On the Imbalance of the Security Problem Space and its Expected Consequences

Konstantin (Kosta) Beznosov
Electrical and Computer Engineering
University of British Columbia
Vancouver, Canada

Olga Beznosova
Political Science
University of British Columbia
Vancouver, Canada
Outline

- where and how large the imbalance
- why should defenders care
- how attackers use social aspects
- where to go
  - Looking outside of today security
  - Questions for future research
Where and How Large the Imbalance?
Decomposed Problem Space

Human

Social

Technological

Factors that are due to interactions among more than one person in social or formal organizations and within wider social context.

Such factors as human psychology, physiology, and cognition at the individual level.
Mapped Subareas Of Security

Human

Social

Technology

- economics of security
- organizational and social factors
- phishing
- political and security

- social engineering
- information assurance
- access control

- malware
- intrusion detection
- cryptography
- security usability
Grouped Sub-areas

- Technology-centric
  - cryptography
  - intrusion detection
  - access control

- Social-centric
  - economics of security
  - social engineering
  - organizational and social factors

- Human-centric
  - phishing
  - security usability
  - malware

Keywords:
- security usability
- social engineering
- information assurance
- economics of security
- cryptography
- intrusion detection
- access control
- phishing
- malware
- organizational and social factors
# Performed Searches

<table>
<thead>
<tr>
<th>Category/sub-area</th>
<th>Query</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Technology-centric</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Cryptography</strong></td>
<td>cryptography OR cryptographic OR encryption OR decryption</td>
</tr>
<tr>
<td></td>
<td>(&quot;access control&quot; OR authorization) AND computer AND security</td>
</tr>
<tr>
<td><strong>Access Control</strong></td>
<td>intrusion AND detection AND computer AND security</td>
</tr>
<tr>
<td><strong>Intrusion detection</strong></td>
<td>computer (&quot;security assurance&quot; OR &quot;information assurance&quot;) -financial -social</td>
</tr>
<tr>
<td><strong>information assurance</strong></td>
<td>malware OR &quot;computer worm&quot; OR &quot;computer virus&quot; OR &quot;malicious software&quot;</td>
</tr>
<tr>
<td><strong>malware</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Human-centric</strong></td>
<td></td>
</tr>
<tr>
<td><strong>security usability</strong></td>
<td>security AND (usability OR usable OR HCI)</td>
</tr>
<tr>
<td><strong>phishing</strong></td>
<td>phishing</td>
</tr>
<tr>
<td><strong>Social-centric</strong></td>
<td></td>
</tr>
<tr>
<td><strong>social engineering</strong></td>
<td>&quot;social engineering&quot;</td>
</tr>
<tr>
<td><strong>economics of security</strong></td>
<td>(economics AND (&quot;information security&quot; OR &quot;computer security&quot;)) OR &quot;security economics&quot;</td>
</tr>
<tr>
<td><strong>politics and security</strong></td>
<td>(politics OR bill OR legislation OR regulation) AND (&quot;information security&quot; OR &quot;computer security&quot;)</td>
</tr>
<tr>
<td><strong>human factors</strong></td>
<td>(security AND &quot;human factor&quot;) OR &quot;security awareness&quot; OR &quot;security training&quot; OR &quot;security culture&quot; AND (computer OR information)</td>
</tr>
</tbody>
</table>
Engineering Village

Technology 96%

Human 2%

Social 2%

engineeringvillage2.org
Compendex -- 9M engineering references and abstracts
Inspec -- 8M records from scientific and technical journals and conferences
Web of Science

- Technology: 95%
- Human: 2%
- Social: 3%

isiknowledge.com
8,700 research journals
So What?
Attackers Increasingly Aware of Human and Social Aspects

- “Most users encounter PC security issues because they fall for social engineering tactics ...”
  
  Fathi, Microsoft’s vice president for the Windows core operating system (Hines 2007)

- “I was so successful in that [social engineering] line of attack that I rarely had to resort to a technical attack.”

  Kevin Mitnick in testimony before the U.S. Congress (The Associated Press 2000)
Social Engineering Attacks

Social organizational practices and societal norms

actions of a particular human being

Human

Technological technology and interfaces
Level of User Security Knowledge Declines

Household Penetration: Residential Broadband Services
(Percentage of U.S. Households)

- 2004: 31%
- 2005: 40%
- 2006: 47%
- 2007: 55%

Source: Digital Lifestyles: 2007 Outlook
© 2007 Parks Associates
Ought to Explore the Social Aspects To Achieve Results Not Possible Otherwise

“If the enemy leaves a door open, you must rush in.”
(Sun Tzu, *The Art of War*, ca. 515 BC)
Case Study: Cyber War In Estonia

source: slate.com
Estonia 2007

- Highly dependant on computers
  - parking payments
  - Wi-Fi
  - national elections
- Political Incident
  - Estonia's embassy sealed and attacked
  - Cyber attacks continued ...

"Police arrested 600 people and 96 were injured in a second night of clashes in Estonia's capital over the removal of a disputed World War Two Red Army monument … Russia has reacted furiously to the moving of the monument … Estonia has said the monument had become a public order menace as a focus for Estonian and Russian nationalists."

CNN
Some times experiencing reciprocity

Estonia forever!
маскальским и сибирским л0хам превед из Таллина!

But most importantly ...
Bringing Critical Sites Down ... 

Availability of Estonian Ministry of Foreign Affairs Web site
May 5-9, 2007

Total time for www.vm.ee from Italy/Aruba

<table>
<thead>
<tr>
<th>Time in seconds</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
</tr>
<tr>
<td>6</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>1</td>
</tr>
</tbody>
</table>

Total time from Italy/Aruba to www.vm.ee

<table>
<thead>
<tr>
<th>Failures</th>
</tr>
</thead>
<tbody>
<tr>
<td>73</td>
</tr>
</tbody>
</table>

source: f-secure.com
Through Distributed Denial of Service Attacks

- protesters running DoS programs
- botnets
- 128 attacks
  - 115 were ICMP floods
  - 4 TCP SYN floods
  - 9 generic traffic floods
- maxing to 95 Mbps
- up to 10 hours
- shutting 58 sites at once

source: asert.arbornetworks.com

"at its peak over one million computers were involved"

www.crime-research.org
Case Study Social Aspects

Attacker employed
- simple DoS attacks
- mobilization of activists
- botnet rentals
- flexible communications

Defenders could’ve
- avoided/reduced sentiments
- disrupted mobilization
- employed deception
- built up social capital
- rented anti-botnets
- made botnets not feasible
Where to go?
Organizational Processes and Behavior

behavioral school (Simon and March, 1950s)

- individuals and organizations have to rely upon programmed behavior in making decisions

Example: Cuban Missile Crisis
Organizational Structure

- **Netwar** (Arquilla and Ronfeldt, RAND Corporation)
  - organizational purposes affect the suitability and effectiveness of various types of social structures

- agile networks and virtual organizations
  - flexible internal communication networks
  - strategic connections
  - responding rapidly to external opportunities and challenges
  - rapid information processing
  - quick decision making

Source: wikipedia.org
Social Capital

- what is it?
  - social networks and norms of social cooperation
- organizations with higher levels of trust, horizontal cooperation, and loyalty show better performance and efficiency
- ‘modern classic example’
  - difference between Northern (civic) and Southern Italy (parochial) (Putnam 1993)
Suggestions for Further Research

- relationship between organizational processes and behavior and the effectiveness of security defenses
- relationship between organizational structures and security
- models of attackers’ organizations
- relationship between organizational cultures, norms, and social capital and the effectiveness of organizational security strategies and programs
- societal aspects of security promotion mechanisms
  - education, awareness building, and policy
  - recycling, seat belt use, as well as drinking and smoking
Summary

- Technology: 95%
- Social: 3%
- Human: 2%

Total time for www.vm.es from Italy/Aruba

<table>
<thead>
<tr>
<th>Time in seconds</th>
<th>Sample</th>
<th>No. samples</th>
<th>Average</th>
<th>Max</th>
<th>Latest</th>
<th>Failures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total time from Italy/Aruba to <a href="http://www.vm.es">www.vm.es</a></td>
<td>479</td>
<td>1.473</td>
<td>37,097</td>
<td>0.608</td>
<td>73</td>
<td></td>
</tr>
</tbody>
</table>
“people who think their security problem can be solved with only technology do not understand the problem and do not understand the technology”
(Konstantin Beznosov & Olga Beznosova, 2007)