Countering Denial of Information Attacks

Gregory Conti
www.cc.gatech.edu/~conti
conti@acm.org

Disclaimer

The views expressed in this presentation are those of the author and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, the Department of Defense or the U.S. Government.
Denial of Information Attacks:

Intentional Attacks that overwhelm the human or otherwise alter their decision making

http://www.consumptive.org/sasquatch/hoax.html

http://www.colinfahey2.com/spam_topics/spam_typical_inbox.jpg
The Problem of Information Growth

- **The surface WWW contains ~170TB (17xLOC)**
- IM generates five billion messages a day (750GB), or 274 terabytes a year.
- Email generates about 400,000 TB/year.
- P2P file exchange on the Internet is growing rapidly. The largest files exchanged are video files larger than 100 MB, but the most frequently exchanged files contain music (MP3 files).

In the end, all the power of the IDS is ultimately controlled by a single judgment call on whether or not to take action.

- from Hack Proofing Your Network

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Signal (s)</th>
<th>Noise (n)</th>
<th>s/n</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>#1</td>
<td>High</td>
<td>Low</td>
<td>Very Good</td>
<td>Good to excellent ability to find information</td>
</tr>
<tr>
<td>#2</td>
<td>Low</td>
<td>Low</td>
<td>Parity</td>
<td>Marginal to good ability to find information</td>
</tr>
<tr>
<td>#3</td>
<td>Low</td>
<td>High</td>
<td>Bad</td>
<td>DoI</td>
</tr>
<tr>
<td>#4</td>
<td>Very High</td>
<td>Very High</td>
<td>Parity</td>
<td>DoI, processing, I/O or storage capability exceeded (aka DoS)</td>
</tr>
</tbody>
</table>
### DoI Attack Scenarios

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Signal (s)</th>
<th>Noise (n)</th>
<th>s/n</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>#1</td>
<td>High</td>
<td>Low</td>
<td>Very Good</td>
<td>Good to excellent ability to find information</td>
</tr>
<tr>
<td>#2</td>
<td>Low</td>
<td>Low</td>
<td>Parity</td>
<td>Marginal to good ability to find information</td>
</tr>
<tr>
<td>#3</td>
<td>Low</td>
<td>High</td>
<td>Bad</td>
<td>DoI</td>
</tr>
<tr>
<td>#4</td>
<td>Very High</td>
<td>Very High</td>
<td>Parity</td>
<td>DoI, processing, I/O or storage capability exceeded (aka DoS)</td>
</tr>
</tbody>
</table>

### DoI Attack Scenarios

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Signal (s)</th>
<th>Noise (n)</th>
<th>s/n</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>#1</td>
<td>High</td>
<td>Low</td>
<td>Very Good</td>
<td>Good to excellent ability to find information</td>
</tr>
<tr>
<td>#2</td>
<td>Low</td>
<td>Low</td>
<td>Parity</td>
<td>Marginal to good ability to find information</td>
</tr>
<tr>
<td>#3</td>
<td>Low</td>
<td>High</td>
<td>Bad</td>
<td>DoI</td>
</tr>
<tr>
<td>#4</td>
<td>Very High</td>
<td>Very High</td>
<td>Parity</td>
<td>DoI, processing, I/O or storage capability exceeded (aka DoS)</td>
</tr>
</tbody>
</table>


## DoI Attack Scenarios

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Signal (s)</th>
<th>Noise (n)</th>
<th>s/n</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>#1</td>
<td>High</td>
<td>Low</td>
<td>Very Good</td>
<td>Good to excellent ability to find information</td>
</tr>
<tr>
<td>#2</td>
<td>Low</td>
<td>Low</td>
<td>Parity</td>
<td>Marginal to good ability to find information</td>
</tr>
<tr>
<td>#3</td>
<td>Low</td>
<td>High</td>
<td>Bad</td>
<td>DoI</td>
</tr>
<tr>
<td>#4</td>
<td>Very High</td>
<td>Very High</td>
<td>Parity</td>
<td>DoI, processing, I/O or storage capability exceeded (aka DoS)</td>
</tr>
</tbody>
</table>

---

---
http://www.mindsim.com/MindSim/Corporate/OODA.html
http://www.mindsim.com/MindSim/Corporate/OODA.html
Microsoft, AOL, Earthlink and Yahoo file 6 antispam lawsuits (Mar 04)

Federal Can Spam Legislation (Jan 04)

California Business and Professions Code, prohibits the sending of unsolicited commercial email (September 98)

First Spam Conference (Jan 03)

Defense Taxonomy (Big Picture)

<table>
<thead>
<tr>
<th>Legal</th>
<th>Lawsuits</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>New Laws</td>
</tr>
<tr>
<td>Regulatory</td>
<td>Government Regulation</td>
</tr>
<tr>
<td>Moral</td>
<td>PR Campaign</td>
</tr>
<tr>
<td></td>
<td>Code of Ethics</td>
</tr>
<tr>
<td>Cultural</td>
<td>Communities</td>
</tr>
<tr>
<td>Organizational</td>
<td>Topical counter-Dol groups</td>
</tr>
<tr>
<td>Financial</td>
<td>Increasing cost of Dol operations</td>
</tr>
<tr>
<td>Violence</td>
<td>Violence against Dol perpetrators</td>
</tr>
<tr>
<td>Technology</td>
<td>(see next slide)</td>
</tr>
</tbody>
</table>

http://www.metroactive.com/papers/metro/12.04.03/buether-0349.html
Microsoft, AOL, Earthlink and Yahoo file 6 antispam lawsuits (Mar 04)

Federal Can Spam Legislation (Jan 04)

California Business and Professions Code, prohibits the sending of unsolicited commercial email (September 98)

First Spam Conference (Jan 03)

http://www.metroactive.com/papers/metro/12.04.03/booher-0349.html
Example DoI Attacks

- Exploit round off algorithm
- Trigger many alerts
- Spoof browser
- Misleading advertisements

Very small text
from Slashdot...

I have a little PHP script that I use whenever I get a phishing email. The script generates fake credit card numbers, expiration dates, etc. and repeatedly hits the phishing site's form dumping in random info.

Any halfway intelligent phisher would record the IP address of each submission and just dump all of mine when he saw there were bogus, but it makes me feel good that I at least wasted some of his time ;)

http://yro slashdot org/ news pl?id=150848&sid=12651434
For more information...


---

email me…

---

DoI Countermeasures in the Network Security Domain
**information visualization** is the use of interactive, sensory representations, typically visual, of abstract data to reinforce cognition.


rumint security PVR
Last year at DEFCON

First question...

How do we attack it?
Malicious Visualizations...

Objectives

- Understand how information visualization system attacks occur.
- Design systems to protect your users and your infrastructure.

There attacks are entirely different...
Basic Notion

A malicious entity can attack humans *through* information visualization systems by:

- Inserting relatively small amounts of malicious data into dataset (not DOS)
- Altering timing of data

Note that we do not assume any alteration or modification of data, such as that provided from legitimate sources or stored in databases.

---

Attack Domains...

- Network traffic
- Usenet
- Blogs
- Web Forms
- syslog
- Web logs
- Air Traffic Control
Attack Manifestations
Labeling Attack
(algorithm)

- 100 elements
- $X = 1..100$
- $Y = \text{rand()} \times 10$

CDX 2003 Dataset
X = Time
Y = Destination IP
Z = Destination Port
AutoScale Attack/Force User to Zoom
(algorithm)

http://www.neti.gatech.edu/
Precision Attack
(algorithm)

http://www.nersc.gov/nusers/security/Cube.jpg
http://developers.slashdot.org/article.pl?sid=04/06/01/1747223&mode=thread&tid=126&tid=172

Occlusion
(visualization design)
Jamming
(visualization design)

Countermeasures

- **Authenticate users**
- Assume an intelligent and well informed adversary
- **Design system with malicious data in mind**
- Assume your tool (and source) are in the hands of an attacker
- **Train users to be alert for manipulation**
- Validate data
- Assume your infrastructure will be attacked
- In worst case, assume your attacker has knowledge about specific users
- Design visualizations/vis systems that are resistant to attack
- If you can’t defeat attack, at least facilitate detection
- **Use intelligent defaults**
- **Provide adequate customization**
For more information...


See also www.rumint.org for the tool.

on the con CD…

Other Sources of Information...

- Guarding the Next Internet Frontier: Countering Denial of Information Attacks by Ahamad, et al
  - http://portal.acm.org/citation.cfm?id=844126
- Denial of Service via Algorithmic Complexity Attacks by Crosby
  - http://www.cs.rice.edu/~scrosby/hash/
- A Killer Adversary for Quicksort by McIlroy
- Semantic Hacking
Demo

On the CD...

- Talk Slides (extended)
- Code
  - rumint
  - secvis
  - rumint file conversion tool (pcap to rumint)
- Papers
  - SOUPS Malicious Visualization paper
  - Hacker conventions article
- Data
  - SOTM 21 .rum

See also: www.cc.gatech.edu/~conti and www.rumint.org
rumint feedback requested...

- **Tasks**
- **Usage**
  - provide feedback on GUI
  - needed improvements
  - multiple monitor machines
  - bug reports
- **Data**
  - interesting packet traces
  - screenshots
    - with supporting capture file, if possible
- **Pointers** to interesting related tools (viz or not)
- New viz and other analysis **ideas**

**Volunteers to participate in user study**

---

**Acknowledgements**

404.se2600, Kulsoom Abdullah, Sandip Agarwala, Mustaque Ahamad, Bill Cheswick, Chad, Clint, Tom Cross, David Dagon, DEFCON, Ron Dodge, EliO, Emma, Mr. Fuzzy, Jeff Gribschaw, Julian Grizzard, GTISC, Hacker Japan, Mike Hamelin, Hendrick, HoneyNet Project, Interz0ne, Jinsuk Jun, Kenshot0, Oleg Kolesnikov, Sven Krasser, Chris Lee, Wenke Lee, John Levine, David Maynor, Jeff Moss, NETI@home, Henry Owen, Dan Ragsdale, Rockit, Byung-Uk Roho, Charles Robert Simpson, Ashish Soni, SOUPS, Jason Spence, John Stasko, StricK, Susan, USMA ITOC, IEEE IAW, VizSEC 2004, Grant Wagner and the Yak.
• **100+ Graduate Level InfoSec Researchers**
• **Multiple InfoSec degree and certificate programs**
• **Representative Research**
  - User-centric Security
  - Adaptive Intrusion Detection Models
  - Defensive Measures Against Network Denial of Service Attacks
  - Exploring the Power of Safe Areas of Computation
  - Denial of Information Attacks (Semantic Hacking)
  - Enterprise Information Security
• **Looking for new strategic partners, particularly in industry and government**

www.gtisc.gatech.edu

Questions?

Greg Conti
conti@cc.gatech.edu
www.cc.gatech.edu/~conti
www.rumint.org

http://www.museumofhoaxes.com/tests/hoaxphototest.html