iTTi
e-technologie i biznes

Protection of critical Infrastructure against cybercrimes

Warsaw 30.11.2011

Prof. Witold Hołubowicz

Krzysztof Samp

Agenda

- Company information
- Trends in cyber security
- On-going research in cyber security area
- Recomendations

ITTI – company information

- ITTI mission:
  - consulting independent from equipment, system or software suppliers in the area of **telecommunications**, **IT** and **business**
  - applied research in **Information & Communication Technologies** and **interdisciplinary projects** with ICT component
- Facts and figures:
  - company founded in **1996**
  - **employment**: around 50 employees
  - fully owned by **ITTI partners**



  - „CristalBrusselsPrize2006 and 2010” for the most active and successful Polish SME participatinginFP6 andFP7
  - Leader of entrepreneurship in Wielkopolska region (2008)
  - Prize for innovation in IT appliance given by Polish IT Association (2009)
  - Reward for the high performance in R&D projects for European Defence Agency given by Polish Ministry of Defence(2009)

Cyber security

- Our way of life and economic prosperity depend on a reliable cyberspace
- ICT is now a strategic instrument of industry, administration, and the military
- Important Milestones in cyber security related with the Critical Infrastructure:
  - During the Kosovo-Crisis, NATO faced its first serious incidents of cyber-attacks – e-mail accounts being blocked for several days for external visitors, and repeated disruption of NATO's website.
  - Incidents in Estonia in summer shows this growing source of threats to public safety and state stability.
  - In 2008, via simple USB-stick connected to a military-owned laptop computer at a military base in the Middle East, spy software spread undetected on both classified and unclassified systems.
  - In June 2010 the malware “Stuxnet” was used to attack the Iranian nuclear programme (approximately 45,000 industrial Siemens control systems worldwide had been infected by a tailored trojan virus that could manipulate technical processes critical to nuclear power plants).
  - U.S. has accused both **China and Russia of using cyber espionage** to steal its trade and technology secrets.

Levels of threats in cyber security

- Level 1: Garden Variety:
  - Inexperienced
  - Limited funding
  - Opportunistic bahavior
  - Target known vulnerabilities
  - Uses viruses, worms, trojans, bots
  - Easy detected
- Level 2: Mercenary:
  - Higher-order skills
  - Well-financed
  - Targeted activity
  - Target known vulnerabilities
  - Uses viruses, worms, trojans, bots and more sophisticated tools
  - Target and exploit valuable data
  - Detectable, but hard to attribute
- Level 3: Nation States
  - Very sophisticated tradecraft
  - Foreign intel agencies
  - Very well financed
  - Target technology and info
  - Use wide range of tradecraft
  - Establish cover presence on sensitive networks
  - Difficult to detect

Trends in cyber security

- The most dangerous actors in the cyber-domain are still nation states
- Highly sophisticated espionage and sabotage in the cyber-domain still needs the capabilities, determination and cost-benefit-rationale of a nation state
- Physical damage and real kinetic cyber-terrorism has not taken place yet
- Cyber-attacks are clearly evolving from a mere nuisance to a serious threat against information security and critical national infrastructure
- Attacks are increasing at an exponential rate

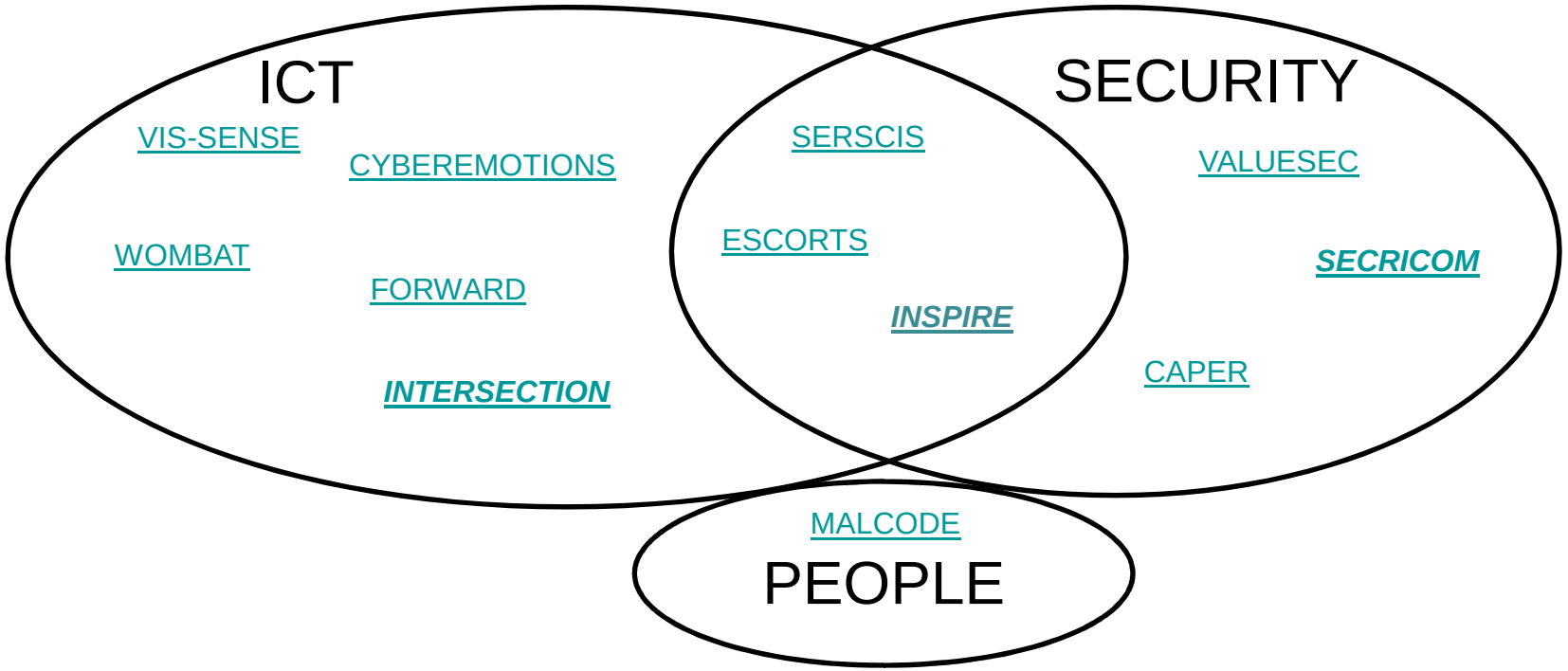
Trends in cyber security

- Top Cyber Security Trends in 2011:
  - Security of Mobile Apps
  - New platforms – eg. Android
  - Security of devices connected to the Internet – eg. Medical gadgeds and car devices
  - Open Source Hacking Tools
  - Security For The Cloud Computing
  - PCI 2.0 and Web Security
  - Wikileaks Publishes Corporate Secrets
  - Cyber Terrorism

Source: www.cenzic.com

Research projects

- NATO:
  - The Science for Peace and Security Programme:
    - A.2.d Defence against terrorist threats: Computer terrorism countermeasures and **cyber defence** (i.e. the defence of Communication and Information Systems (CIS)). Computer network exploitation by terrorists
- EU FP7 Research areas which includes Cyber Security:



Research projects

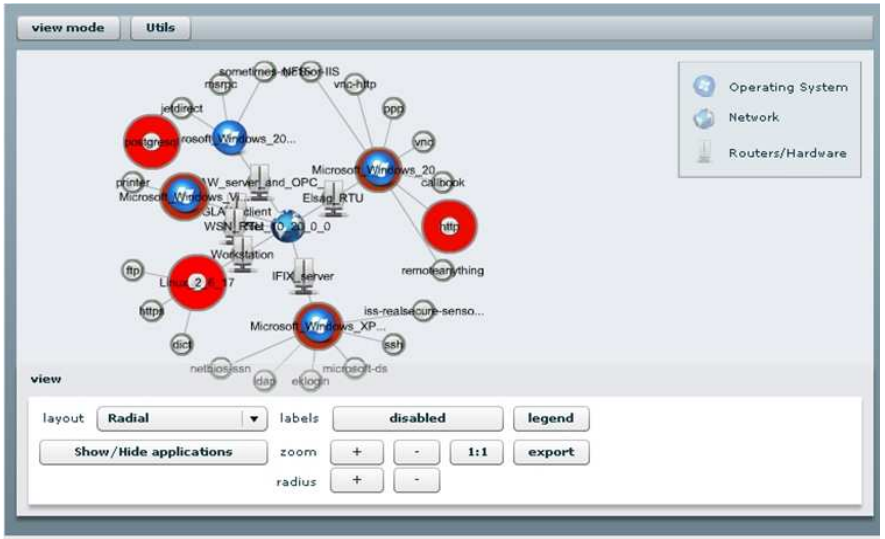
- EU FP7 Research areas:
  - Join ICT – SECURITY
    - ICT-SEC-2007.1.7 Critical infrastructure protection
    - ICT-SEC-2007-7.0-02 European Security Research Networks (incl. for standardization)
  - ICT:
    - ICT-2009.1.4 Trustworthy ICT
    - ICT-2007.1.4 Secure, dependable and trusted infrastructures
    - ICT-2007.8.4 Science of complex systems for socially intelligent ICT
  - SECURITY:
    - SEC-2010.1.2-1 Information and knowledge management for the prevention of organized crime
    - SEC-2010.6.3-3 Research on rigorous methodologies for assessment of ***security*** investments and trade-off between ***security*** and other societal objectives (e.g. privacy and social cohesion),SEC-2010.6.4-1 Cost-benefit analysis of the present and future ***security*** measures in Europe
    - SEC-2007-4.2-04 Wireless communication for EU crisis management
  - PEOPLE:
    - FP7-PEOPLE-2009-IOF Marie Curie International Outgoing Fellowships for Career Development

Research projects - INSPIRE

- **Title:** INcreasing Security and Protection through Infrastructure REsilience-International cooperation aspects
- Objectives:
  - assuring the protection of critical information infrastructures through the identification of their vulnerabilities
  - development of innovative techniques for securing networked process control systems
- Main core:
  - protect critical information infrastructures by appropriately configuring, managing, and securing the communication network which interconnect the distributed control systems
- Adopted way:
  - development of traffic engineering algorithms
  - self-reconfigurable architecture
  - diagnosis and recovery techniques

Research projects - INSPIRE

- ITTI's results:
  - Security ontology – to understand relations Cyber security area
  - DAT tool (Decision Aid Tool for CI operators) – intended to be used in industrial SCADA environments for security status/ evaluation/assesment. Main features:
    - Rank threats to SCADA network
    - Proposes solutions/countermeasures
    - Visualizes topology (local/global view)
    - Manages Knowledge (the ontological description of system)
    - Manages Security Rules
    - Can be used for different critical infrastructures (by replacing the ontology)
    - Allow to estimate the impact of particular action prior the physical modifications (estimated risk via simulation)



Research projects - INTERSECTION

- **Title:** Infrastructure for heterogeneous, resilient, secure, complex, tightly inter-operating networks
- Objectives:
  - assuring the protection of heterogeneous networks and infrastructures
  - implement and integrated security framework made of different subsystems and components providing network and infrastructure security
  - contribute to standardisation process in order to foster multi-operator interoperability and coordinated strategies for securing networked systems
  - definition of security metrics for assessment and certification of network infrastructures and systems

Research projects - INTERSECTION

- ITTI's results:
  - Ontology-based approach to vulnerability handling
  - IVD (INTERSECTION Vulnerability Database) – based on the CVE (Common Vulnerabilities and Exposures) vulnerability naming standard and uses the following SCAP (Security Content Automation Protocol) standards:
    - Common Configuration Enumeration (CCE)
    - Common Platform Enumeration (CPE)
    - Common Vulnerability Scoring System (CVSS)
  - Vulnerabilities and threats ontology
    - use Shared Information/Data(SID) Model in which networks assets and relations between them are defined
    - Assets description is specified in UML
  - PIVOT (Project INTERSECTION Vulnerability Ontology Tool) – the ontology-logic based manager tool for vulnerability data management and classification. Basic functions:
    - Searching vulnerabilities matching prompted criteria
    - Adding, modifying, removing ontology instances
    - Removing ontology instances
  - Anomaly detections (Matching pursuit)
  - Network Traffic Track Analyzer

Research projects - SECRICOM

- **Title:** Seamless communication for crisis management
- Objectives:
  - development of a reference security platform for EU crisis management operations
  - Solve or mitigate problems of contemporary crisis communication infrastructures (Tetra, GSM, Citizen Band, IP) such as poor interoperability, vulnerability against tapping and misuse, lack of possibilities to recover from failures.
- ITTI's Results:
  - Secure wireless fault tolerant communication solution
  - IPv6 based secure communication solution
  - Communication infrastructure threat Analysis and challenges for dynamic heterogeneous communication infrastructure domains
  - Communication infrastructure security Model and Service Definition

Recommendations

Obligatory actions:

- Assess cyber attacks to inform cyber defense – focus on high risk technical areas first.
- Ensure that security investments are focused to counter highest threats.
- Maximize use of automation to enforce security controls — negate human errors.
- Define metrics for critical controls.
- Use consensus process to collect best idea.

Recommendations

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
4. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
5. Boundary Defense
6. Maintenance, Monitoring, and Analysis of Security Audit Logs
7. Application Software Security
8. Controlled Use of Administrative Privileges
9. Controlled Access Based on Need to Know

Recommendations

10. Continuous Vulnerability Assessment and Remediation
11. Account Monitoring and Control
12. Malware Defenses
13. Limitation and Control of Network Ports, Protocols, and Services
14. Wireless Device Control
15. Data Loss Prevention
16. Secure Network Engineering
17. Penetration Tests and Red Team Exercises
18. Incident Response Capability
19. Data Recovery Capability
20. Security Skills Assessment and Appropriate Training to Fill Gaps

Contact

Thank you for your attention

ITTI Sp. z o.o.

ul. Rubież 46

61-612 Poznań

Tel: (61) 622 69 85 fax: (61) 622 69 73

e-mail: witold.holubowicz@itti.com.pl