Nippon-European Cyberdefense-Oriented Multilayer threat Analysis

Hervé Debar
Institut Mines-Télécom,
Télécom SudParis

Youki Kadobayashi
Nara Institute of Science and Technology


FP7-ICT-2013-EU-JAPAN

- Selected as the funded project for call:
  - ICT-2013.10.1(c): Cybersecurity for improved resilience against cyber threats
- Articulated around three technical work packages:
  - Threat data collection
  - Threat data analysis
  - Cyberdefense for improved resilience
- Scope: cross border and cross layer
The Challenges of Cybersecurity

- Widespread incidents
  - Large scale
  - Target both Internet infrastructure and endpoints
- Technological advances
  - Professionalization of malware development
  - Commercialization of attack kits
- Cross border
  - Internet is the final frontier
  - Problems are widely shared
Need for an International Cooperation

- **Data collection**
  - Broaden collection scope across borders
  - Extend collection sources to cover multiple layers

- **Data analysis**
  - Bridge cultural gap in eliciting knowledge
  - Share analysis results in a unified manner

- **Cyber-defense for improved resilience**
  - Cooperate in flexible threat mitigation
  - Build and share demonstration resources

A Complementary Consortium

- Balanced in numbers and institution types
- Complementary skills: malware analysis and network operation
- Responsibility sharing on task management
- Resources and facilities sharing for advancing research

sotiris@ics.forth.gr - www.necoma-project.eu
Already a Success

- International teams
- Common research objectives
- Successful proposal submitted within a restricted timeframe
- Renowned researchers from both sides
- Personnel training in both sides
- Regular online meetings
- Already produced results after 6 months
The First Deliverable: D3.1

- Survey of Policy Enforcement Points (PEPs)
  - Examine existing and deployed PEPs in terms of capabilities and management functions
  - Analyze the potential gap between existing PEPs and NECOMA cyberdefense requirements

- Highlights:
  - Need for reconfiguration-oriented approach
  - Need for network key control point identification
  - Need threat-to-countermeasure pipeline

Sample Results: Visual tuning of anomaly detectors

- Objective: develop a better parameter tuning method for multiple anomaly detectors
- Approach: visualizing overwrap of detectors output with Chord diagrams
- Preliminary results: 19% accuracy improvement in anomaly detection

Mazel et al.: Visual comparison of Network Anomaly Detectors with Chord Diagrams, SAC2014 (accepted)
Sample Results: DDoS mitigation

- DDoS mitigation with LISP (Locator/ID Separation Protocol)
  - Enhanced LISP Map table: for normal traffic and attack traffic
  - Attack packets are routed to decoy server

Characteristics

- Victim servers and decoy servers are unidentifiable to confuse attackers
- Mitigation at egress boundary of offending AS or ingress boundary of victim AS to minimize the impact on the Internet backbone

![Diagram showing LISP map and mitigation process]

Intensive and Fruitful Teamwork

Japan consortium meeting, June 2013 at Keio University

<table>
<thead>
<tr>
<th>Date</th>
<th>Activity Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013/4/5</td>
<td>Teleconference</td>
</tr>
<tr>
<td>2013/7/2</td>
<td>日欧テレカンファレンス</td>
</tr>
<tr>
<td>2013/7/6</td>
<td>NECOMA日本側コンソーシアム会議</td>
</tr>
<tr>
<td>2013/7/26</td>
<td>NECOMA日本側コンソーシアム会議</td>
</tr>
<tr>
<td>2013/9/5-6</td>
<td>パリ Telecom SudParis にて全体会合</td>
</tr>
<tr>
<td>2013/9/18-20</td>
<td>SDN Japan にて発表、西田教授の講演</td>
</tr>
<tr>
<td>2013/9/26</td>
<td>NECOMA日本側コンソーシアム会議</td>
</tr>
<tr>
<td>2013/9/27</td>
<td>WPI 日欧テレカンファレンス</td>
</tr>
<tr>
<td>2013/9/30-10/4</td>
<td>日欧OpenFlow ワークショップでの発表・検証</td>
</tr>
<tr>
<td>2013/10/9</td>
<td>WPI 日欧テレカンファレンス</td>
</tr>
<tr>
<td>2013/10/18</td>
<td>WPI 日欧テレカンファレンス</td>
</tr>
<tr>
<td>2013/10/23</td>
<td>WPI 日欧テレカンファレンス</td>
</tr>
<tr>
<td>2013/10/24</td>
<td>インターネットカンファレンス2013発表 SDN利用データ収集技術に関する報告</td>
</tr>
<tr>
<td>2013/10/29-30</td>
<td>WPI 日欧テレカンファレンス</td>
</tr>
<tr>
<td>2013/11/3-8</td>
<td>インターネットカンファレンス</td>
</tr>
<tr>
<td>2013/11/9</td>
<td>WPI 日欧テレカンファレンス</td>
</tr>
<tr>
<td>2013/11/12</td>
<td>WPI 日欧テレカンファレンス</td>
</tr>
<tr>
<td>2013/11/13</td>
<td>WPI 日欧テレカンファレンス</td>
</tr>
<tr>
<td>2013/11/15</td>
<td>WPI 日欧テレカンファレンス</td>
</tr>
<tr>
<td>2013/11/19</td>
<td>WPI 日欧テレカンファレンス</td>
</tr>
<tr>
<td>2013/11/21</td>
<td>NECOMA日本側コンソーシアム会議</td>
</tr>
<tr>
<td>2013/11/26</td>
<td>WPI 日欧テレカンファレンス</td>
</tr>
</tbody>
</table>
Towards Horizon 2020

- NECOMA is one of many collaborations made possible thanks to FP7 and MIC
- EU and Japan need further collaboration to continue successful research
- Cyber security should participate to « Secure Societies », societal challenge addressed by H2020