Academic Research on Cybersecurity

Todor Tagarev, Zlatogor Minchev, Nataliya Ivanova
IT for Security Department, Institute of ICT, Bulgarian Academy of Sciences

Sixth Scientific Conference of the International Information Security Research Consortium

October 1-2, 2012 Sofia, Bulgaria, Park Inn Renaissance
IT for Security Department

• Institute of Information and Communication Technologies, Bulgarian Academy of Sciences, http://iict.bas.bg
• IT4Sec Department, www.IT4Sec.org
• CSDM & Strategic Security and Defence Management site, www.defencemanagement.org
• Joint Training, Simulation and Analysis Centre
• “Information and Security” journal
Outline

• Requirements (expectations) to academic research on cybersecurity
  – Policy support
  – Technologies
  – Support to education and training
  – Knowledge dissemination

• Academic research in Bulgaria and partner networks

• Discussion
Policy support

• Awareness of cyber risks and threats
• Defining capability requirements and assignment of responsibilities
• Defining ‘Rules of Engagement’
  – Including preservation of human rights and freedoms
• Coordination & Cooperation
  – Operations, Training
  – Capabilities development
• Allocation of resources
• Provision of transparency, accountability, integrity
http://defencemanagement.org/
Specific topics

• Assigning cybersecurity responsibilities in the national security sector
  – Analysis of alternatives

• National roles and specialization in the framework of NATO and the European Union
  – Management of the scientific and technological ‘infrastructure’
Cybersecurity Knowledge Management

- Definitions
- Policies
- Strategies
- Organisations & Responsibilities
- Cyber Threats
- Cyberwar & Cyberdefence
- Standards & Technologies
- Education & Training
- Research Centres
- Studies
- Democratic oversight & human rights and liberties
Knowledge Dissemination

  – v.28: Critical Infrastructures Safety and Security
  – v.18: Cybercrime and Cybersecurity
  – v.15: e-Government and Security of Information
  – v. 4: Dialectics of Information Security

• Standing call:

  *Cybersecurity Challenges and Responses*
The Nowadays Cyber World
In summary: policy-making needs to be forward looking; outward looking; innovative, flexible and creative; evidence-based; inclusive; joined up; to learn lessons from experience; to be communicated effectively; and to incorporate ongoing evaluation and review.
Social Awareness Rising

Change Management

Seven Steps of Social Change
Key Players

- Politicians
- Policy Makers
- Cyber Experts
- ICT Business
- Media
- Integrated Security Sector
- Civil Society
- End-Users
- Other
Common Used Approaches

- Summits
- Sessions
- Discussions
- Forums
- Meetings
- Brainstorming & Delphi
- Surveys
- Interviews
- Media Campaigns
- Legal Acts
- Analyses
- Road Maps
- Other...
Some Examples
Recent EU Policy & Awareness Activities

ACTA - Anti-counterfeiting Trade Agreement !?
Recent USA & NATO Policy & Awareness Activities

‘NATO Cyber Red Team’
‘US Cyber Command’
SOPA & PIPA !?
Selected NGO Recent Policy & Awareness Related Activities
Institute of ICT
Bulgarian Academy Of Sciences

IT for Security Department

Computer Networks & Architectures Department

http://it4sec.org

A European Network of Excellence in Managing Threats and Vulnerabilities in the Future Internet: Europe for the World, SySSSec, EU FP7

... Instead of reactively chasing after attackers, we should start working proactively and think about emerging threats and vulnerabilities...

http://www.syssec-project.eu
<table>
<thead>
<tr>
<th>Threat-Enabler</th>
<th>Assets</th>
<th>Personal Assets</th>
<th>Societal Assets</th>
<th>Professional Assets</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Privacy (Human Rights)</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Anonymous Internet Access</td>
<td>Digital Identity</td>
<td>Medium</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Ubiquitous networks</td>
<td>Financial Assets</td>
<td>High</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Human Factors</td>
<td>Health Safety</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Insider attacks</td>
<td>Critical Infrastructures</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Botnets</td>
<td>GRIDS Clouds</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Program Bugs</td>
<td>Data Sales etc.</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Scale and Complexity</td>
<td></td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Mobile Devices</td>
<td></td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>24/7 connectivity</td>
<td></td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>More private info available</td>
<td></td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Smart meters</td>
<td></td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Tracking</td>
<td></td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Smart Environments</td>
<td></td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Unsecured Devices</td>
<td></td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Social networks</td>
<td></td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Cyber-physical connectivity for Infrastructures, cars etc.</td>
<td></td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Organized Cyber Crime</td>
<td></td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Mobile Malware</td>
<td></td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>SCADA Malware</td>
<td></td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
</tr>
</tbody>
</table>

*SySSec Cybersecurity Priorities 2011*
A Study on IT Threats and Users Behavior Dynamics in Online Social Networks, DMU03/22, 2011-2013

www.snfactor.com

www.syssec-project.eu
Some of our activities in 2012
Recent Results
Recent Results: New Methods for malware attacks prevention with applications for contents recognition in real-time for multicore configuration and cloud computing (Team Leader Prof. Eugene Nikolov)

http://www.bas.bg/cgi-bin/e-cms/vis/vis.pl?s=001&p=0317&n=4&g=
Institute of Mathematics & Informatics

Mathematical Foundations of Informatics Department

RESEARCH FIELDS: Coding theory, Cryptography, Combinatorics, Theoretical informatics
Institute of Defence - MoD

http://www.mod.bg/bg/EXT/InstitutOtbrana/index.htm

Thematic areas:
Armaments & combat supplies
Combat equipment & systems
CBRN protection and ecology
Combat supply
Communication and Information Systems & Technologies
Radiolocation & navigation
Informatics & Information Technologies
Cyberdefence, cryptography & Information Security
Defence Economic Aspects
Logistics
Military-political studies
Human Factor & Medicine
Military Standards, quality and specifications
Military Tests & Control Measurements

http://di.mod.bg/hemus2012/
Artillery, AAD & CIS Faculty
http://www.nvu.bg/node/361

Shumen, November 3-4, 2011


Scientific Session 2011

Problems of Information Security of XXI century Proceedings
Scientific-Research Lab for Cybersecurity
Leader: Prof. Dragomir Pargov

International Conference ‘Bulgarian Cryptography Days’ BulCrypt 2012
Sofia University “St. Kliment Ohridski”

Partner on the International Cyber Investigation Training Academy

Sofia University – Center for Educational Services

Cybersecurity - one year qualification course
The policy making and awareness rising processes concerning the human society are rather complex research field. Whilst, nowadays the cybersecurity is an indispensable part of the 21st century information society the solution of this task is evidently becoming a serious challenge that incorporates a comprehensive necessity for integration of academic research in both social and technical sciences.
THANK YOU FOR THE ATTENTION!

QUESTIONS?