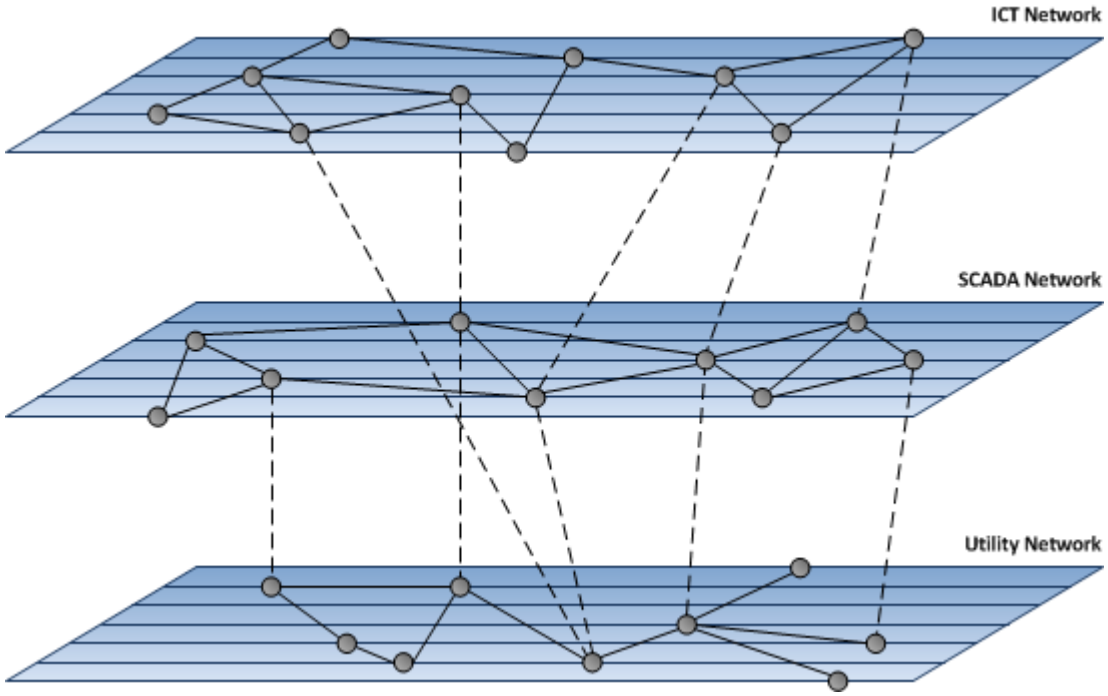
Interconnected Networks

- Networks operated by utility providers become more and more interconnected
  - Utility network (e.g. power lines, water pipes, oil pipelines, etc.)
  - Control networks (e.g. SCADA networks, smart grids, etc.)



Interconnected Networks

- Networks operated by utility providers become more and more interconnected
  - Utility network (e.g. power lines, water pipes, oil pipelines, etc.)
  - Control networks (e.g. SCADA networks, smart grids, etc.)
  - ICT networks (e.g. office networks, communication networks, intranet, etc.)



Novel Threats and Challenges

- Requirements of utility providers have changed
  - Number of cyber-physical systems increases (e.g. SCADA networks)
  - Threats evolve more rapidly and become more complex (e.g. Advanced Persistent Threats – APT)
  - Intentional threats became more popular in recent years (e.g. terrorism, cyber-terrorism/hacktivists, espionage, etc.)

- Threats affecting one part of a utility provider can propagate through the network and affect other, distant parts, too
  - Malware infection on the ICT network might cause the failure of a SCADA system and thus affect the utility network itself
  - Security issue of a SCADA system might give access to business data handled in the ICT network
- Additionally, utility providers are interconnected and interacting with each other

Novel Threats and Challenges

- Novel approaches towards security and risk management have to be identified to address these issues
  - Solutions for each network level exist and are applied separately
  - "Hybrid" risk management methodologies are required, providing a holistic overview (i.e. looking at several networks simultaneously)
  - Interconnections and the related cascading effects need to be considered

- Sole focus on technical threats and technical solutions is no longer adequate
  - Social engineering is a major aspect in many attack strategies
  - Organizational factors are essential for every security measure or security strategy performed in an organization

- Security and risk management methodologies explicitly have to take societal factors into account

Workshop Goals

- Presentation of current activities in the field of risk management
  - Based on the EU project HyRiM, SPARKS and MEDUSA

- Presentation of novel approaches towards risk and security assessment for utility providers
  - Technical aspects (cyber-physical security, interconnected networks, threat propagation and cascading effects, surveillance, etc.)
  - Societal aspects (threat awareness, influence of the human factor, effects on the supply chain, etc.)

- Identification of potential future challenges and emerging threats in the fields of risk management and risk assessment for utility providers

- Building awareness among end users and creating an end user group

Workshop Agenda

10:00 – 10:15	Welcome and introduction to risk management for utility providers *Dr Stefan Schauer, AIT Austrian Institute of Technology*
10:15 – 11:15	Interpreting, Preempting and Misunderstandings of Risk *Dr David Lund, HW Communications Ltd (UK)*
11:15 – 11:45	Coffee break and networking
11:45 – 13:15	The HyRiM Project: A Short Introduction *Dr Stefan Schauer, AIT Austrian Institute of Technology (AT)*
	Threat Awareness for Critical Infrastructures *Dr Antonios Gouglidis, Lancaster University (UK)*
	Mathematical Models for Risk Assessment in Utility Networks *Dr Sandra König, AIT Austrian Institute of Technology (AT)*

Workshop Agenda

11:45 – 13:15	Using Vulnerable Hosts to Assess Cyber Security Risk in Critical Infrastructures *Xiaobing He, University of Passau (DE)*
13:15 – 14:15	Lunch break
14:15 – 15:05	Human and Organisational Aspects in Critical Infrastructures *Dr Mark Rouncefield, Lancaster University (UK)*
	Smartphone-based surveillance *Ali Alshawish, University of Passau (DE)*
15:05 – 15:45	The SPARKS Project: A Short Introduction *Dr Paul Smith, AIT Austrian Institute of Technology (AT)*
	Structured Threat Analysis for the Smart Grid *Dr Martin Hutle, Fraunhofer AISEC (DE)*

Workshop Agenda

15:45 – 16:15	MEDUSA tool for assessing physical and cyber risks in ports' supply chains *Spyros Papastergiou, University of Piraeus (GR)*
16:15 – 16:45	Coffee break and networking
16:45 – 17:45	Panel Discussion: *"*Major Challenges and Emerging Trends for Utility Providers" *Dr David Lund, HW Communications Ltd (UK)* *Prof Hermann de Meer, University of Passau (DE)* *Alma Solar, CEA - Cooperativa Elèctrica d' Alginet (SP)* *Karl Rossegger, Linz AG (AT)*
17:45 – 18:00	Concluding Remarks and Future Engagement Opportunities
18:00	Networking dinner

Novel Approaches to Risk and Security Management for Utility Providers and Critical Infrastructures

Workshop Introduction

Stefan Schauer

HyRiM End User Workshop
Vienna, 02.11.2015