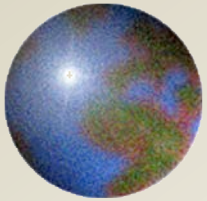


Beyond the Noise:

More Complex Issues with Incident Response

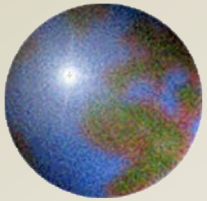
IFIP WG Meeting, June 30, 2006

David Dittrich

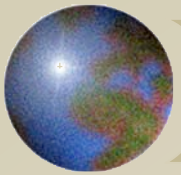
Center for Information Assurance and Cybersecurity/
The Information School
University of Washington

Agenda

- Conceptual foundation
- Some roadblocks to mitigation
- Three Case studies
- What to do?
- Conclusions



Conceptual Foundation



The Problems

- "Malware" deployed regularly on 100,000s of computers world-wide
  - Typical .edu has hundreds per month
- IP theft, CC theft, DDoS attacks on the rise
- *New methods developed constantly*
- *Concealment increasing in sophistication*

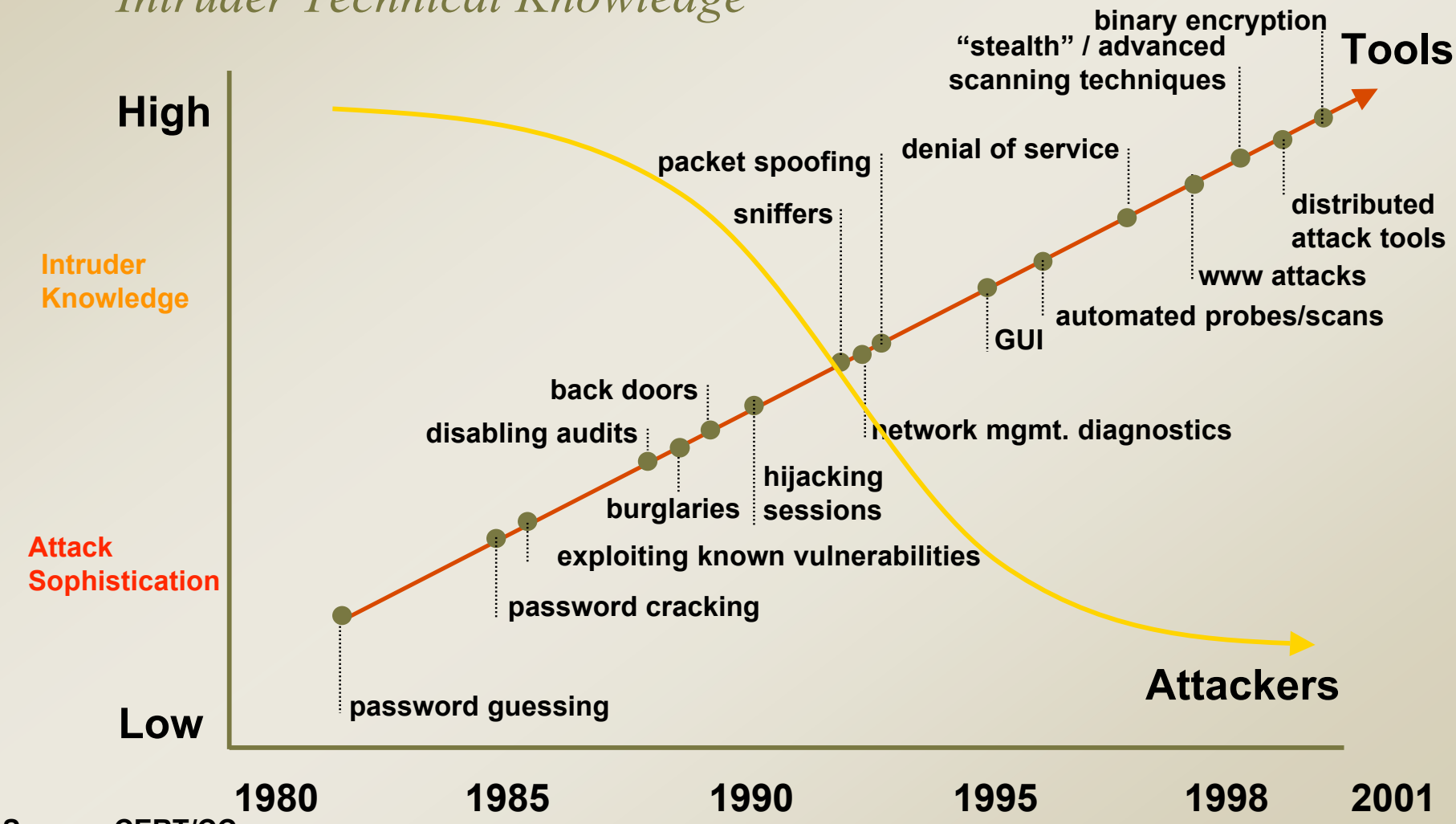
The Problems (cont)

- Attackers are winning
  - Less knowledge/more damage
  - More focus/drive
  - Time to attack: seconds
  - Time to mitigate: days, weeks…
- Number of incidents overwhelming IRTs
- LE swamped with cases

"Trends in Denial of Service Attack Technologies", by CERT/CC
http://www.cert.org/archive/pdf/DoS_trends.pdf

Increasing Attack Sophistication

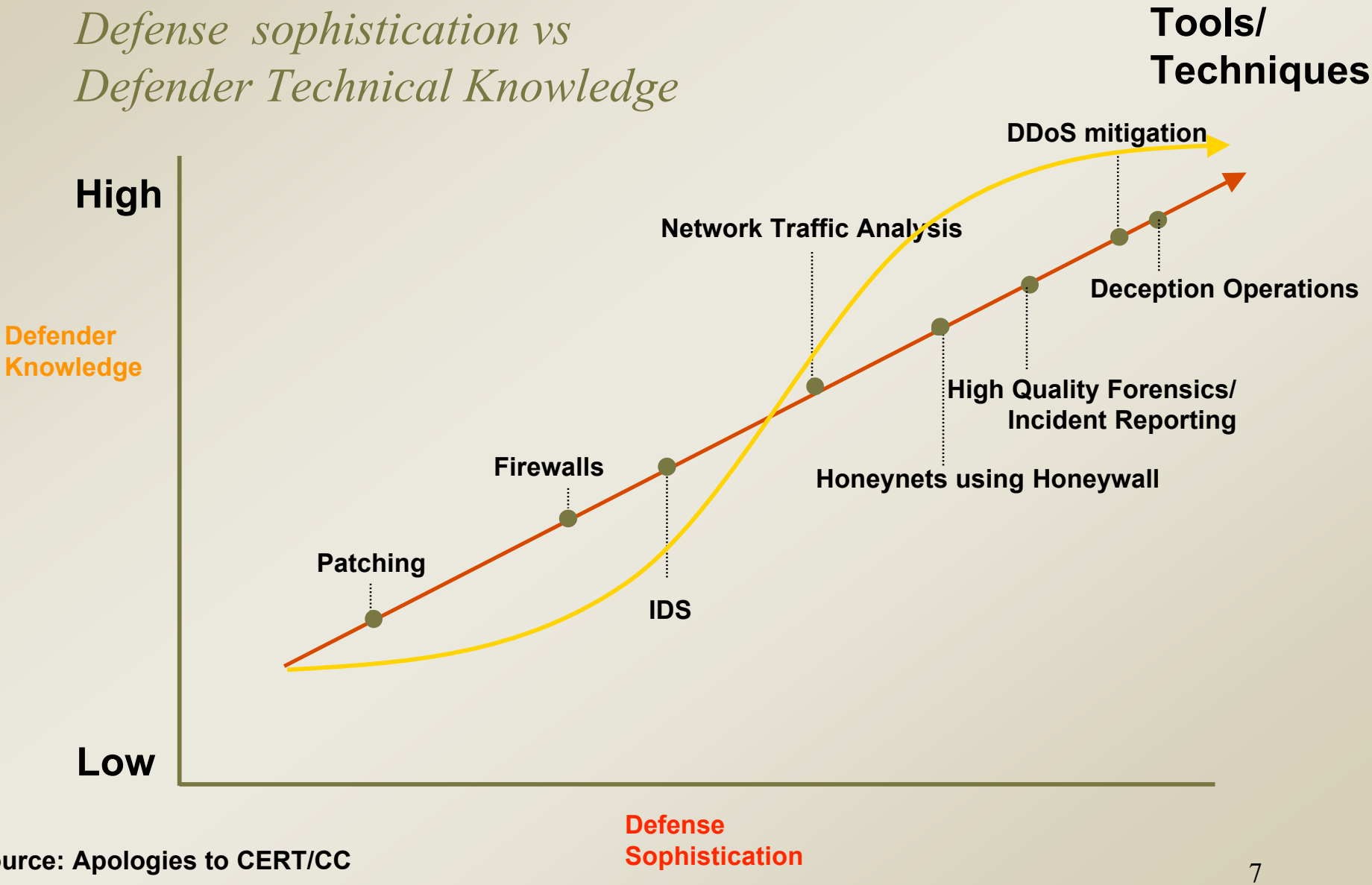
Attack sophistication vs
Intruder Technical Knowledge



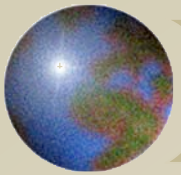
Source: CERT/CC

Defense Sophistication

Defense sophistication vs Defender Technical Knowledge



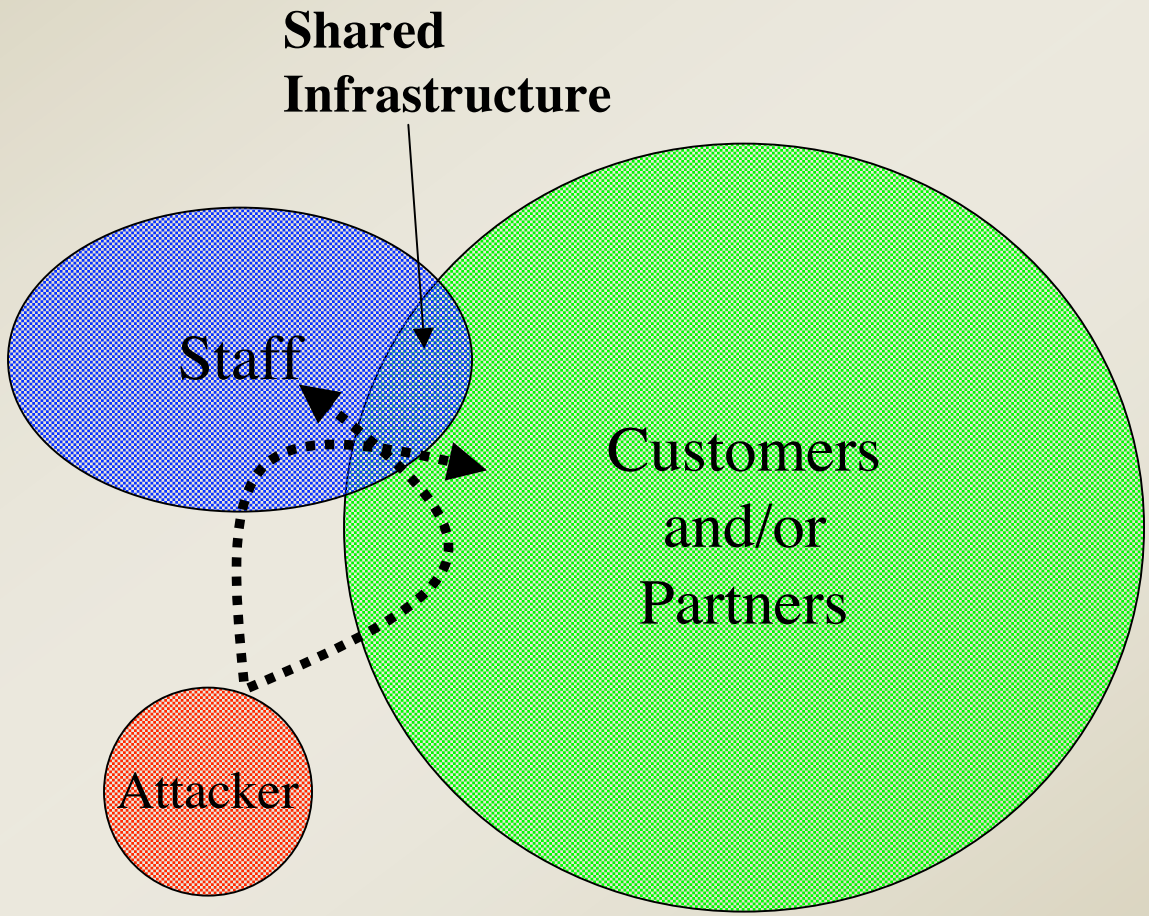
Source: Apologies to CERT/CC

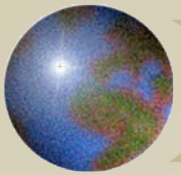


Targets of exploitation

- Passwords (direct/indirect)
- Trust relationships
- Complexity
- Differentials in ability to respond
- Time zone, language, laws…

Target Surface and Attack Paths

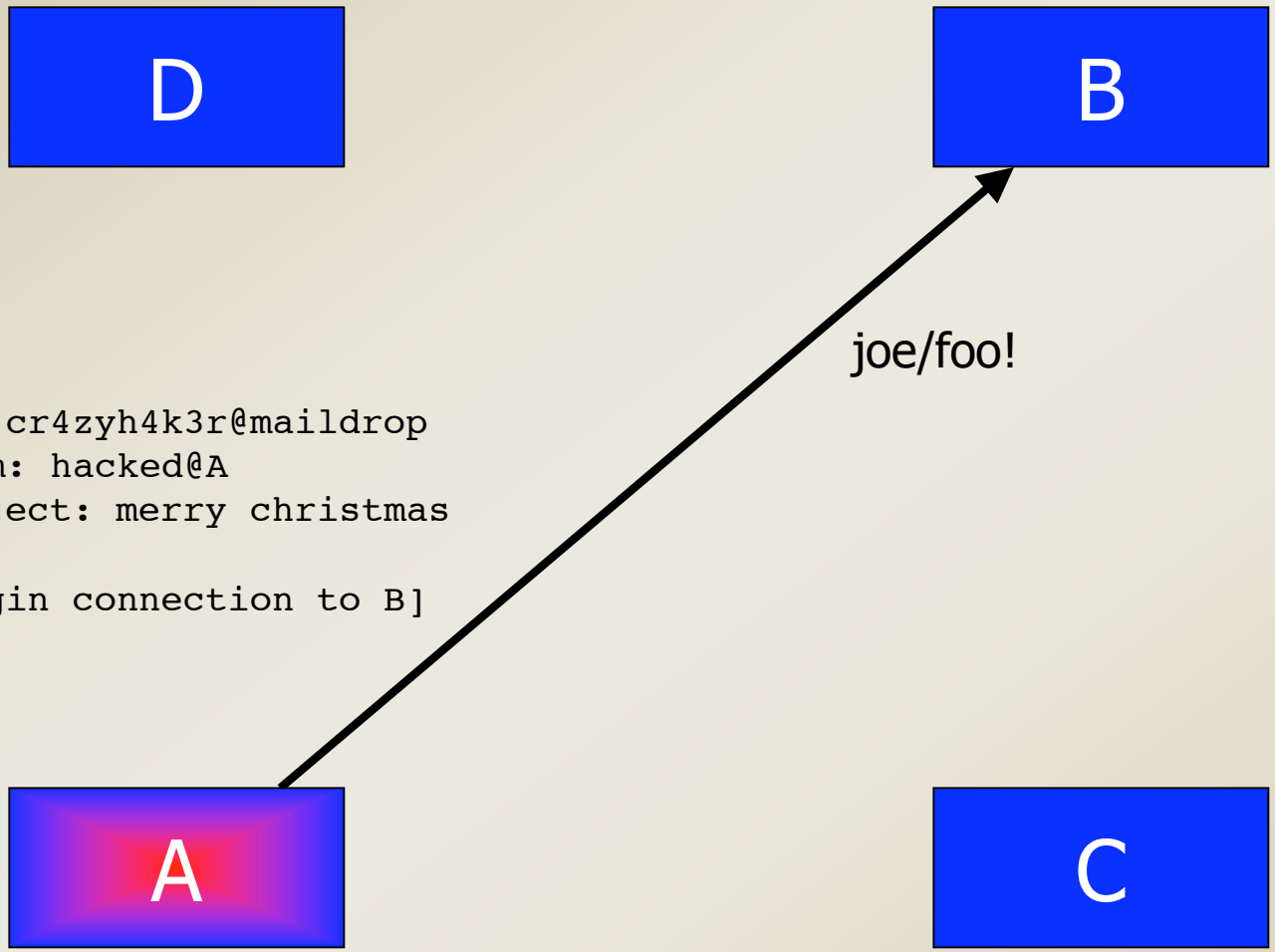




Trust relationships

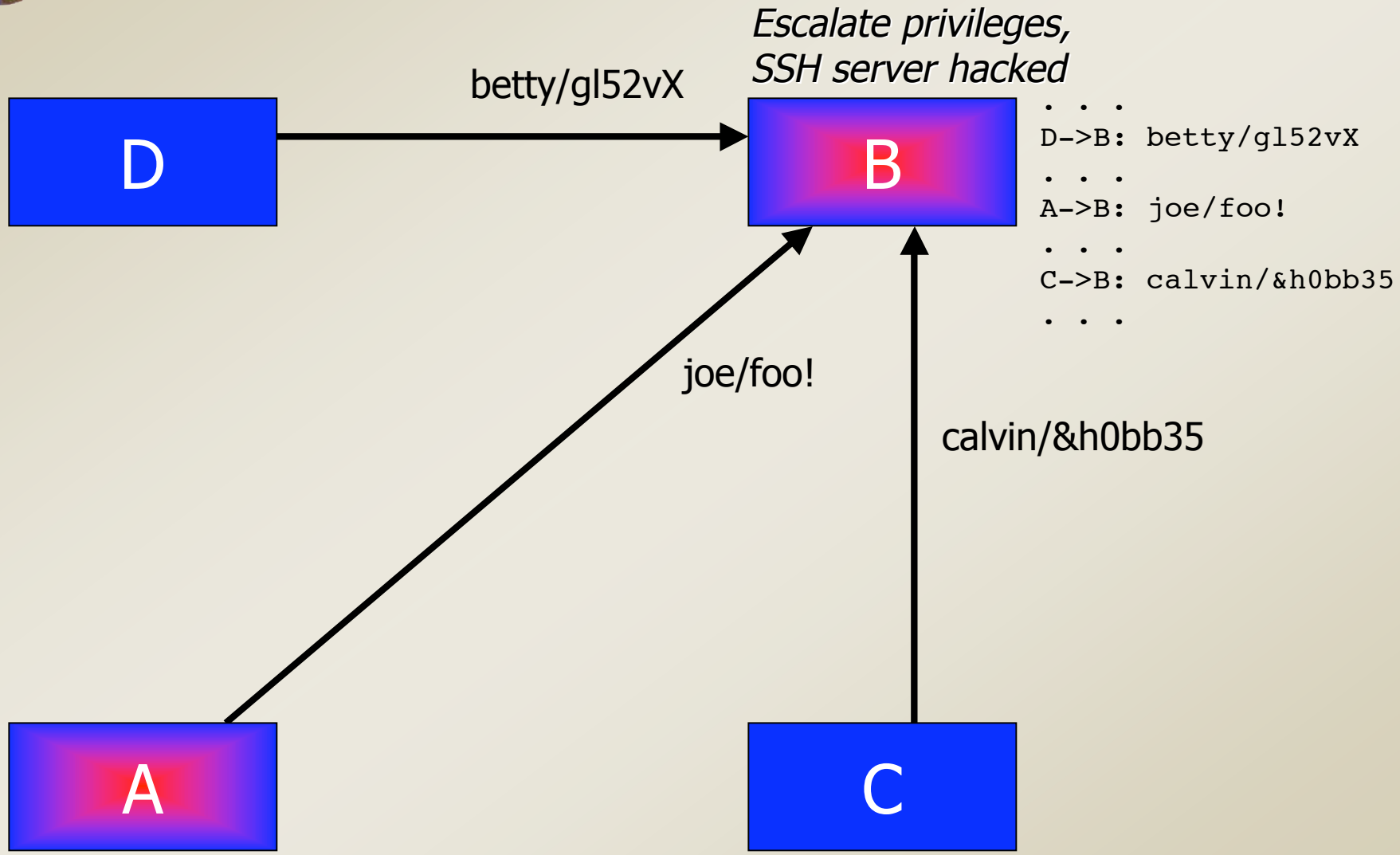
- Client<->Server
- IP based ACLs
- Shared password/symmetric key
- Shared network infrastructure
- Sensitive data in email
- Sensitive files on servers

Exploiting Trust Relationships

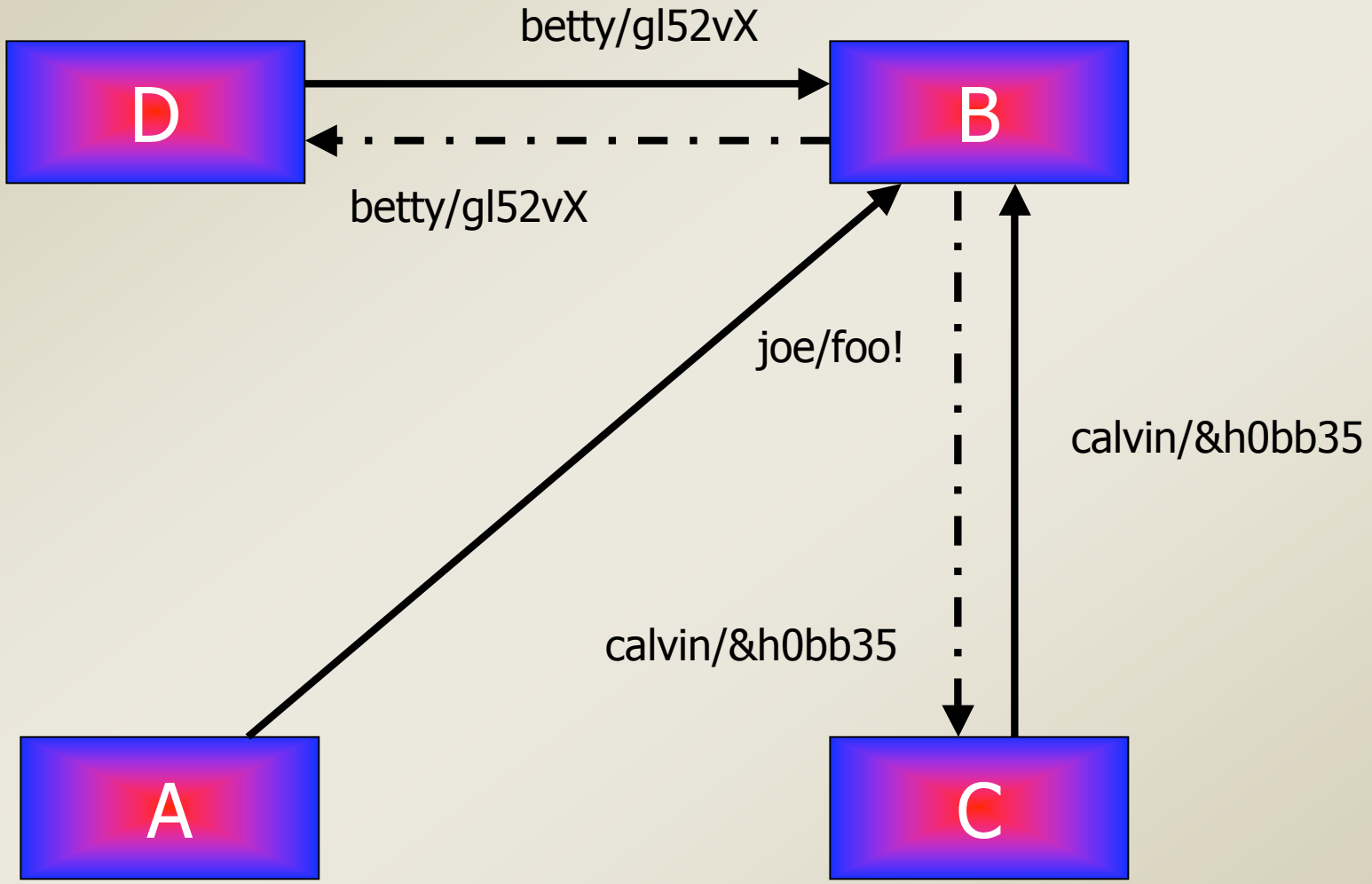


Email attached
Key logger trojan

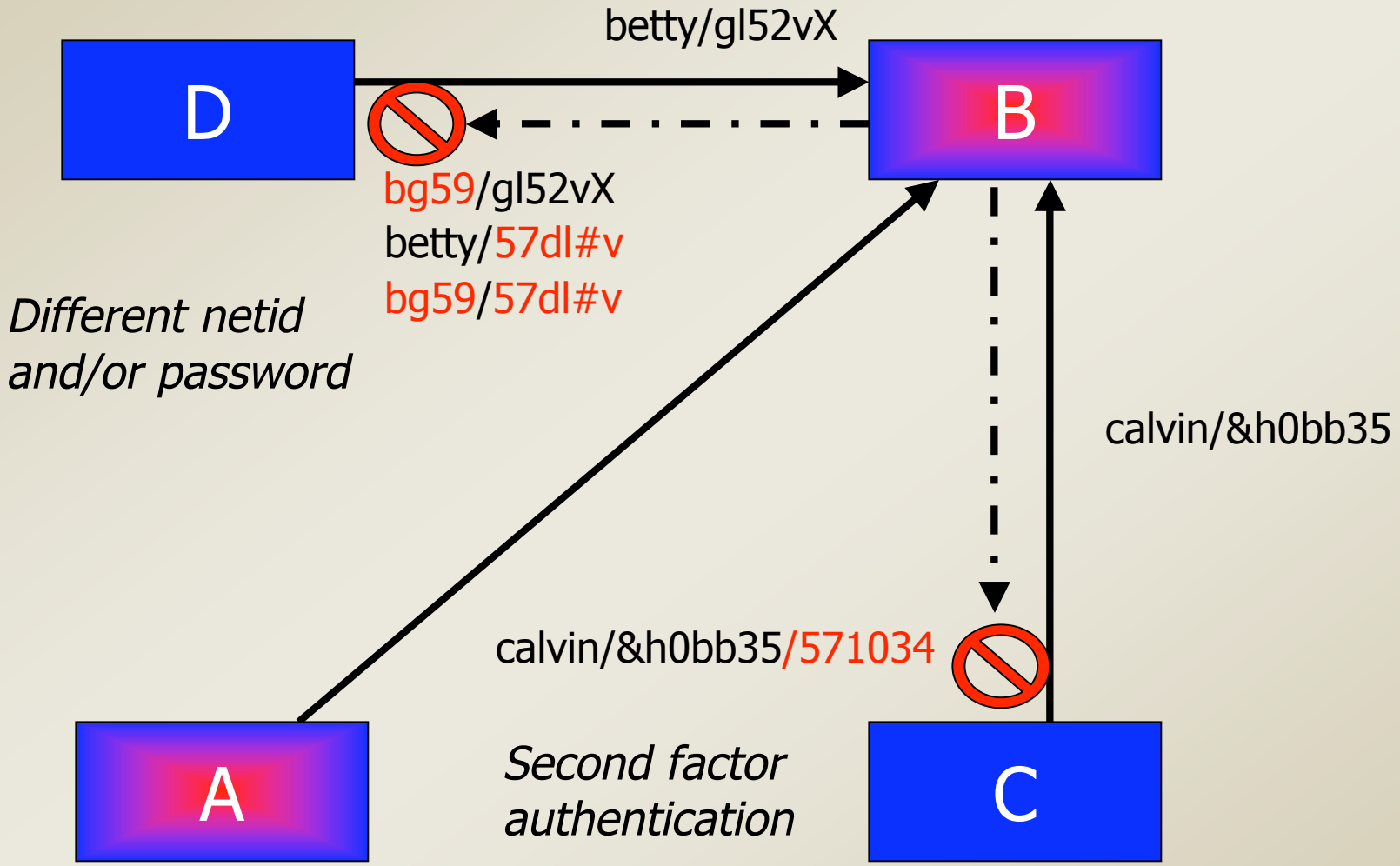
Exploiting Trust Relationships (2)



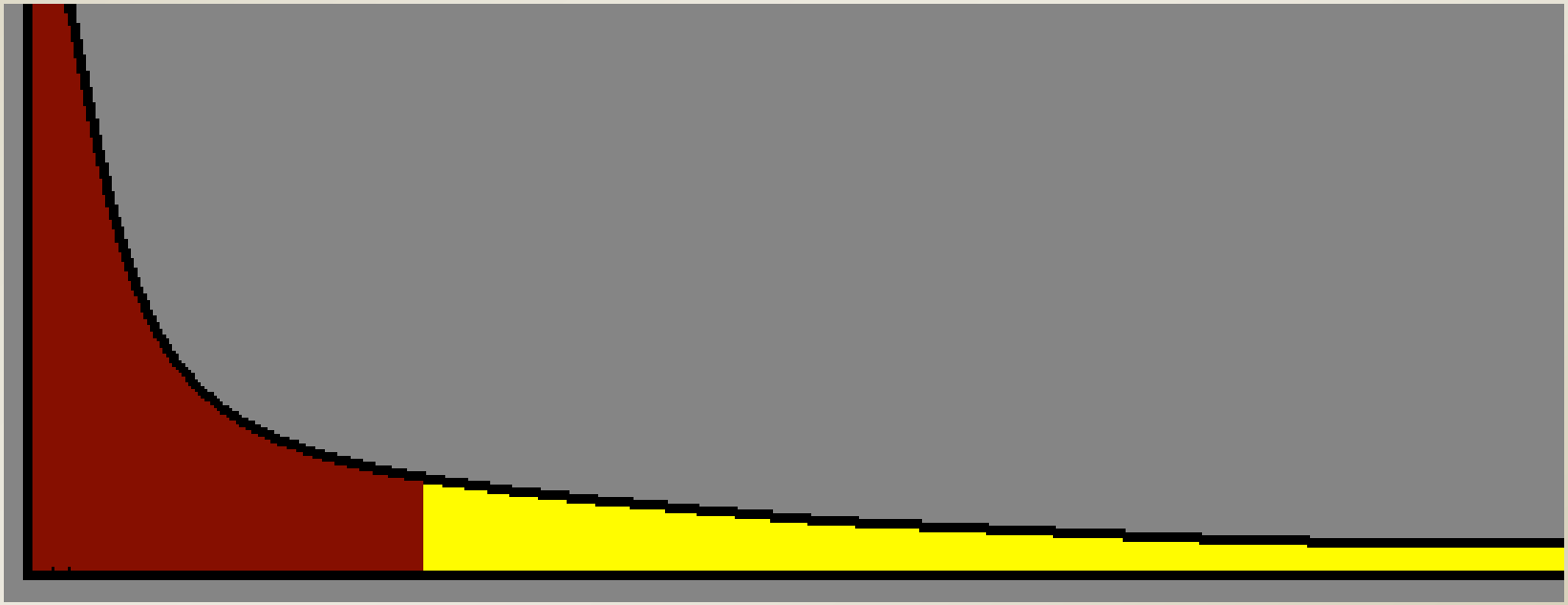
Exploiting Trust Relationships (3)



Two Defense Strategies

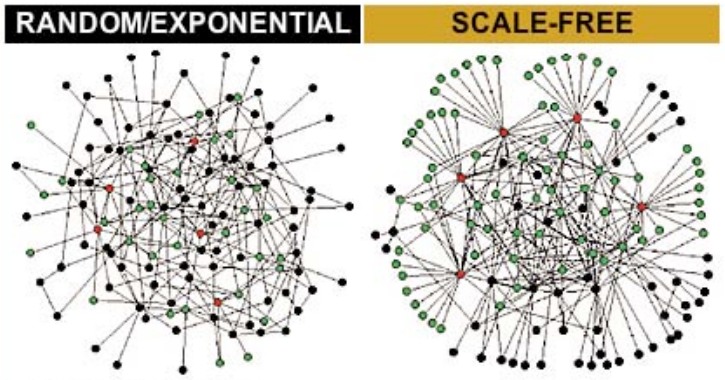


The "Long Tail"

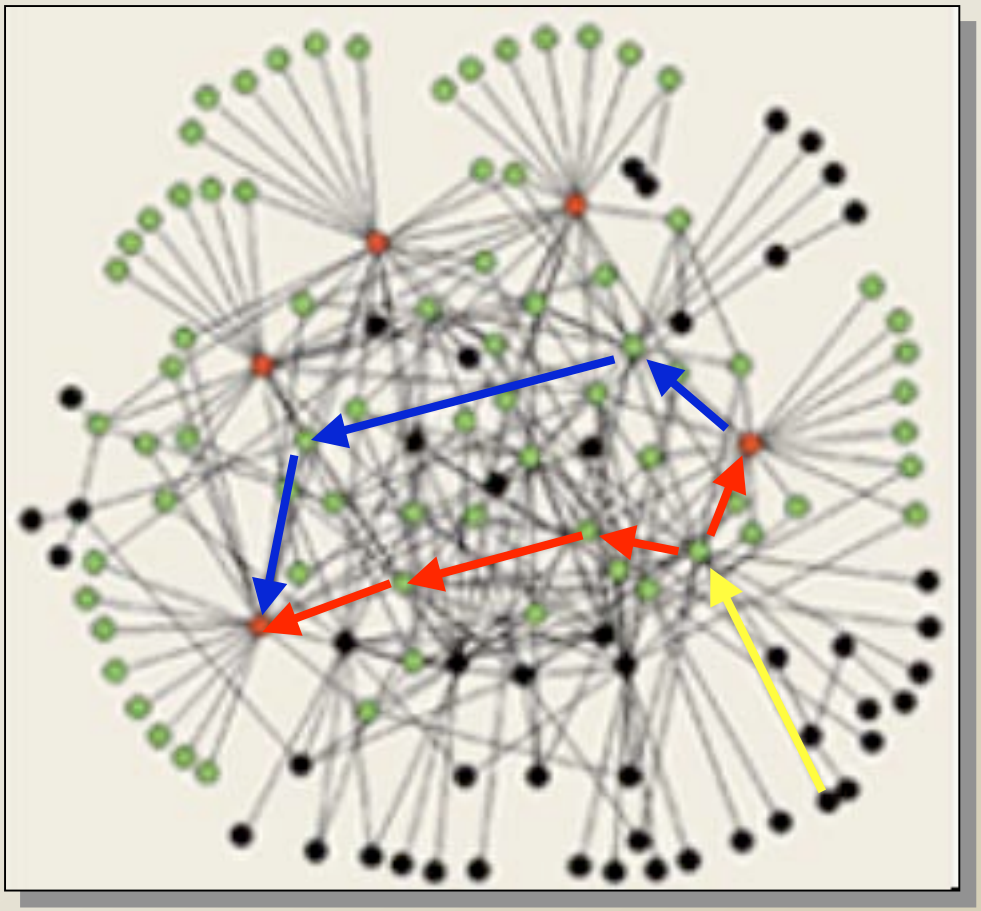


Scale-free networks and trust relationships

Comparing Random and Scale-Free Distribution
In the random network, the five nodes with the most links (in red) are connected to only 27% of all nodes (green). In the scale-free network, the five most connected nodes (red) are connected to 60% of all nodes (green).

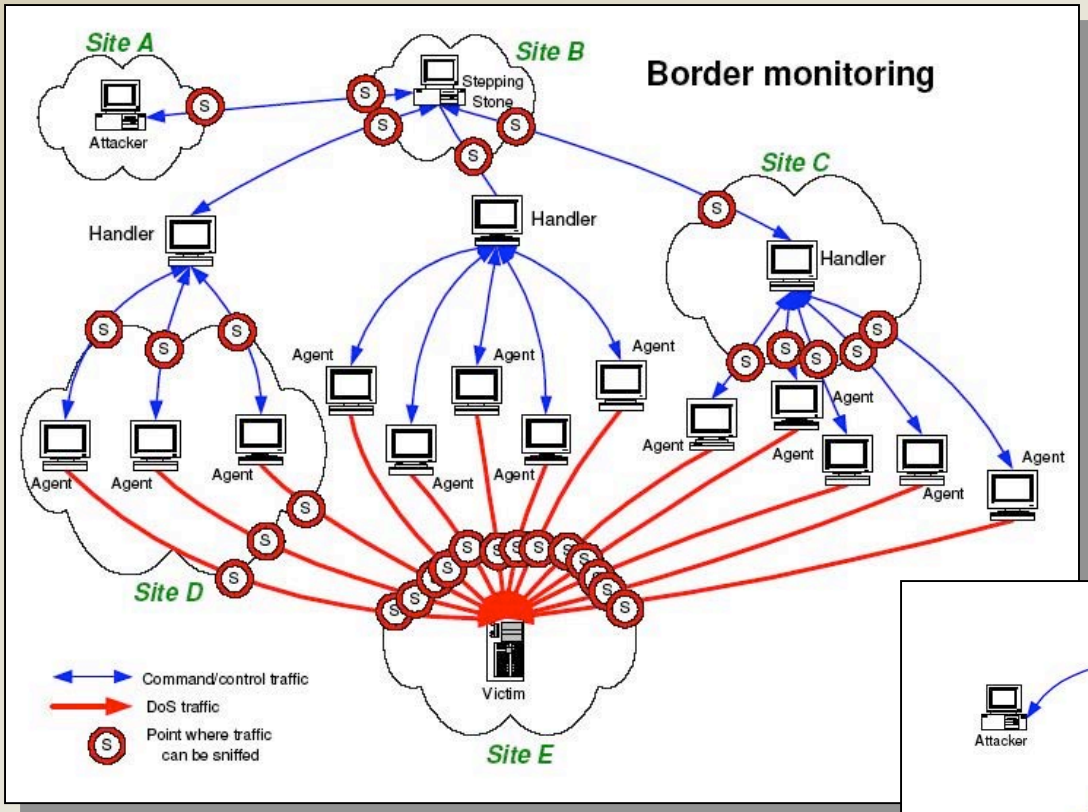


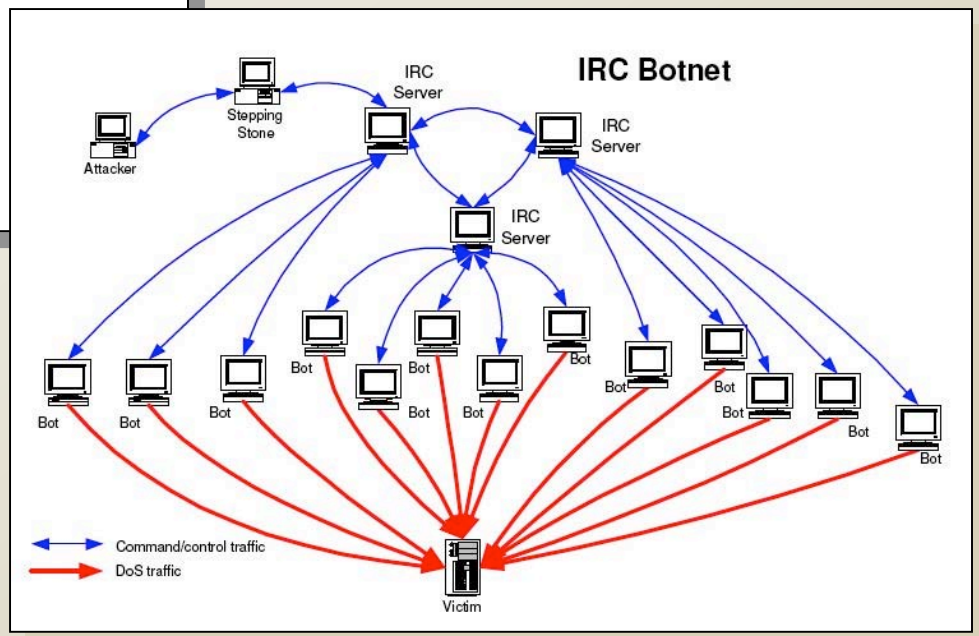
Source: the journal Nature

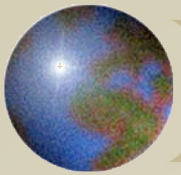


http://www.computerworld.com/networkingtopics/networking/story/0,10801,75539,00.html

Classic Handler/Agent vs. IRC Botnet

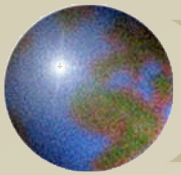






From just 1 host…

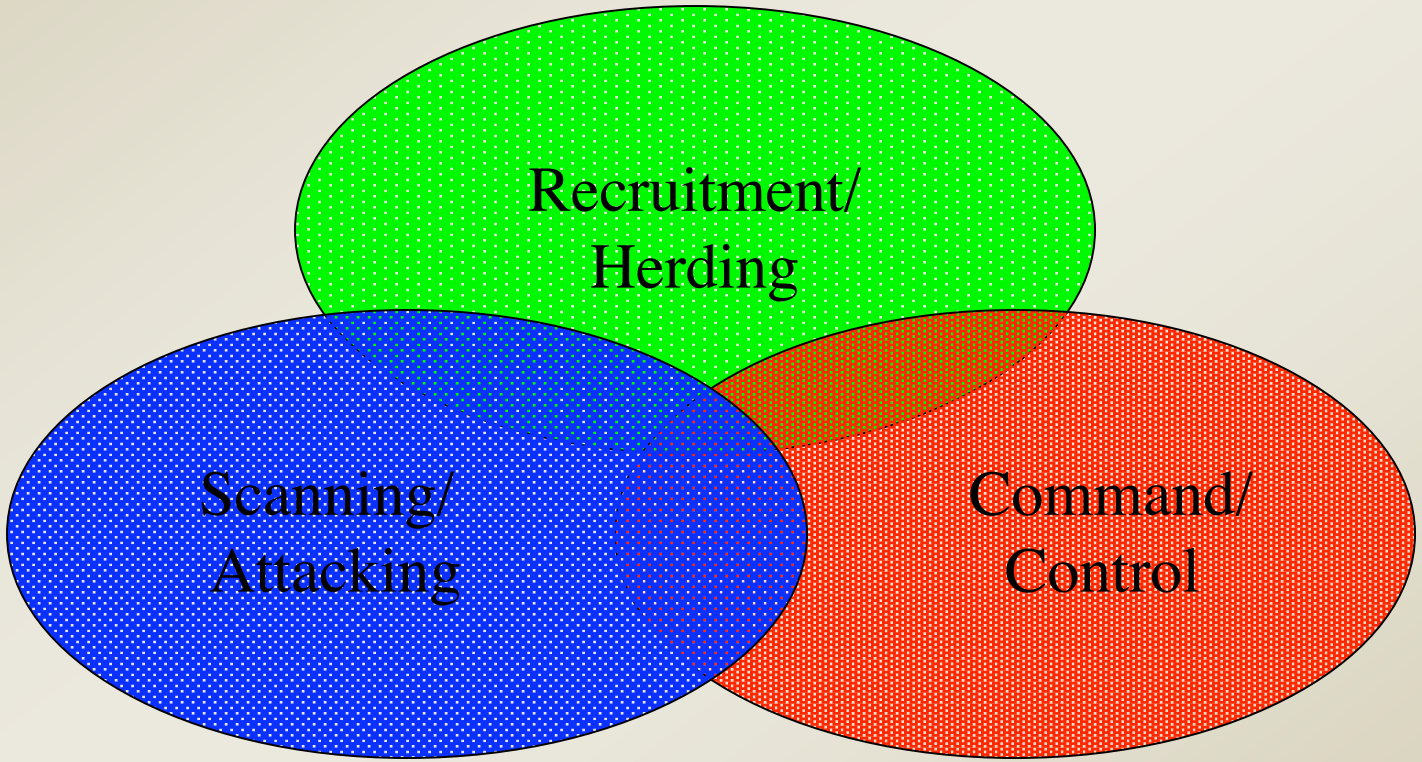
```
DumpFile:  /log/core02-02.dump
FileSize: 386.15MB
Id: 200204292150
StartTime: Mon Apr 29 21:50:44 2002
EndTime:   Mon Apr 29 21:54:45 2002
TotalTime: 240.57 seconds
TotalCapSize: 312.60MB  CapLen: 68 bytes
# of packets: 4820393 (418.34MB)
AvgRate: 28.12Mbps  stddev:8.00M   PeakRate: 40.08Mbps

### IP flow (unique src/dst pair) Information ###
# of flows: 15  (avg. 321359.53 pkts/flow)
Top 10 big flow size (bytes/total in %):
 100.0%  0.0%  0.0%  0.0%  0.0%  0.0%  0.0%  0.0%  0.0%  0.0%

### IP address Information ###
# of IPv4 addresses: 15
Top 10 bandwidth usage (bytes/total in %):
 100.0% 100.0%  0.0%  0.0%  0.0%  0.0%  0.0%  0.0%  0.0%  0.0%
```



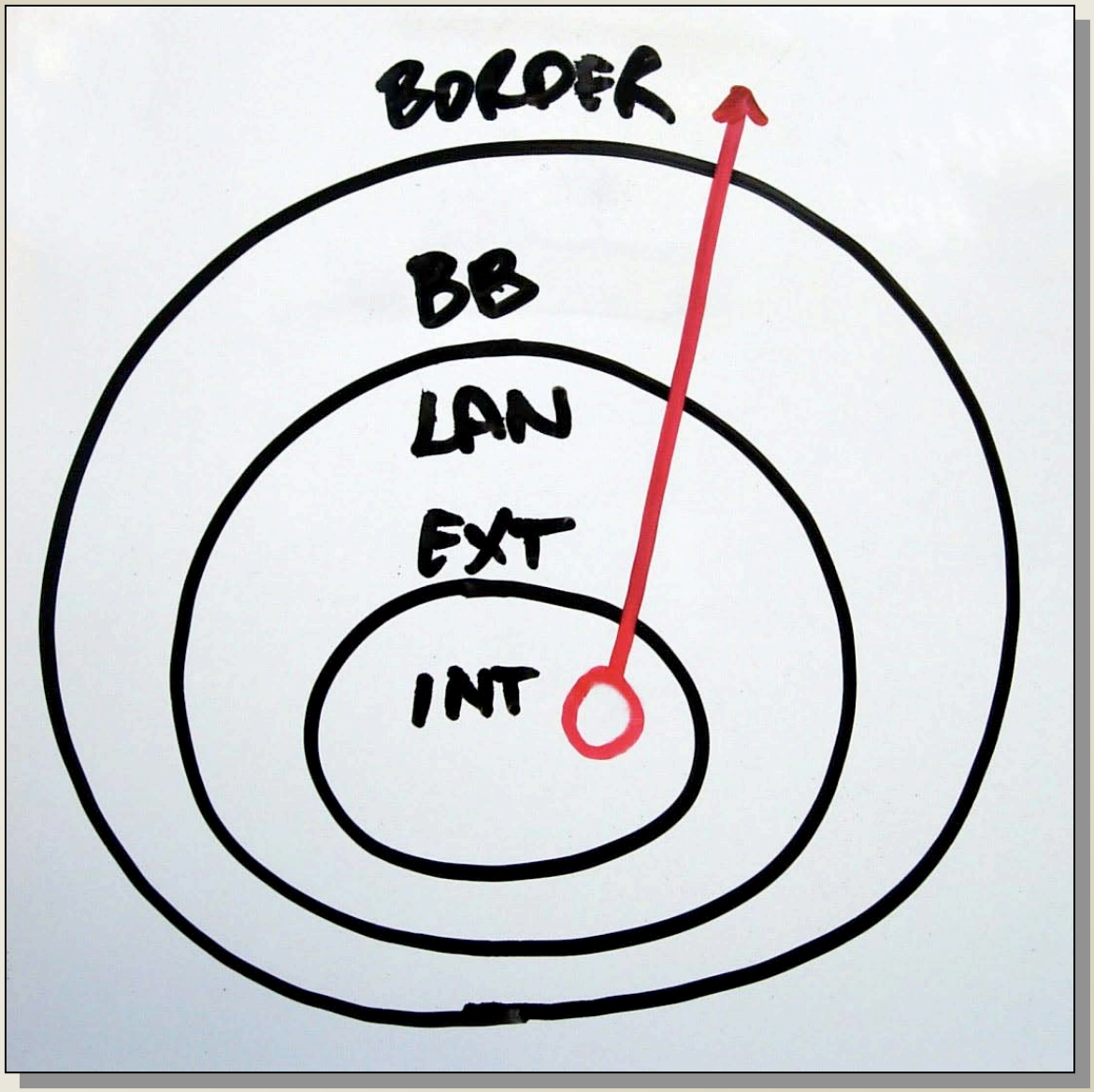
Bots needed for given attack

With this many hosts…	What can you do?
O(10^1)	Take out router via PPS flood, multicast table overflow, or “one packet kill” attack
O(10^2)	Take out TCP service via SYN flood
O(10^3)	Take out web server by excessive requests
O(10^4)	Defeat load balancing; Do reflected DoS attack (e.g., w/DNS)
O(10^5)	Bypass scrubbers
O(10^6)	Whatever you want

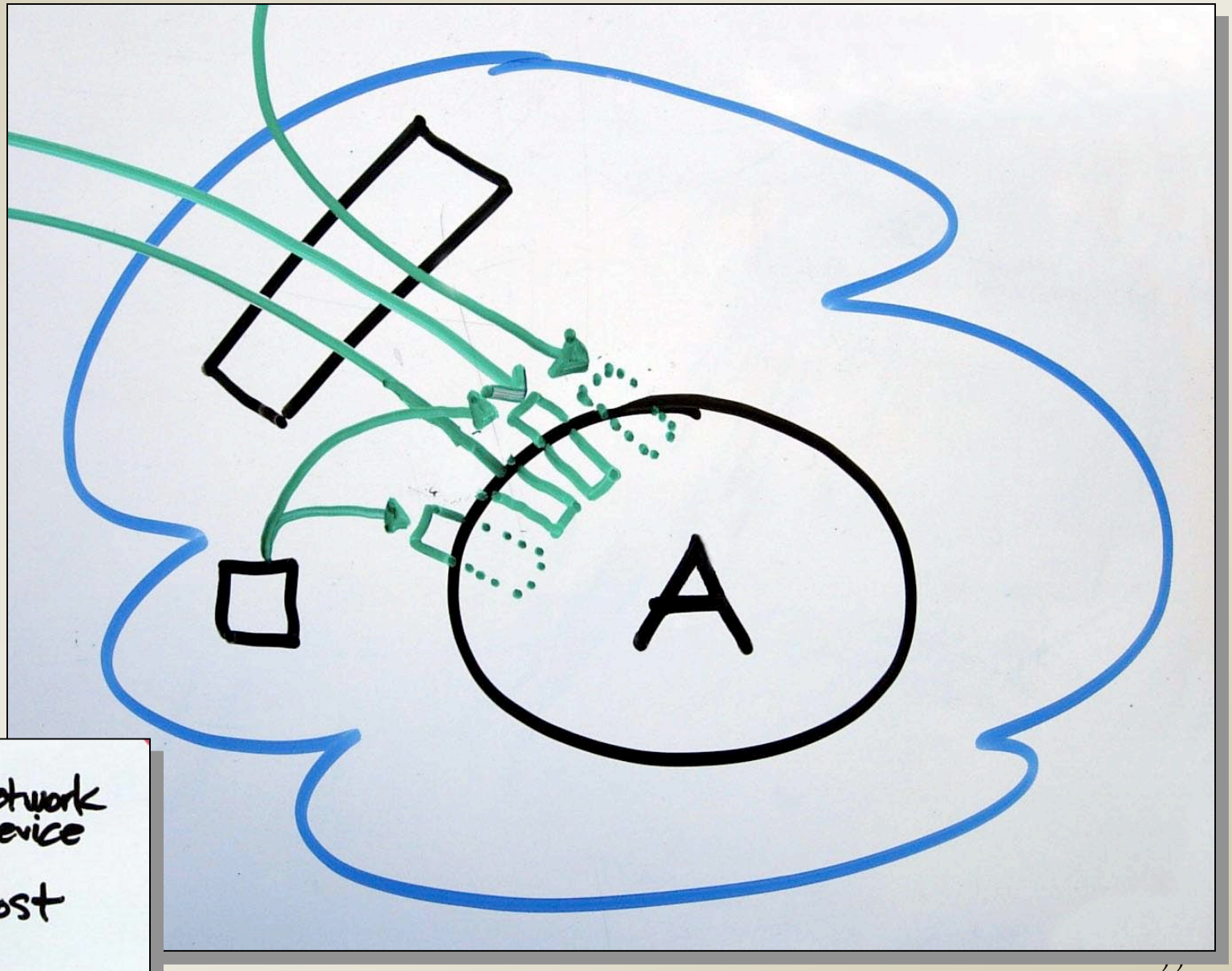
Weaknesses in botnets

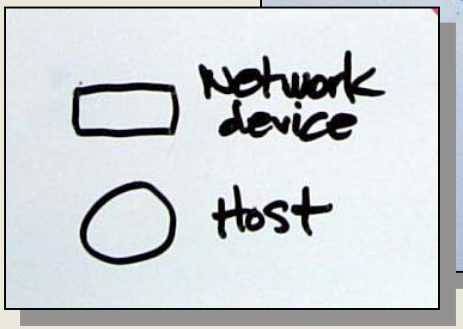


Proximity and Perspective

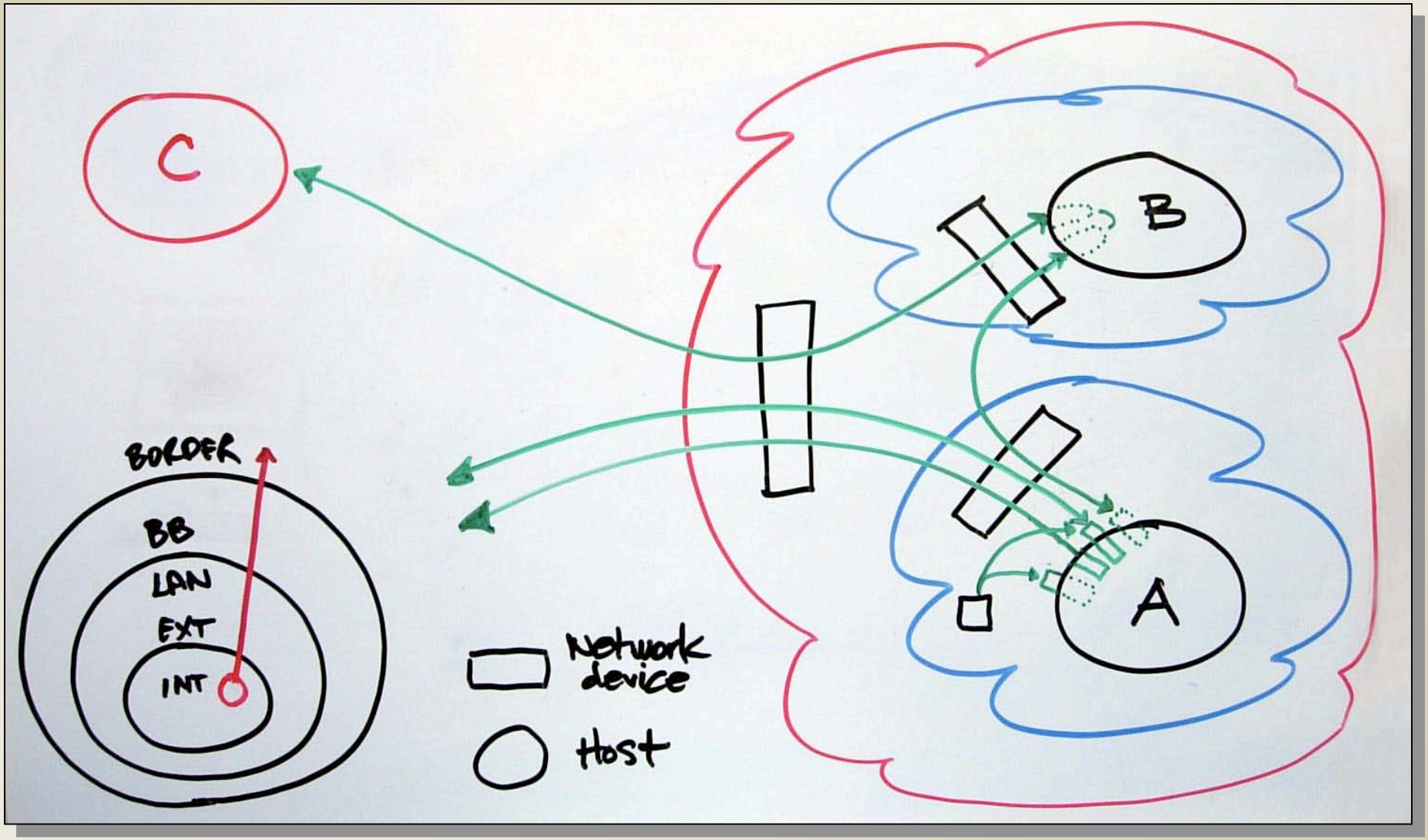


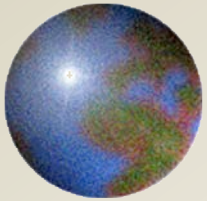
Comparison of Profile





Holistic View of Flows



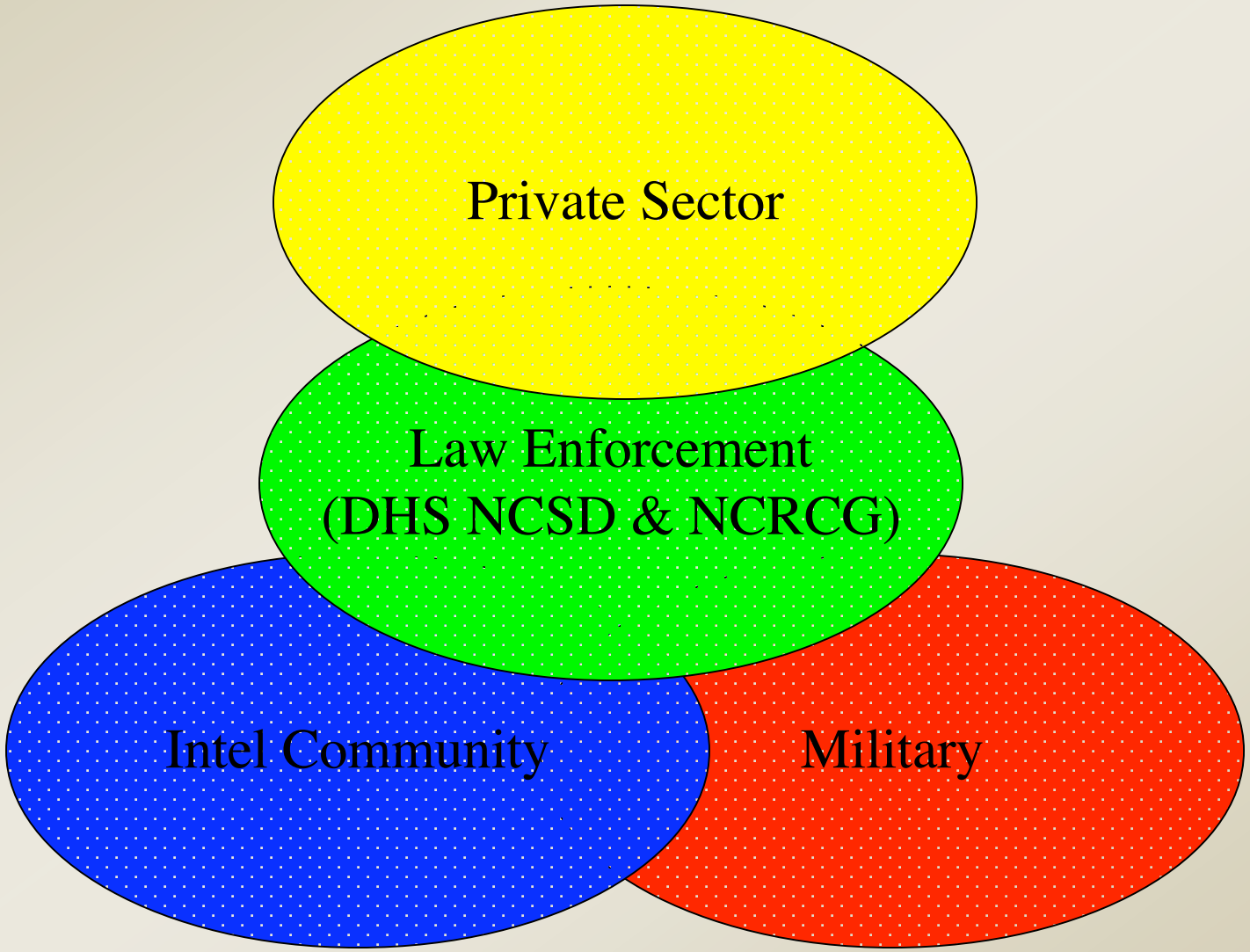


Roadblocks to Mitigation

What you hear (or don't hear)

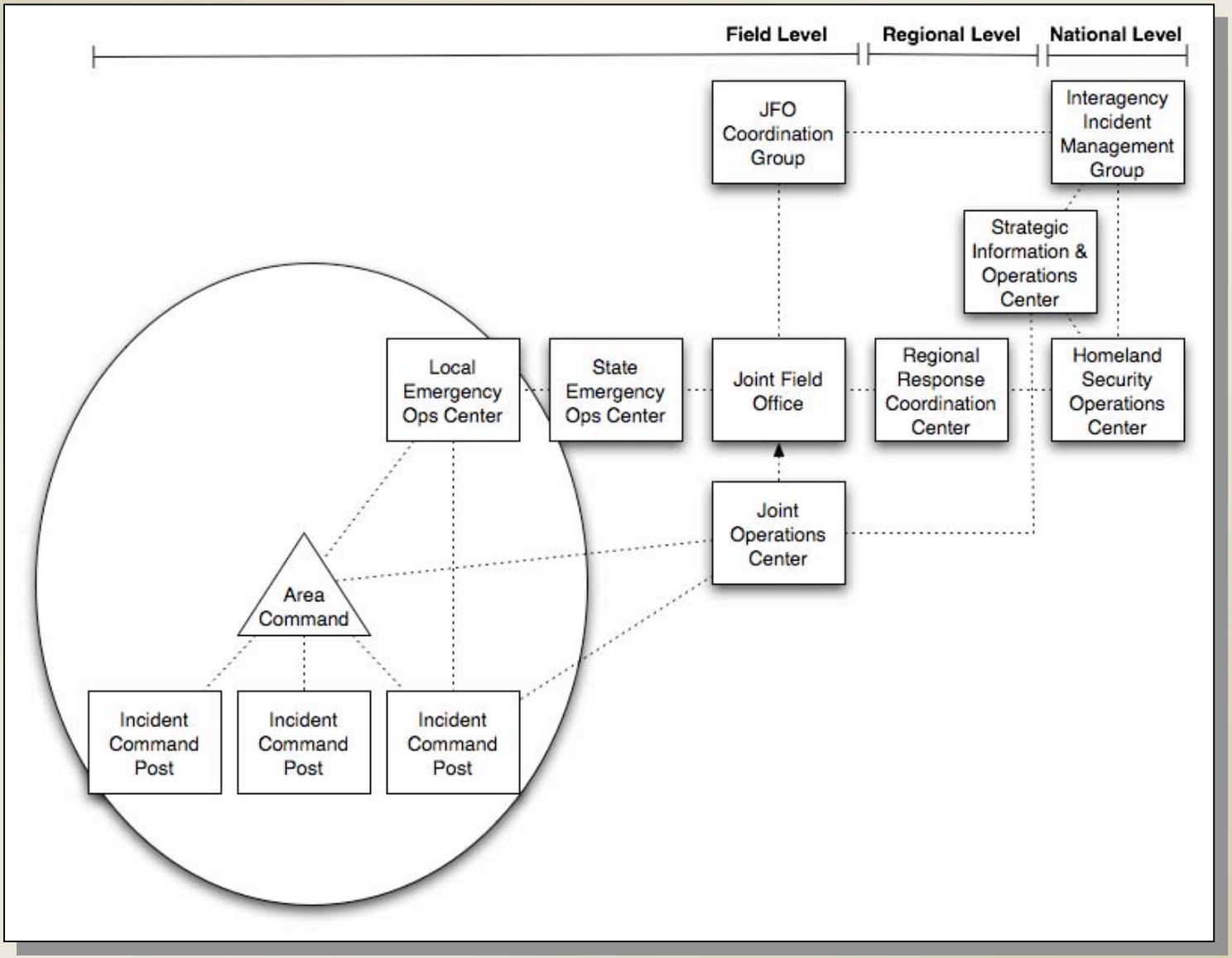
- "Its not my problem."
- "Doing something costs me money."
- "Its only IRC servers. Who cares?"
- "I have nothing important on my computer, so I could care less."
- "We can't afford to have our customers/ competitors know about this."
- "Law enforcement is going to come in here, grab our servers, and we're out of business."
- "The press will find out about this through FOIA requests and we'll be front page news."
- "We weren't prepared for this. We can't tell what happened."

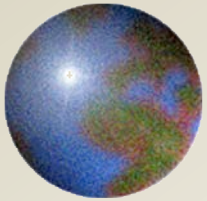
Interfaces (transitions)



http://www.dhs.gov/dhspublic/display?content=4359

NIMS & the National Response Plan





Three Case Studies

COMPUTERWORLD An IDG company

QuickLink Search Compute

Home | News | Browse Topics | Departments | Services | Subscribe | Events | Store

You may retrieve this story by entering QuickLink# 46209

> Return to story

Update: Hackers breach supercomputer centers

University research facilities appear to be targets

News Story by Paul Roberts

APRIL 14, 2004 (IDG NEWS SERVICE) - In recent weeks, malicious hackers have infiltrated computer systems at universities in the U.S. and worldwide, leading to questions about the security of scientific research data, according to an official at the National Science Foundation.

The systems were located at universities and r
including facilities that are part of a project funde
Shared CyberInfrastructure at the NSF, an inde

Supercomputing centers at U.S. universities, in
University of Illinois at Urbana-Champaign and t
Technology, are partners in the TeraGrid projec

Systems at TeraGrid partner facilities were hac
said.

The NSF doesn't know who was behind the atta
that affected high-end systems worldwide, inclu
university research centers, Kim said.

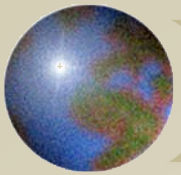
Cisco hacker arrested

Date: **May 11, 2005**
Source: Computer Crime Research Center
By: CCRC STAFF

A global investigation into the theft of a key piece of software that forms the "backbone" of the worldwide web has led to an arrest of a suspected hacker in Sweden.

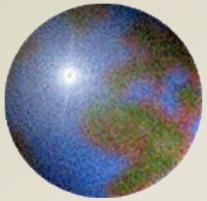
The news followed claims that an internet break-in at Cisco Systems in California last year, which led to a hacker accessing part of Cisco's key IOS source code, was just one part of an extensive operation in which thousands of systems were penetrated.

It is believed that the case has involved attacks on computer systems involving military, NASA and university research laboratories.



UW Medical Center "Kane" Incident

- Goal: "*How hard is it to obtain patient records?*"
- Windows 98 desktop: email w/trojan or open file share?
- Sniffer
  - Linux server -> Windows NT PDC/F&P server
  - Unix email server
- Windows PDCs, BDCs
- Windows Terminal Server (>400 users)
- Access database file (>4000 patient records: *Name, SSN, home telephone number, treatment, date, …*)
- SecurityFocus -> ABC News



What to do?

Collaborative/Distributed Incident Management

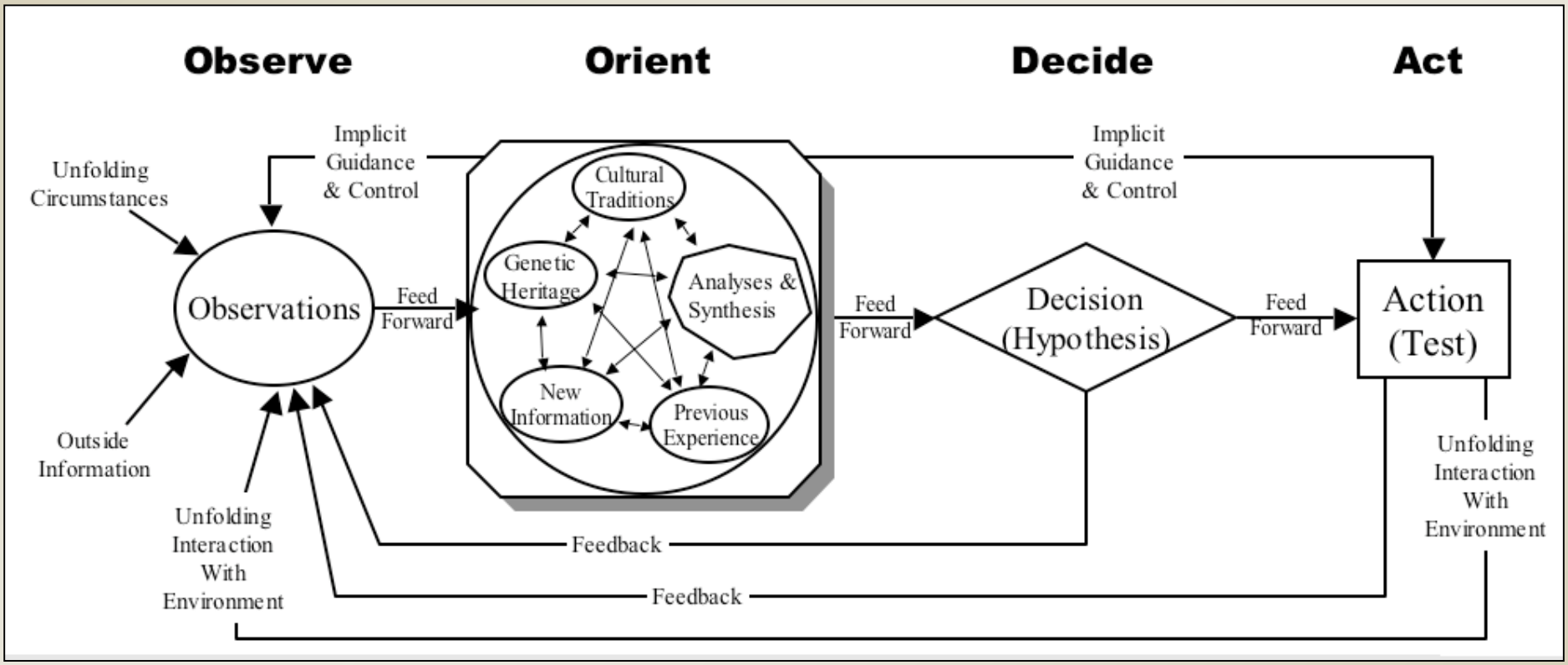
- Optimization of response
- Incident data completeness, accuracy & trustworthiness
- Forensic data preservation
- Communication of incident data
- Incident data correlation
- Incident cost estimation

Levels of "Force"

Figure 2 – Levels of Force

Level	Causal Impacts	Characteristic Actions
Benign	Limited to victim's own systems	Sniffing, scanning, readdressing hosts, honeypots
Intermediate	Impacts on remote systems but not calculated to produce damage	Invasive tracebacks, remote evidence collection
Aggressive	Impacts calculated to produce damage in remote systems	Remote exploitation, corruption of data, denial of service

Col. John Boyd's "OODA Loop"



Source: "The Swift, Elusive Sword," Center for Defense Information, http://www.cdi.org/

Observe & Orient

Table 1 - Observe Tasks and Attributes

Task	Attributes
See the battlespace	• Fused, integrated, deconflicted view of the desired battlespace • Sum of all possible information sources • System identification of information gaps and subsequent collection of missing information
Maintain mobile battlespace view	• Able to pull updated view anytime, anywhere • Easily deployable and transportable with user
Universal access to battlespace view	• Able to tailor picture for relevant AOR, missions, and tasks • Many able to see the same battlespace picture

Table 2 - Orient Tasks and Attributes

Tasks	Attributes
Tailor view of the battlespace	• In-time view of the battlespace • Able to define dimensions and locations of battlespace
Comprehend the battlespace view	• Eliminate biased inputs from one person to another • Eliminate need for mental picture based on another's biases • Able to query for further information; receive in-time answers

Decide & Act

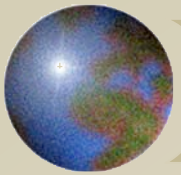
Table 3 - Decide Tasks and Attributes

Task	Attributes
Decide what is important and what may require action	• Decision support tool in transmitter and receiver to filter, sort, and prioritize • Prompts user of significant events for monitoring and action
Determine action required to rectify undesirable situation	• Model effectiveness of potential actions and inactions with in-time feedback • Optimize application of precision force • Ensure least risk to friendly forces

Table 4 - Act Tasks and Attributes

Tasks	Attributes
Immediate access to assets to rectify undesirable situation	• Ready lethal capabilities for employment • Ready nonlethal capabilities for employment • One shot, one kill capability
Feedback on actions and inactions taken	• See in-time mission results • System recommends additional action or inaction

Source: AF2025 v3c2, http://csat.au.af.mil/2025/volume3/vol3ch02.pdf



Conclusions

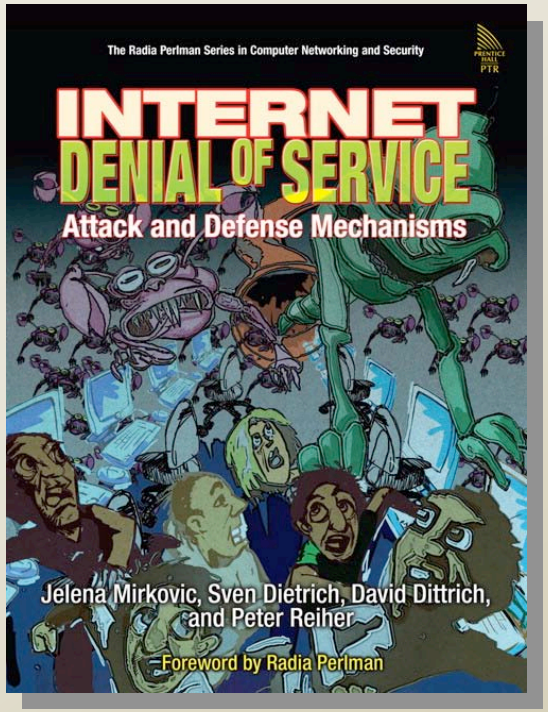
- We need a better view of the “battle space”
- “Trust, but verify”
- We need to think chess, not checkers
- Automation and decision support will provide leverage for defenders
- A lot of people need to do a lot of learning (including me and you!)

Thanks and questions

- *Dave Dittrich*

  IA Researcher
  Center for Information Assurance and Cybersecurity/
  The Information School
  University of Washington

  dittrich(at)u.washington.edu
  staff.washington.edu/dittrich/



http://vig.prenhall.com/catalog/academic/product/0,1144,0131475738,00.html