Countering Denial of Information Attacks

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

Original Photos: National Geographic, Photoshopper: Unknown

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.

image: http://www.leavenworth.army.mil/usdb/standard%20products/vtdefault.htm

Denial of Information Attacks:

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

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

	From	Subject	Received
	Nannie Graves	the miricle for your pen1s! t	3/29/2004 3:44 AM
	Soraya Londa	Haha, U Have A Real Small Pe~nis virginals	3/29/2004 3:47 AM
	Rocky Wright	Your own resort	3/29/2004 3:56 AM
	lynell harrison	Spring Special	3/29/2004 4:06 AM
	Cp001	Fwd:En-crease Your Manhood 2day!.....vitally	3/29/2004 4:13 AM
	Low Rate Advisors	Rates are Low Again - Refinance Before it's Too Late!	3/29/2004 4:32 AM
	FreshFreeStuffNewsle...	[Win a Dell Computer Package]	3/29/2004 4:51 AM
	ScbExpress	Snoring Control FDA Approved	3/29/2004 5:03 AM
	Corrine Walker	Internet Pharmacy - Smart Prices	3/29/2004 5:45 AM
	Faustino McManus	Internet Pharmacy - Smart Prices	3/29/2004 5:45 AM
	lucillabenedetto@mak...	Rates as low as 1.24% - We Will Beat ANY offer	3/29/2004 5:54 AM
	ardellachavis@madvo...	Rates as low as 1.24% - We Will Beat ANY offer	3/29/2004 5:56 AM
	David Roper	Online Canadian Generic Pharmacy, Order Prescription Medicati...	3/29/2004 6:10 AM
	Andres Delaney	Prescription medications by mail' xc svfxdjyvjb	3/29/2004 6:12 AM
	Brenton Rosario	Re: ~ ~ You ready?	3/29/2004 6:58 AM
	Miriam Waller	Get Valium over night - no prescription needed	3/29/2004 7:09 AM
	Taylor Dawkins	19-Mortgages as low as 2.14%	3/29/2004 7:19 AM
	Internet Mail Delivery	Delivery Notification: Delivery has failed	3/29/2004 7:29 AM
	Erik Ames	New Prescription Generic Drugs from Canada	3/29/2004 7:32 AM
	Lucinda Overton	28-Mortgages as low as 2.10%	3/29/2004 7:40 AM
	Dennis Smiley	cc: legend you will be	3/29/2004 9:08 AM
	Melissa Jones	(legal) Marijuana-like product, Mood Enhancers, Herbal Meds	3/29/2004 9:43 AM
	Twila Winn	retention bobble cicada emanuel	3/29/2004 10:48 AM
	Samuel Benjamin	opulent capetown	3/29/2004 10:48 AM
	Francisca Vann	discrete bump	3/29/2004 10:48 AM
	Your Prescription Shop	Budget Medicine	3/29/2004 11:51 AM
	Your Cash Central	Need 500 Now? Apply for an OVERNIGHT Payday advance	3/29/2004 12:15 PM
	Miss Stacy Lane	a girls life on the farm	3/29/2004 12:24 PM
	Carole Dawson	Buy Full Cartons of Cigs at half the price of the store J7r F5	3/29/2004 12:29 PM
	Kim Hendrix	Viagr{a! Levi^tra! Soma! Phentermine! Ambien! Tramadol! SOLD...	3/29/2004 12:41 PM
	Tyrone Branch	Your one stop prescrip]tions	3/29/2004 12:47 PM
	Weight Loss Trial - V-A	Amazing: Diet Patch Trial --Try it Absolutely FREE	3/29/2004 12:48 PM
	Ivan Whitehead	(794)Scientificaly proven to work(]	3/29/2004 1:01 PM
	shment@hotmail.com	read it immediately	3/29/2004 1:03 PM
	Lynnette Sam	780 expensive software titles selll from 25 - 70 bucks bottommost	3/29/2004 1:18 PM
	Vincenza Chrystal	all commercial softwares at cheaap deftly	3/29/2004 1:18 PM
	13tggrd	Cpfahey, |tŬPĔŔ VÍÀGRÀ ÃŤ |tŬP&...	3/29/2004 1:47 PM
	Morgan Sykes	<<NaturalGain+Hundred% MBG-Hundred% No Side-Effects Hu...	3/29/2004 1:48 PM
	Fleet Bank	! official Notice for all Fleet bank customers	3/29/2004 2:05 PM
	Elliot Oneil	babel drawn chest alga bayreuth	3/29/2004 2:33 PM

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).

http://www.sims.berkeley.edu/research/projects/how-much-info-2003/

Source: http://www.advantage.msn.it/images/gallery/popup.gif

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

DoI Attack Scenarios

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

DoI Attack Scenarios

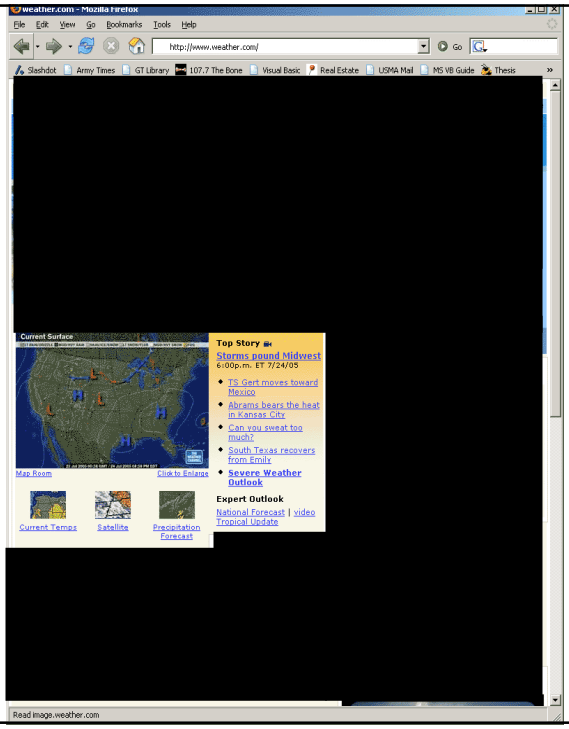
Scenario	Signal (s)	Noise (n)	s/n	Impact
#1	High	Low	Very Good	Good to excellent ability to find information
#2	Low	Low	Parity	Marginal to good ability to find information
#3	Low	High	Bad	DoI
#4	Very High	Very High	Parity	DoI, processing, I/O or storage capability exceeded (aka DoS)

DoI Attack Scenarios

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

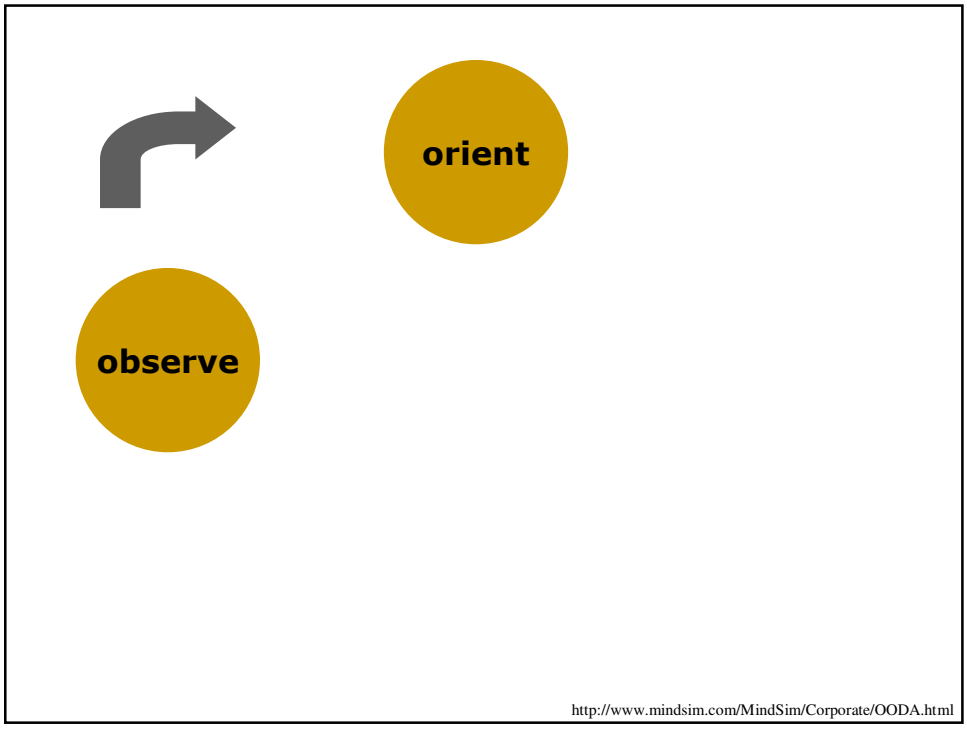
DoI Attack Scenarios

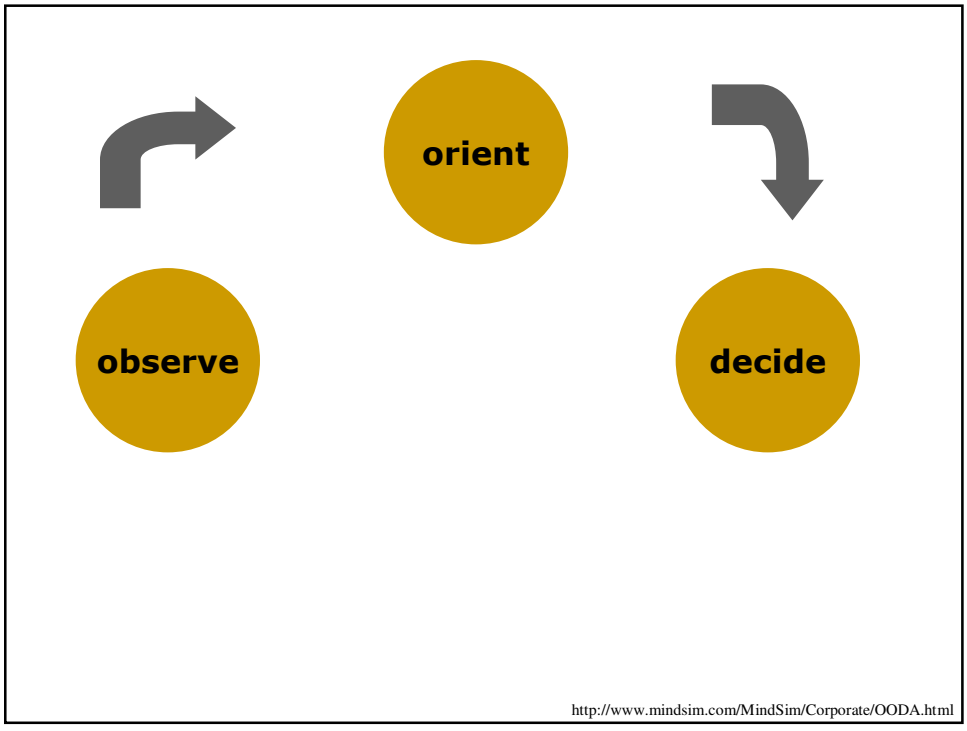
Scenario	Signal (s)	Noise (n)	s/n	Impact
#1	High	Low	Very Good	Good to excellent ability to find information
#2	Low	Low	Parity	Marginal to good ability to find information
#3	Low	High	Bad	DoI
#4	Very High	Very High	Parity	DoI, processing, I/O or storage capability exceeded (aka DoS)

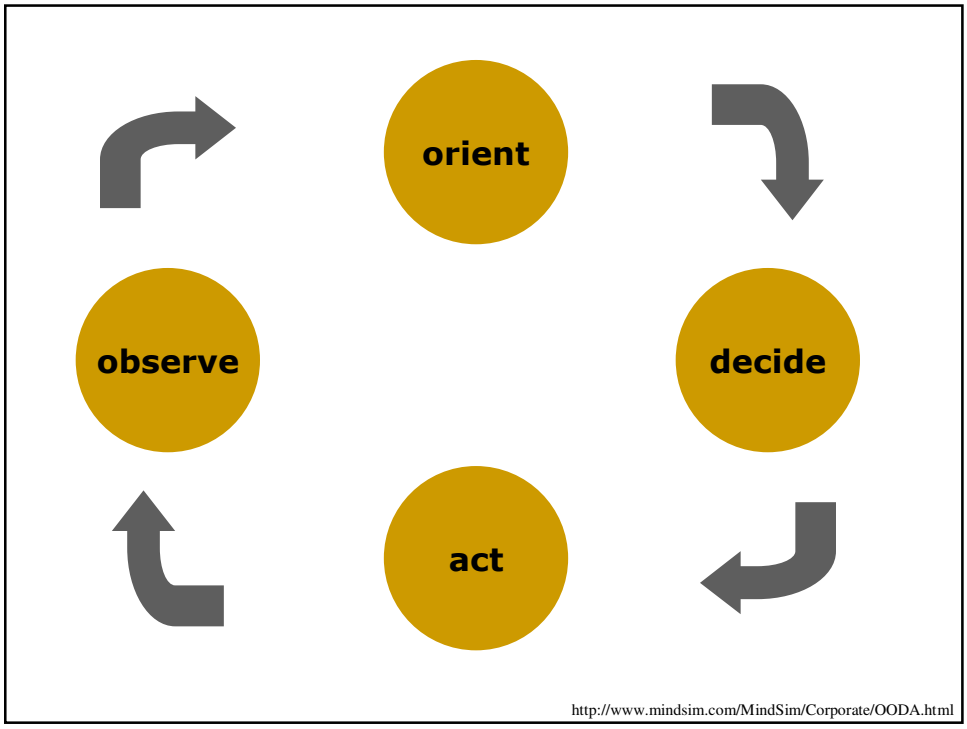


observe

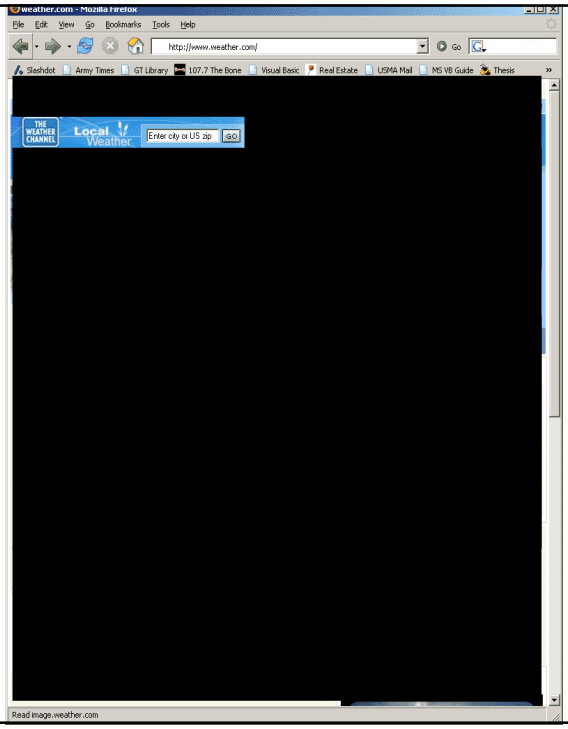
http://www.mindsim.com/MindSim/Corporate/OODA.html


orient
observe
http://www.mindsim.com/MindSim/Corporate/OODA.html


orient
observe
decide
http://www.mindsim.com/MindSim/Corporate/OODA.html



http://www.mindsim.com/MindSim/Corporate/OODA.html



Defense Taxonomy (Big Picture)

Legal	Lawsuits
	New Laws
Regulatory	Government Regulation
Moral	PR Campaign
	Code of Ethics
Cultural	Communities
Organizational	Topical counter-DoI groups
Financial	Increasing cost of DoI operations
Violence	Violence against DoI perpetrators
Technology	(see next slide)

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

Defense Taxonomy (Big Picture)

Legal	Lawsuits
	New Laws
Regulatory	Government Regulation
Moral	PR Campaign
	Code of Ethics
Cultural	Communities
Organizational	Topical counter-DoI groups
Financial	Increasing cost of DoI operations
Violence	Violence against DoI perpetrators
Technology	(see next slide)

Microsoft, AOL, Earthlink and Yahoo file 6 antispam lawsuits (Mar 04)

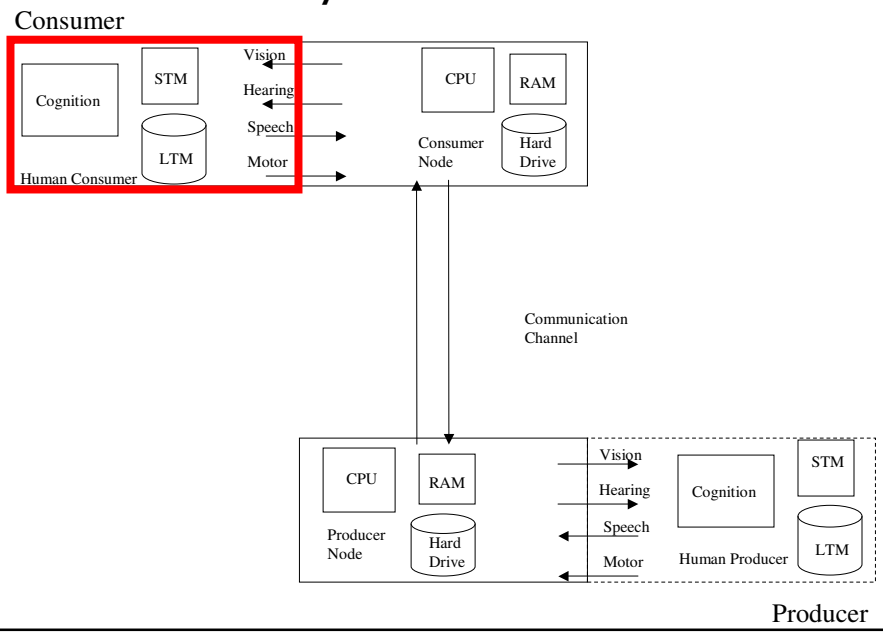
Federal Can Spam Legislation (Jan 04)

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

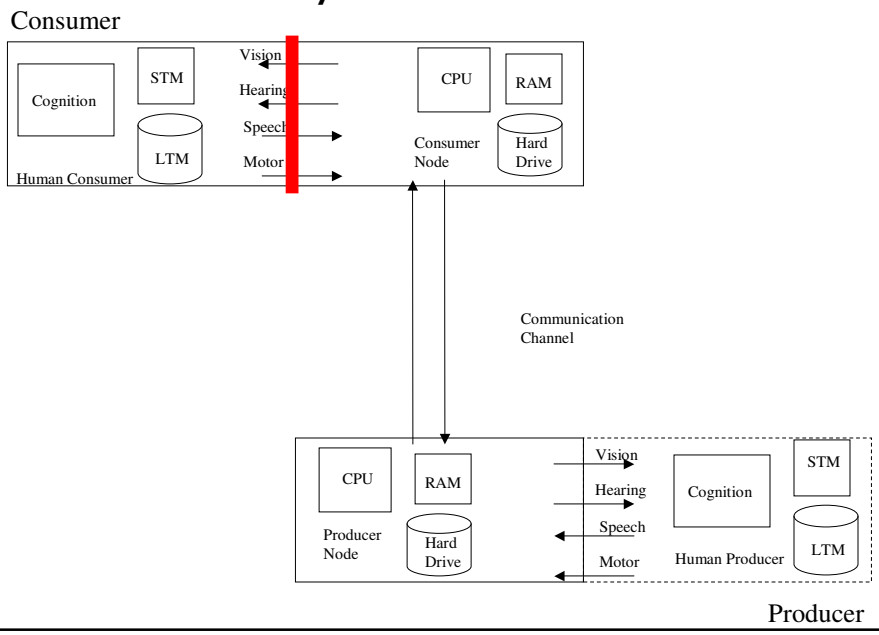
First Spam Conference (Jan 03)

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

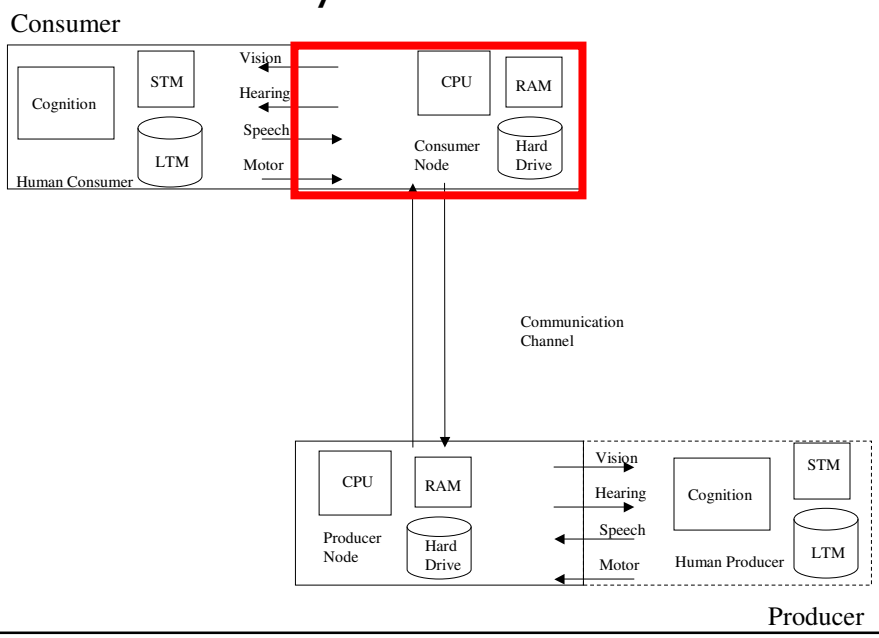
System Model



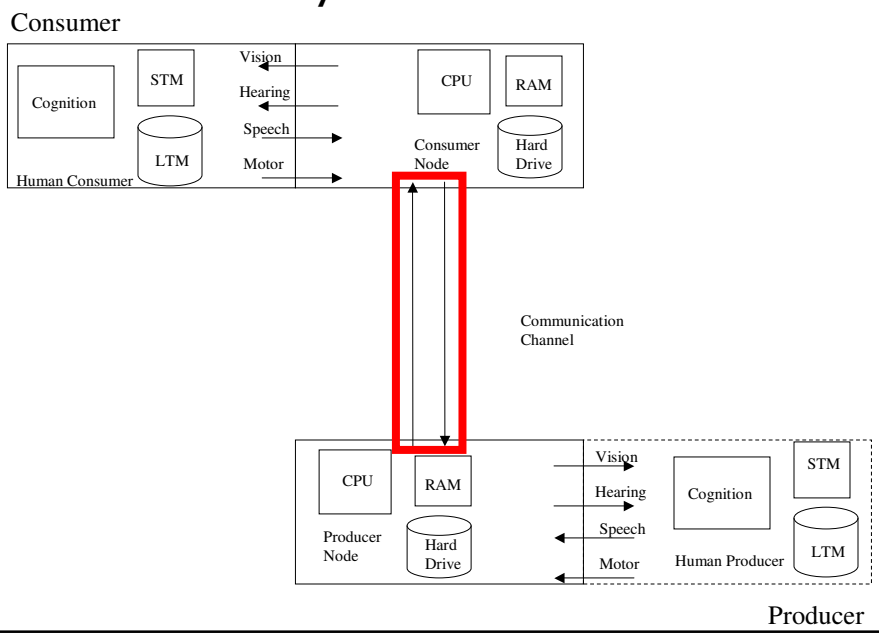
System Model



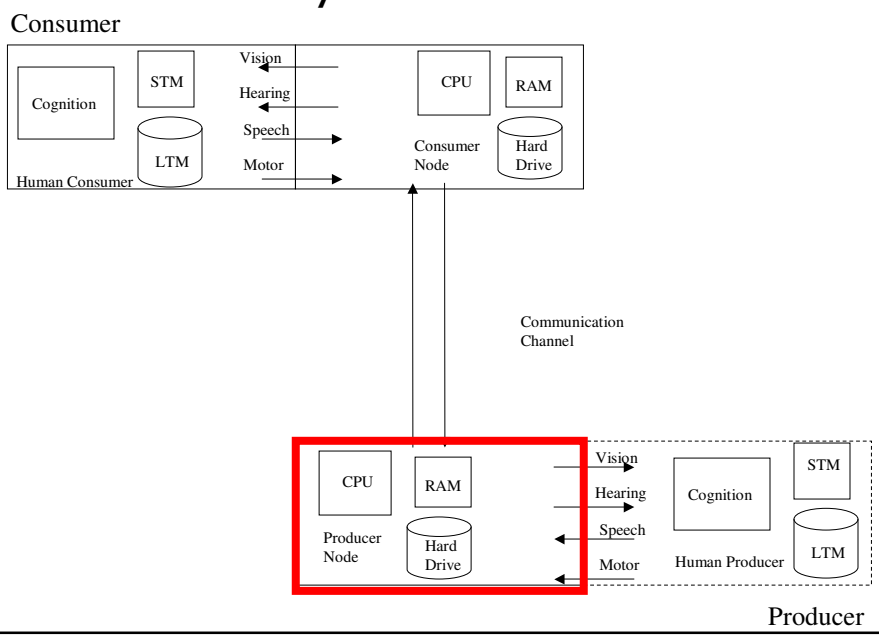
System Model



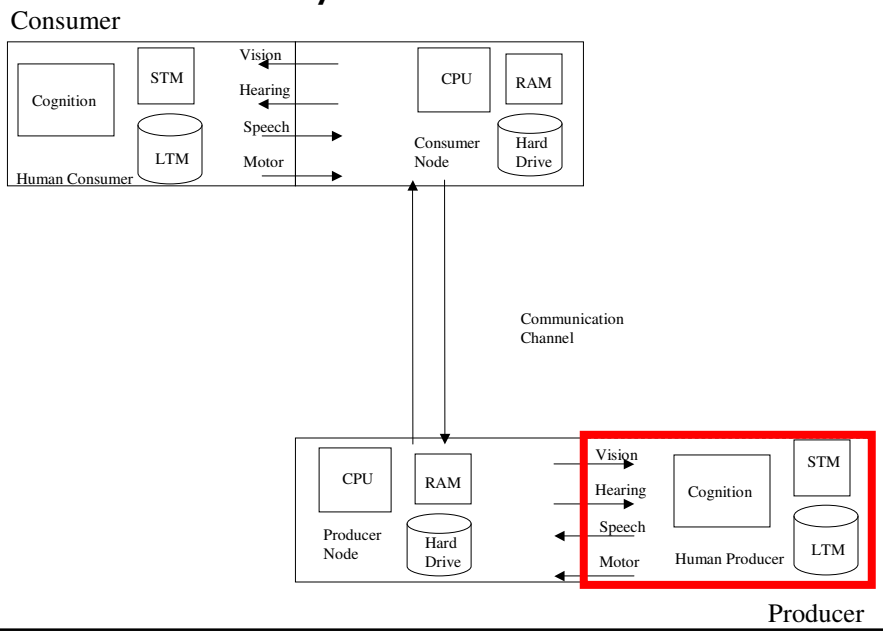
System Model

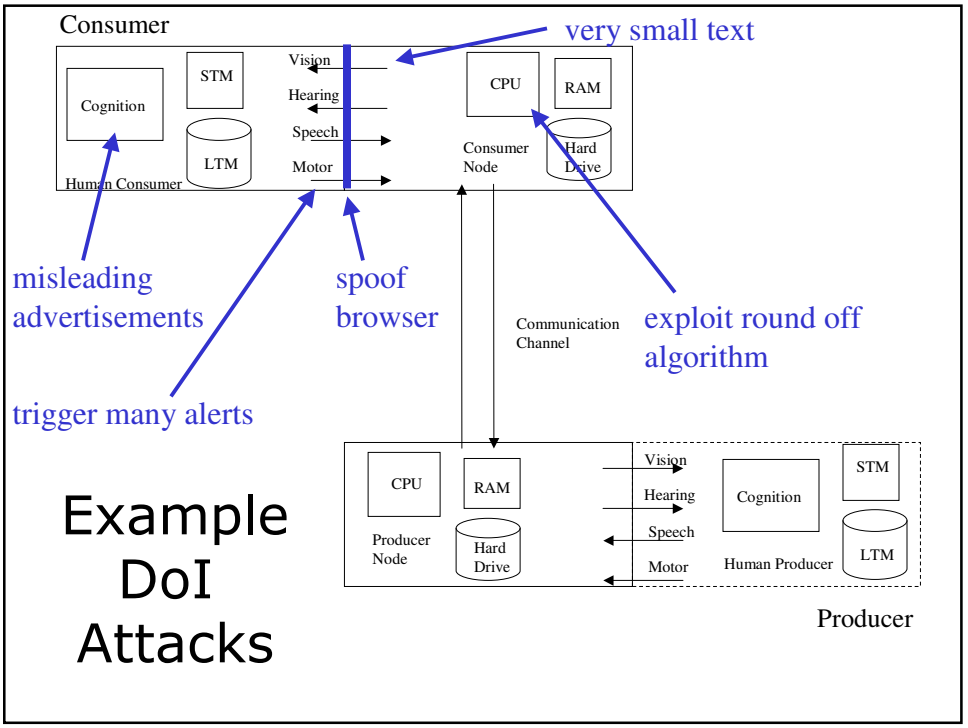


System Model



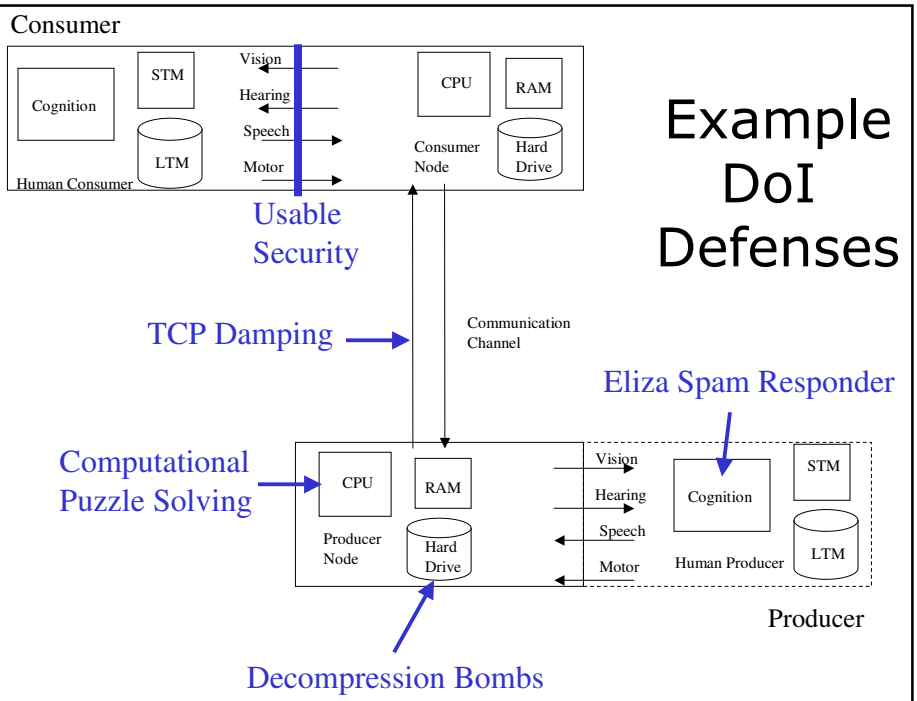
System Model





Example DoI Attacks

Example DoI Defenses



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/comments.pl?sid=150848&cid=12651434

For more information…

G. Conti and M. Ahamad; "A Taxonomy and Framework for Countering Denial of Information Attacks;" *IEEE Security and Privacy*. (to be published)

A Taxonomy and Framework for Countering
Denial of Information Attacks

Gregory Conti and Mustaque Ahamad

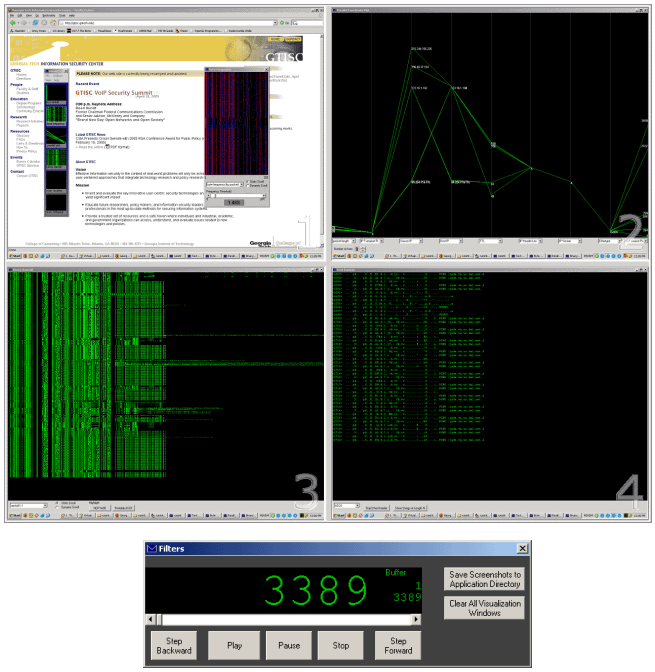
email me…

DoI Countermeasures in the Network Security Domain

information visualization *is the use of interactive, sensory representations, typically visual, of abstract data to reinforce cognition.*

http://en.wikipedia.org/wiki/Information_visualization

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:

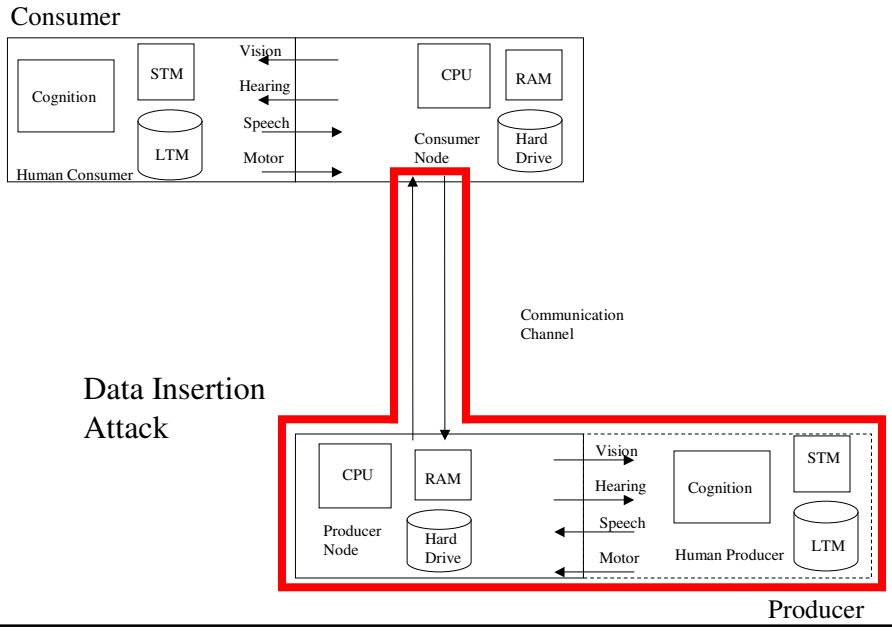
- Inserting relatively small amounts of malicious data into dataset (not DOS)
- Altering timing of data

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

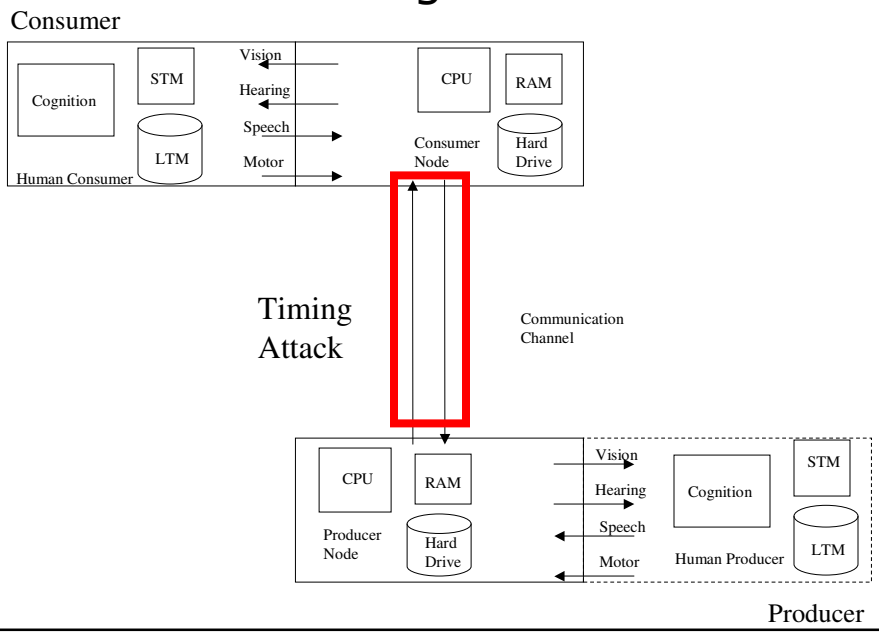
Attack Domains…

- Network traffic
- Usenet
- Blogs
- Web Forms
- syslog
- Web logs
- Air Traffic Control

Data Generation Vector

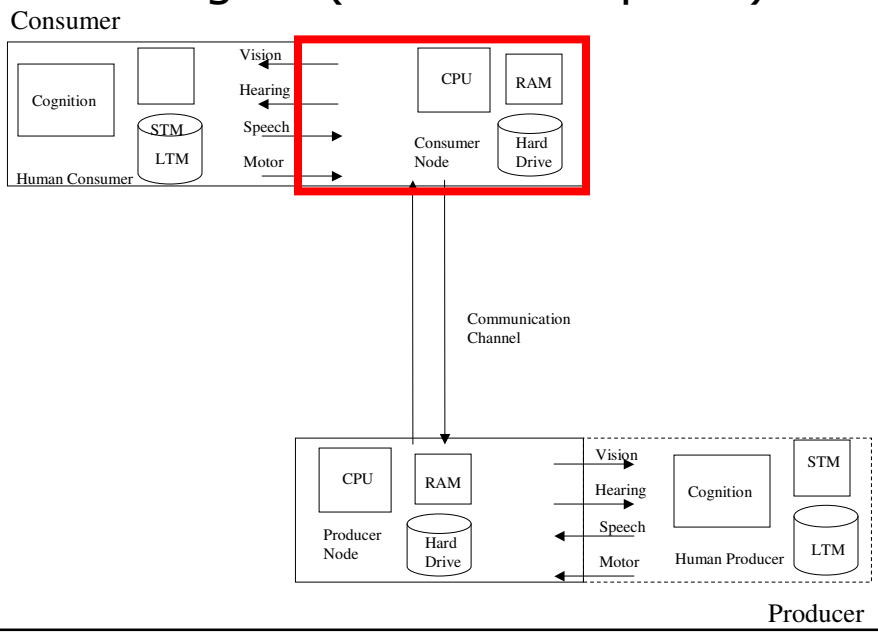


Timing Vector



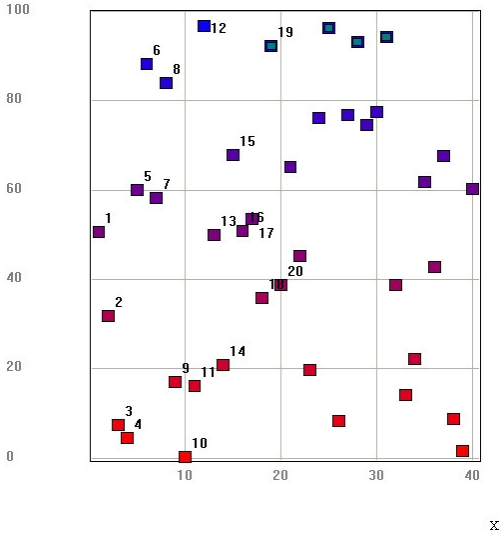
Attack Manifestations

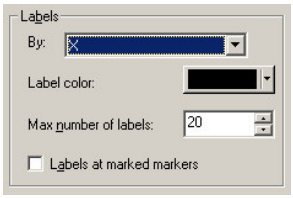
Targets (User's Computer)



Labeling Attack

(algorithm)

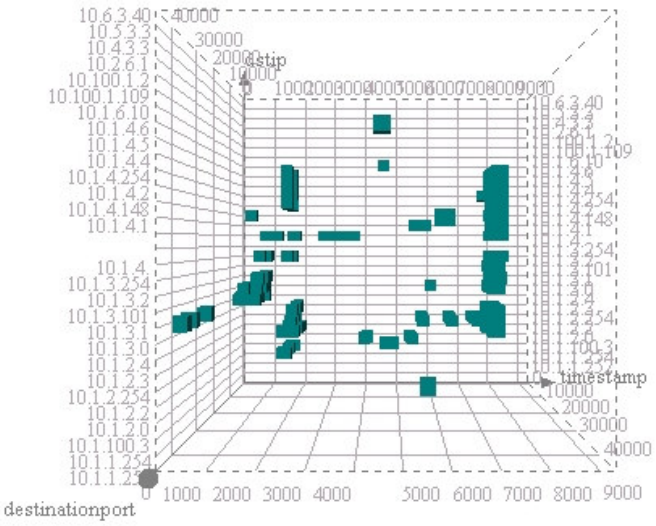




- 100 elements
- X = 1..100
- Y = rand() x 10

Labeling Attack

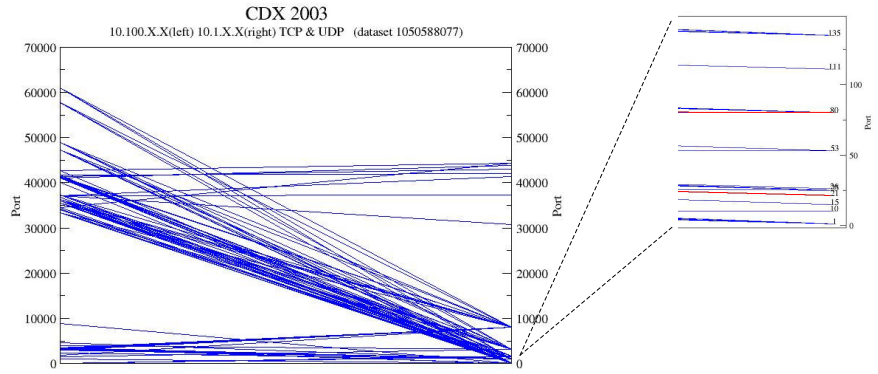
(algorithm)



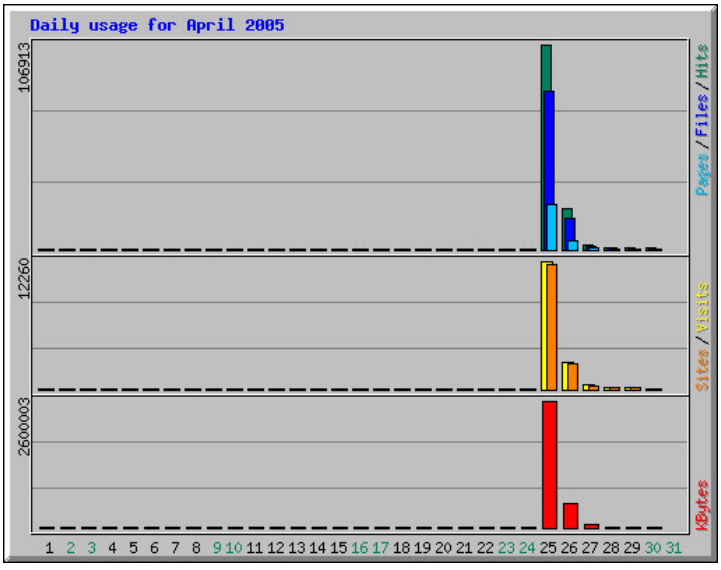
CDX 2003 Dataset
X = Time
Y = Destination IP
Z = Destination Port

AutoScale Attack/Force User to Zoom

(algorithm)



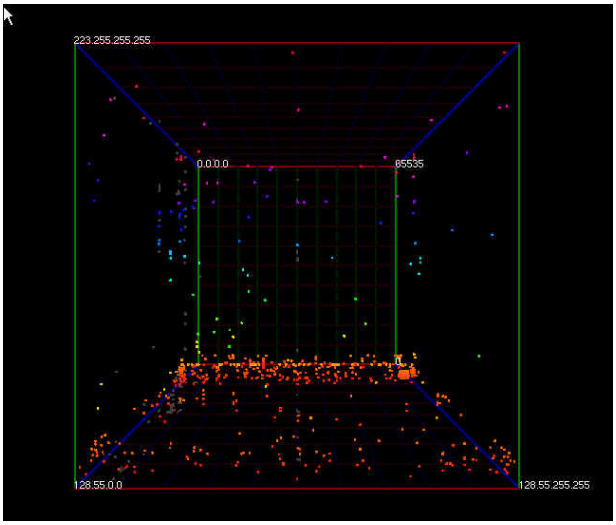
Autoscale



http://www.neti.gatech.edu/

Precision Attack

(algorithm)

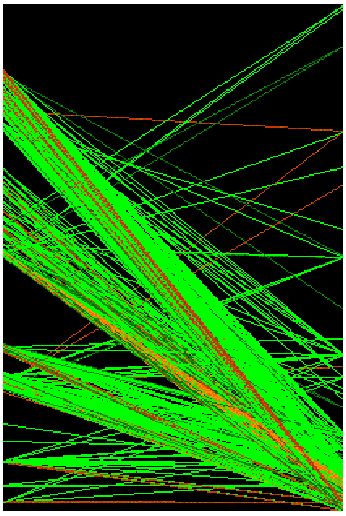


http://www.nersc.gov/nusers/security/Cube.jpg

http://developers.slashdot.org/article.pl?sid=04/06/01/1747223&mode=thread&tid=126&tid=172

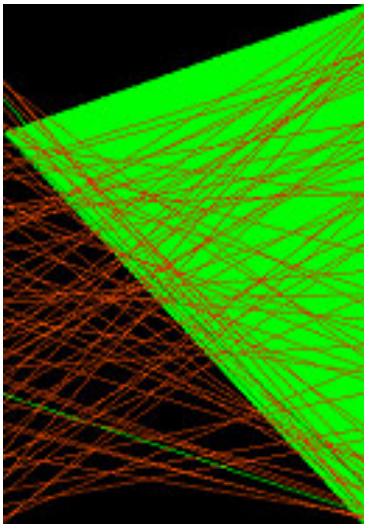
Occlusion

(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…

G. Conti, M. Ahamad and J. Stasko; "Attacking Information Visualization System Usability: Overloading and Deceiving the Human;" *Symposium on Usable Privacy and Security (SOUPS)*; July 2005.

See also www.rumint.org for the tool.

Attacking Information Visualization System Usability
Overloading and Deceiving the Human

Gregory Conti
College of Computing
Georgia Institute of Technology

Mustaque Ahamad
College of Computing
Georgia Institute of Technology

John Stasko
College of Computing
Georgia Institute of Technology

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
  - http://www.cs.dartmouth.edu/~doug/mdmspe.pdf
- Semantic Hacking
  - http://www.ists.dartmouth.edu/cstrc/projects/semantic-hacking.php

Demo

http://www.defcon.org/images/graphics/PICTURES/defcar1.jpg

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

CACM

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

http://www.silverballard.co.nz/content/images/shop/accessories/cd/blank%20stock/41827.jpg

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, Kenshoto, 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.

GEORGIA TECH INFORMATION SECURITY CENTER

- **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