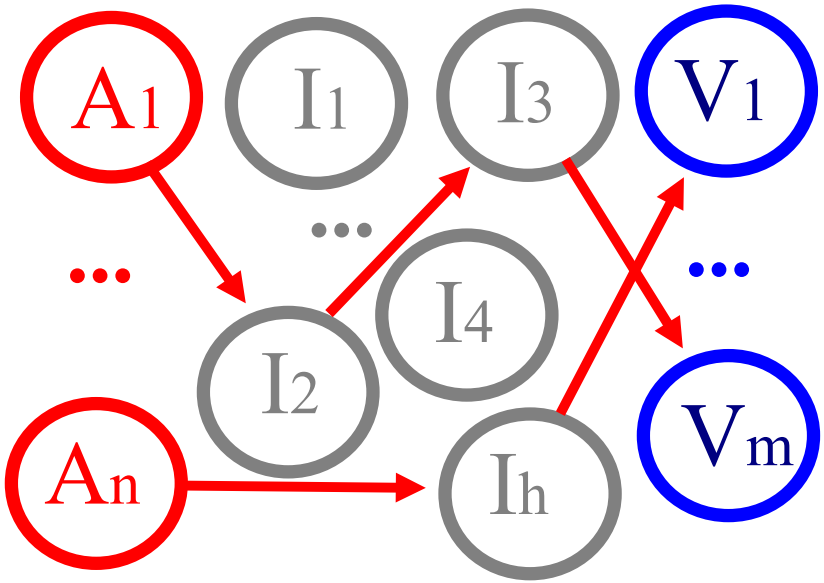
Introduction to Distributed Coordinated Attacks



Your Presenter

Fred Cohen

Principal Member of Technical Staff
Sandia National Laboratories
-AND-
Managing Director
Fred Cohen and Associates

Email:fbcohen@sandia.gov- Tel: 510-294-2087
fc@all.net

I'm from the government ...and I'm here to help you ...really!!!

Full time DOE technical staff

Up to 20 days/year of outside management consulting

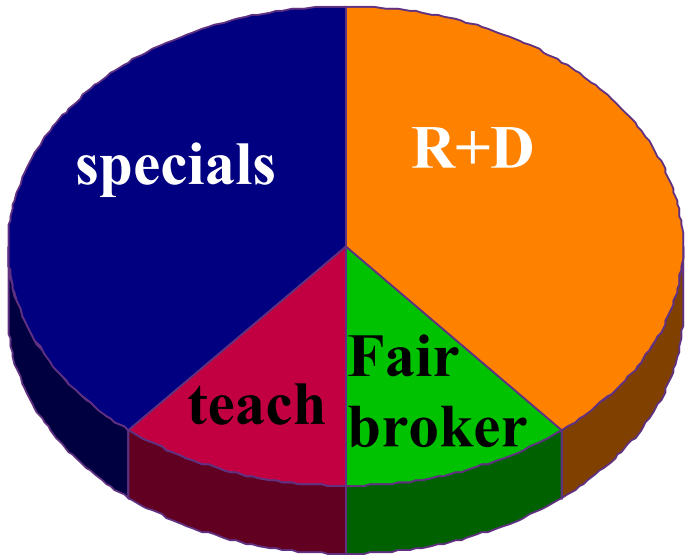
Information Protection:=

Information Assurance:

Getting the right information
to the right place
at the right time

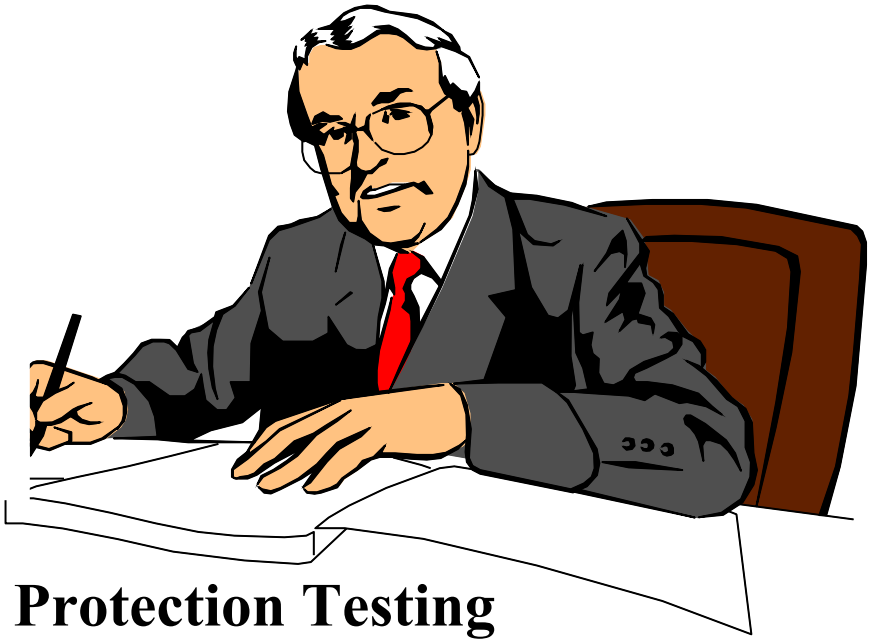
Information Security:

Keeping the wrong information
from getting to the wrong place
at the wrong time



My Approach

1) Look at the big picture
2) Consider many views
3) Provide viable options
4) Facilitate decision making

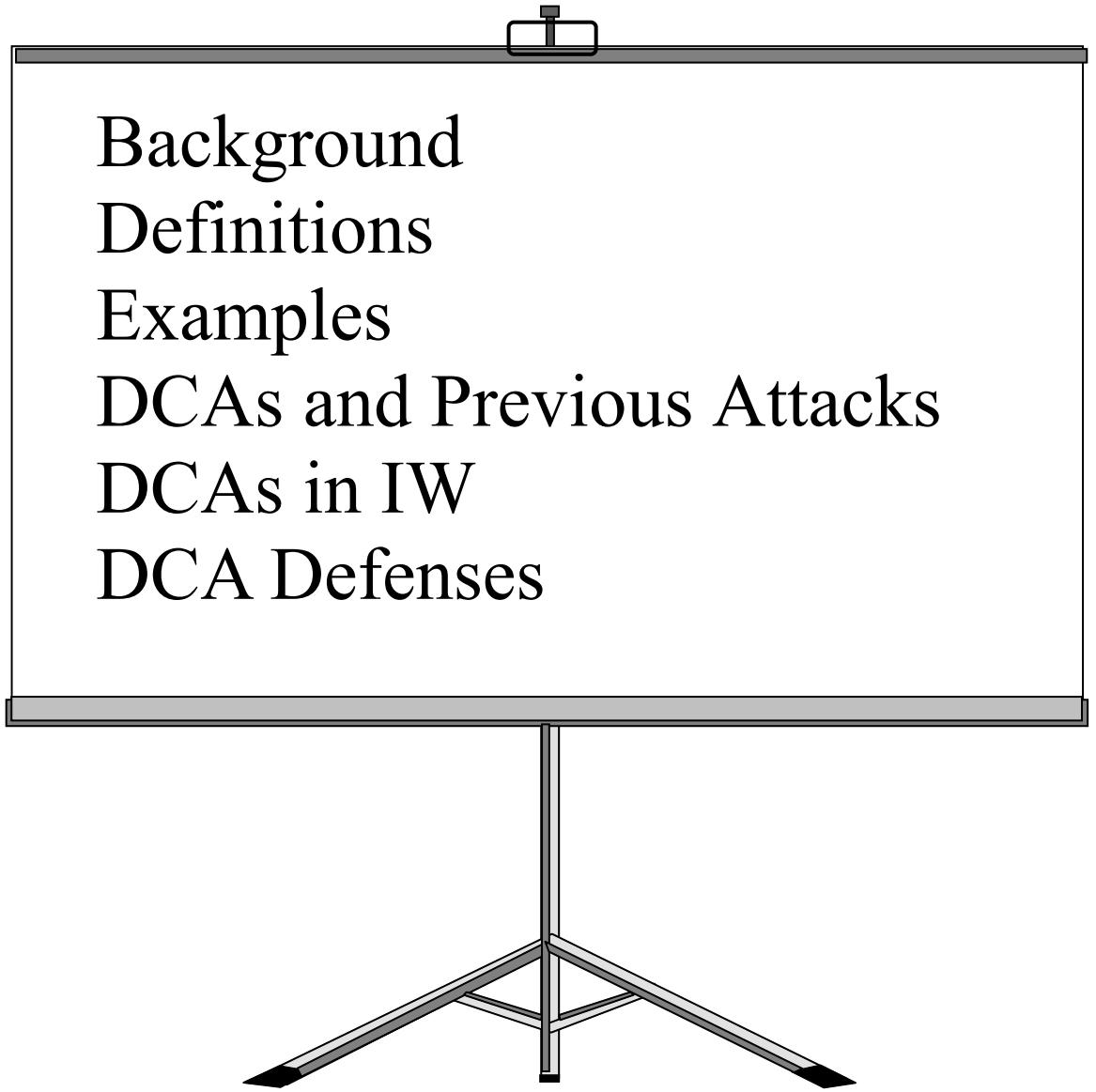


Protection Management
Protection Policy
Standards and Procedures
Technical Safeguards
Protection Audit
Documentation
Incident Response

Protection Testing
Physical Protection
Personnel Issues
Legal Considerations
Protection Awareness
Training and Education
Organizational Suitability

See the big picture when others are caught up in the details
Translate clearly between managers and technical experts

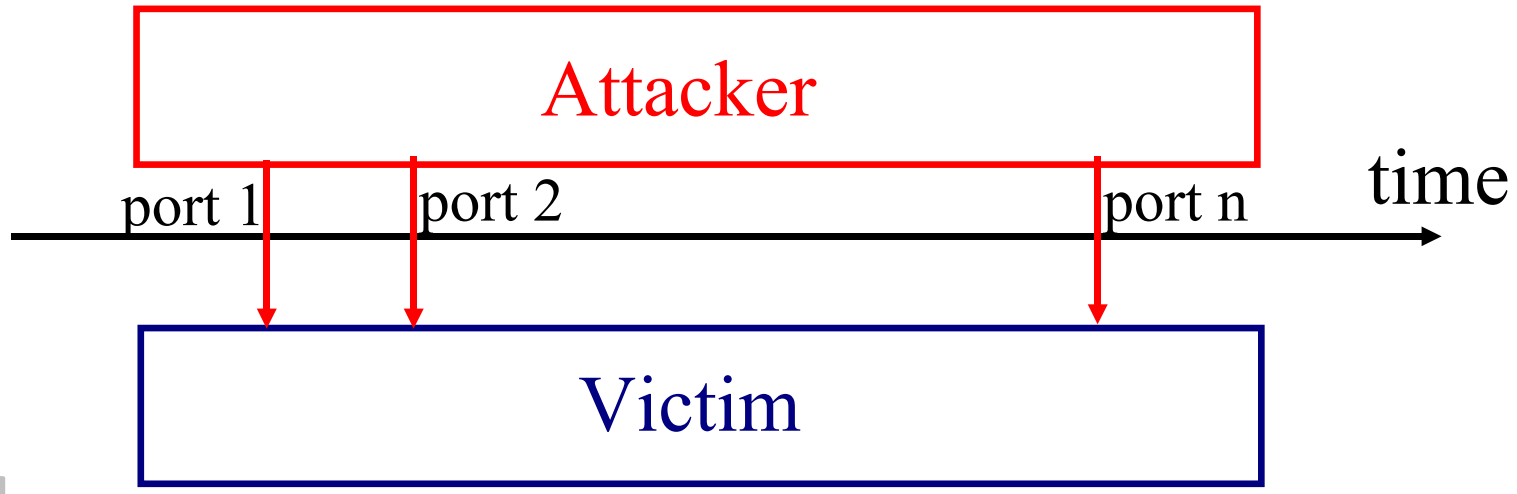
Overview



Background
Definitions
Examples
DCAs and Previous Attacks
DCAs in IW
DCA Defenses

Background

1993: Fred Giessler - "Reflexive Control"
1993: DISA experiments on net noise creep
1994: Internet port scanners
1994: Concerns about distributed scanning and threshold detection schemes

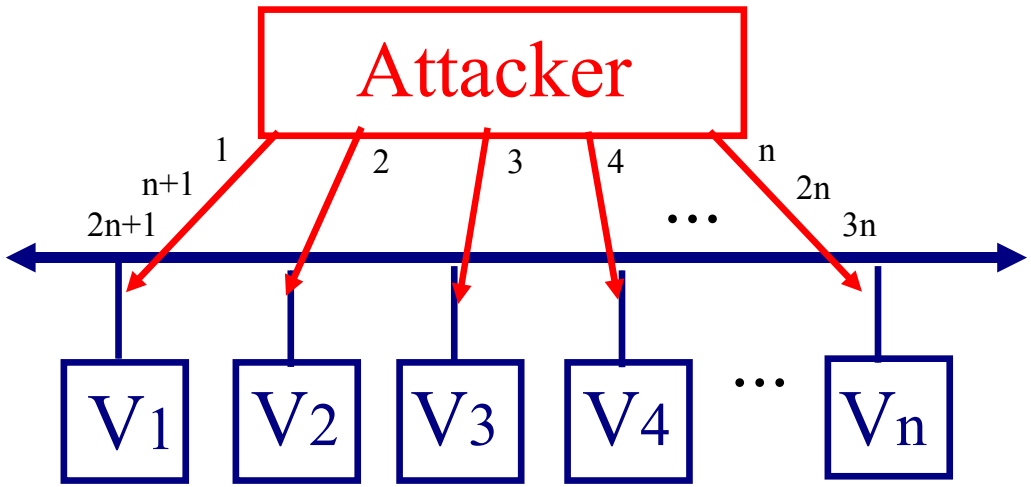


Detected by threshold(source,time)

An degenerative DCA example

Distributed scanning attack

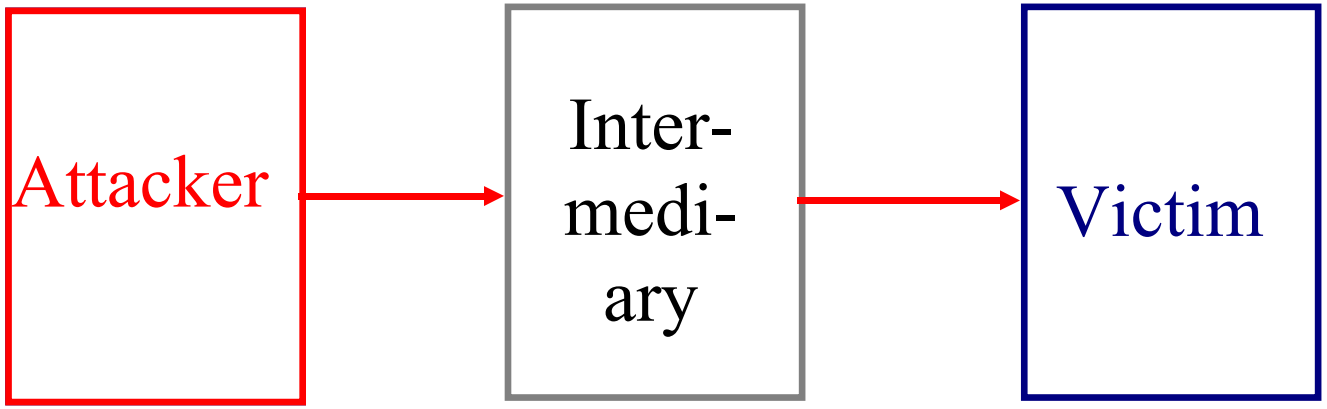
- port scanner spans a class B IP network
- breadth first search instead of depth first
- stays below many detection thresholds
- often more effective than a single system sweep at entering an organization

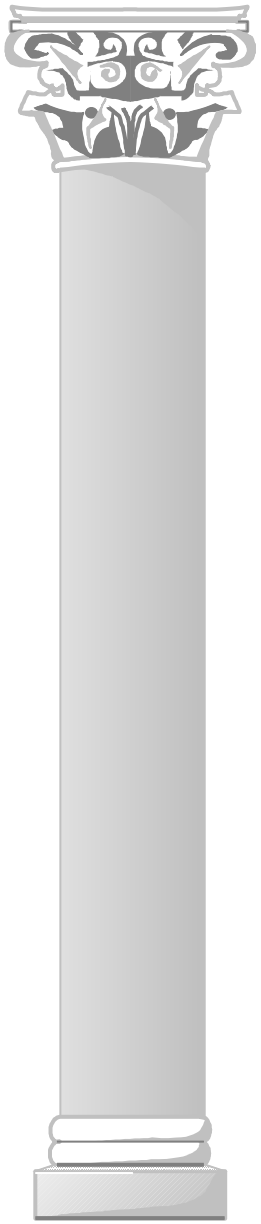


A classic 2-level attack

Break into intermediary site
Attack from there
Known and commonly used for years

- Breaks the link back to the attacker
- Intermediary may have access to victim
- Target rich environment for intermediaries





Distributed Coordinated Attacks

DCA:=(A,V,I,P:(A,I^*,V)) where:

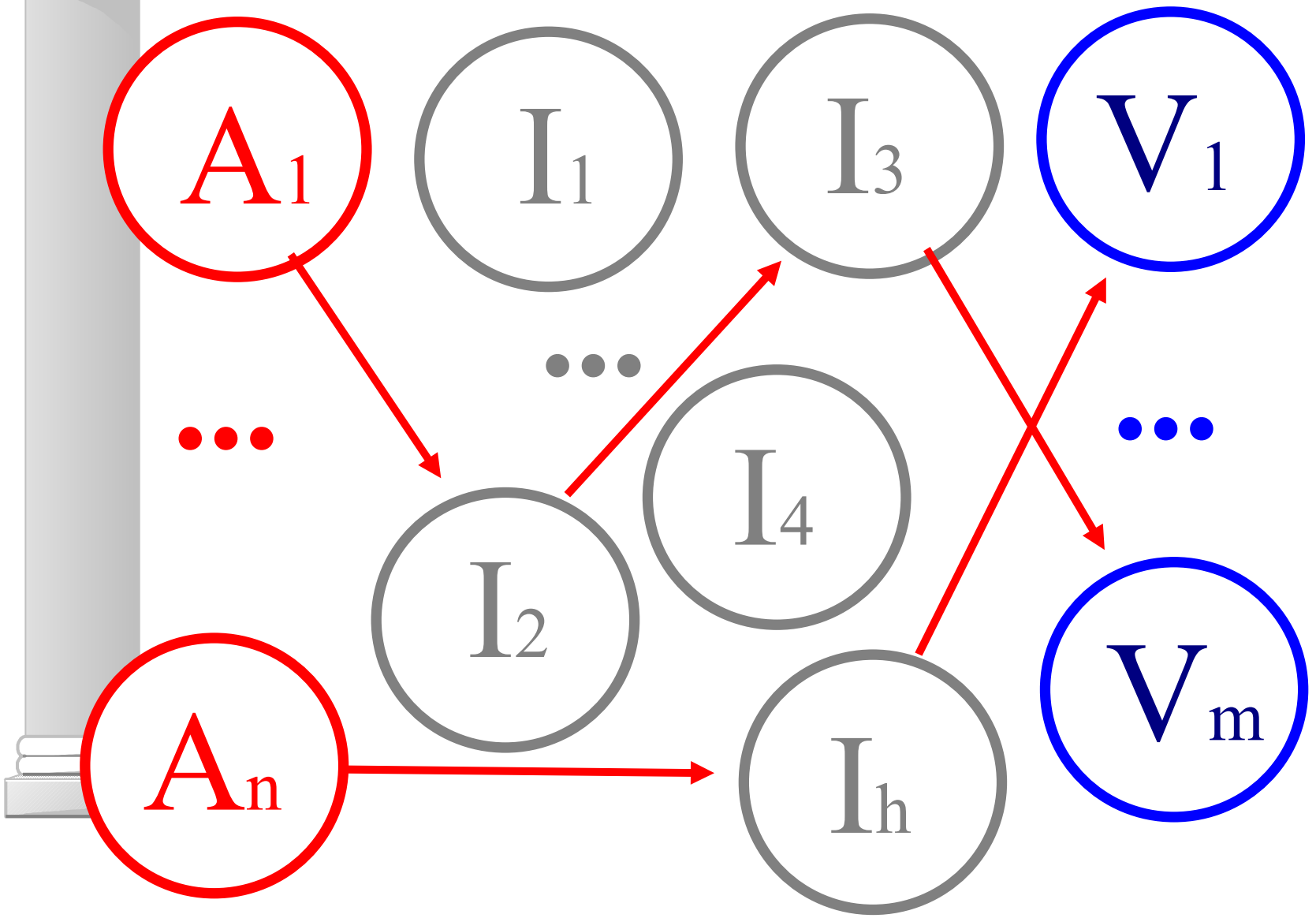
- A:=$\{a_1..a_n\}$ A set of Attackers
- C:=$\{v_1..v_m\}$ A set of Victims
- I:=$\{i_1..i_h\}$ A set of Intermediaries
- P:AxI^*=>V A set of Paths from As to Vs

Informally:

- Distributed:=Multiple indirect paths
- Coordinated:=Against specific victims
- Attack:=Malicious activity

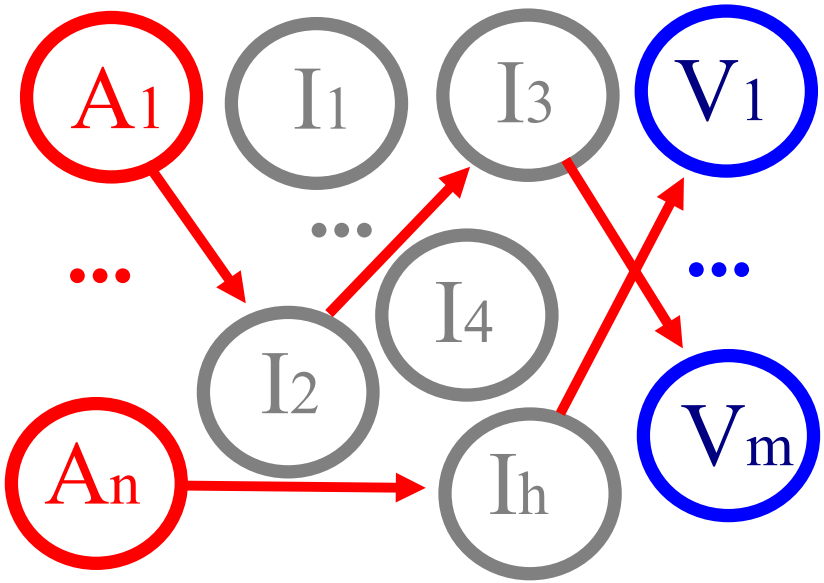
Malicious activity against specific victims using multiple indirect paths.

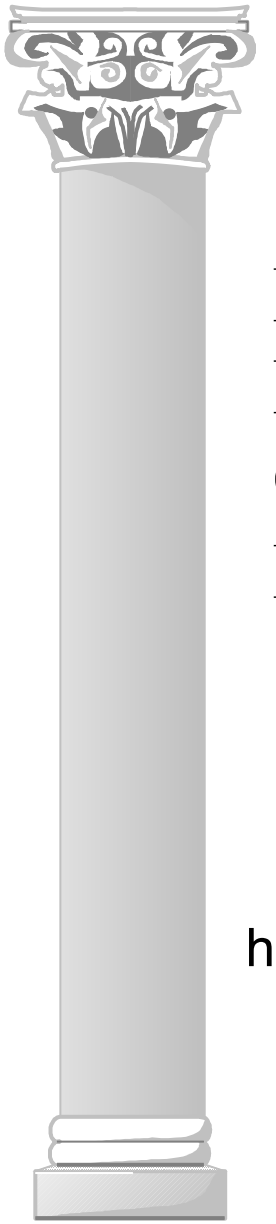
DCAs: a picture definition



A real-world example DCA*

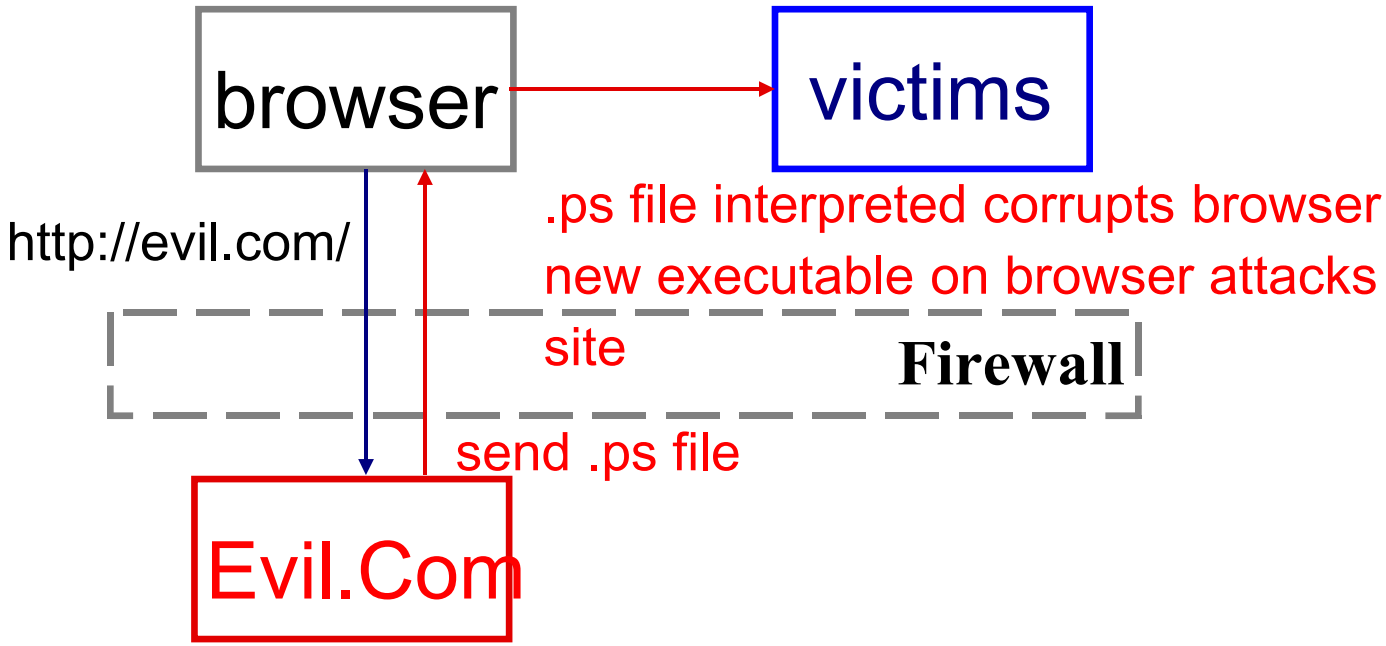
A Web-based firewall bypass
A threat
The attack
The defense
Views of the attack

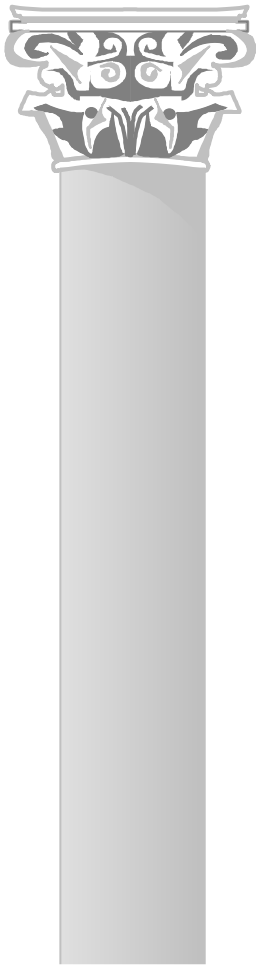




Web-based firewall bypass

Postscript vulnerability in "secure" browsers
Demonstrated in mid-'95 in "self-tests"
Offered to NSA for demonstration in late '95
Demonstrated in all.net tests in '96





A threat

1994-5: SATAN and vulnerability testers
- all.net free remote Internet tests

1995: 50 Ways to attack Web systems
- including the browser as attacker

1995: Test results from all.net
- tests dramatically reduced vulnerabilities

1995: Zero-tollerance approach in effect

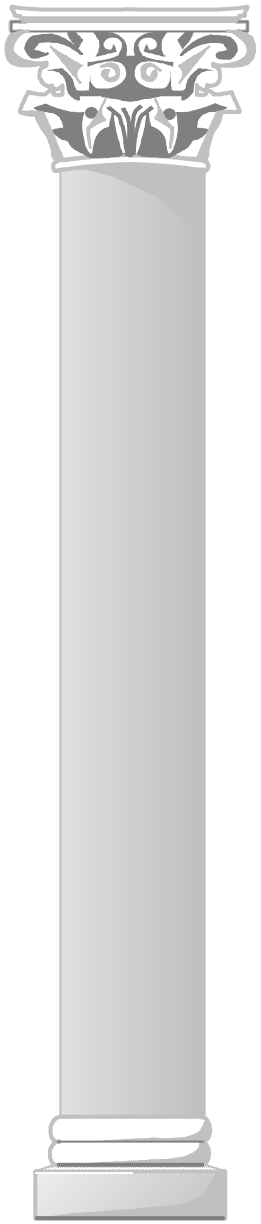
1996: Zero-tollerance approach published

1996: A threat

Subject: Who the Hell are You?

...

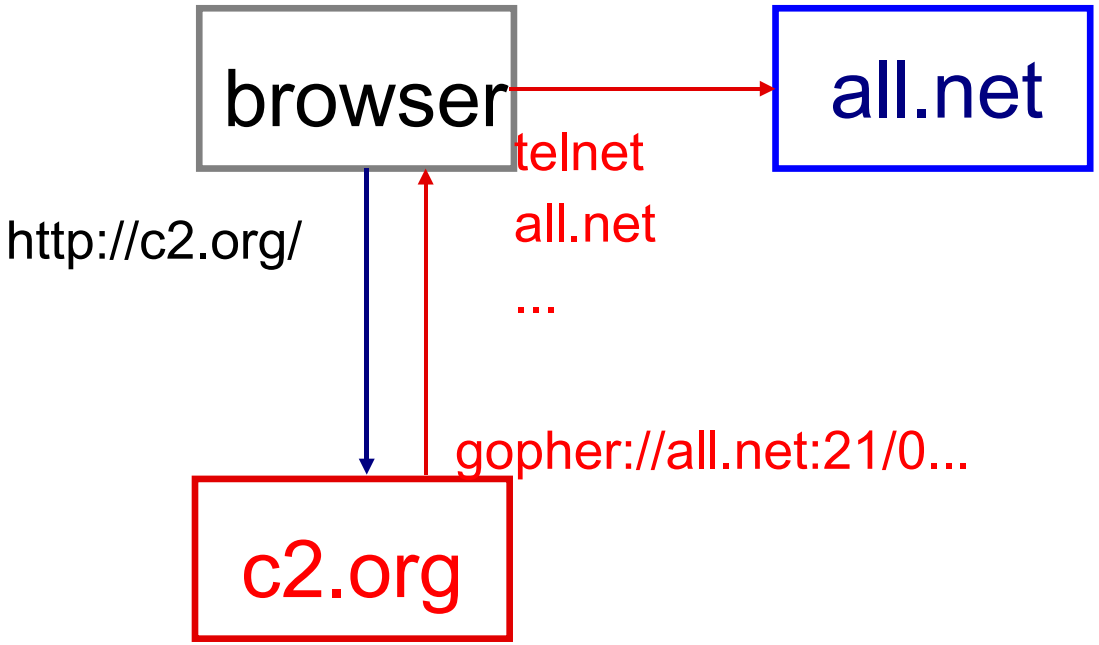
I don't care if you coined "computer virus". I can telnet into whatever I want. Don't be writing me back here again. I WILL get into your system. Feel free to write me back for any other complaints you have to give to me. Bee-ach!!!!!



The attack technique

Telnet attack against an Internet site

- Attacker:=c2.org
- Victim:=All.Net
- Intermediaries:=more than 500 sites in 8h
- Intermediaries are not aware of the activity



The attack begins

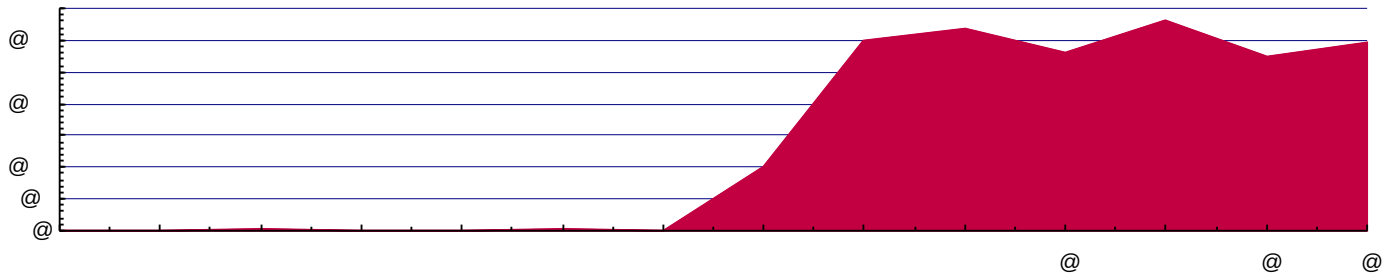
Feb 27-March 10, 20 access attempts

March 11 - 19 attempts

March 12 - 19 attempts

March 13, 00:45 Eastern

- several attempted telnets per minute
- select hosts try scores of times in 1 minute
- 06:30 - 2,000 attempts from 500 sites

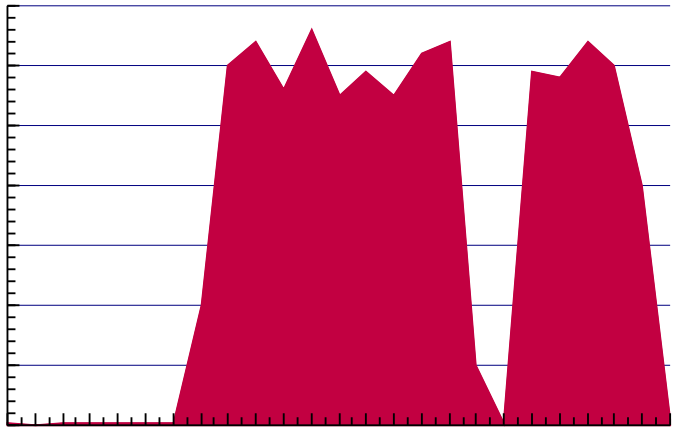


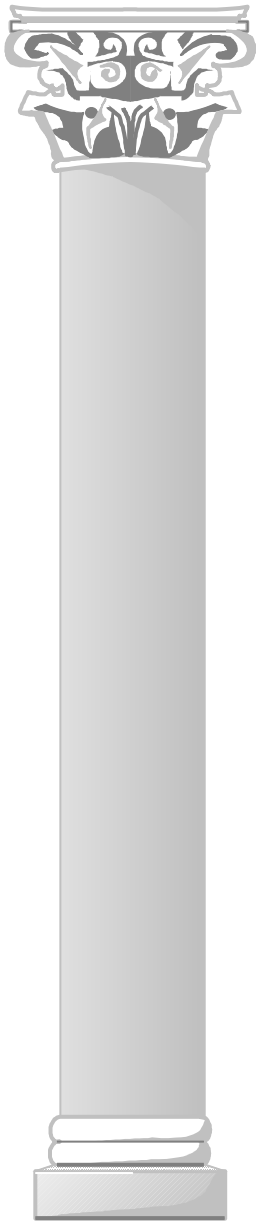
Track the attack

Attack source found in 20 minutes
- by coordinating responses to zero-tolerance
- with cooperation from scores of sites
- more details later

Shutting the attack down - 8 hours
- a silent systems administrator
- he probably initiated the attack
- eventually went to ISP's ISP
- a telephone call really ended it

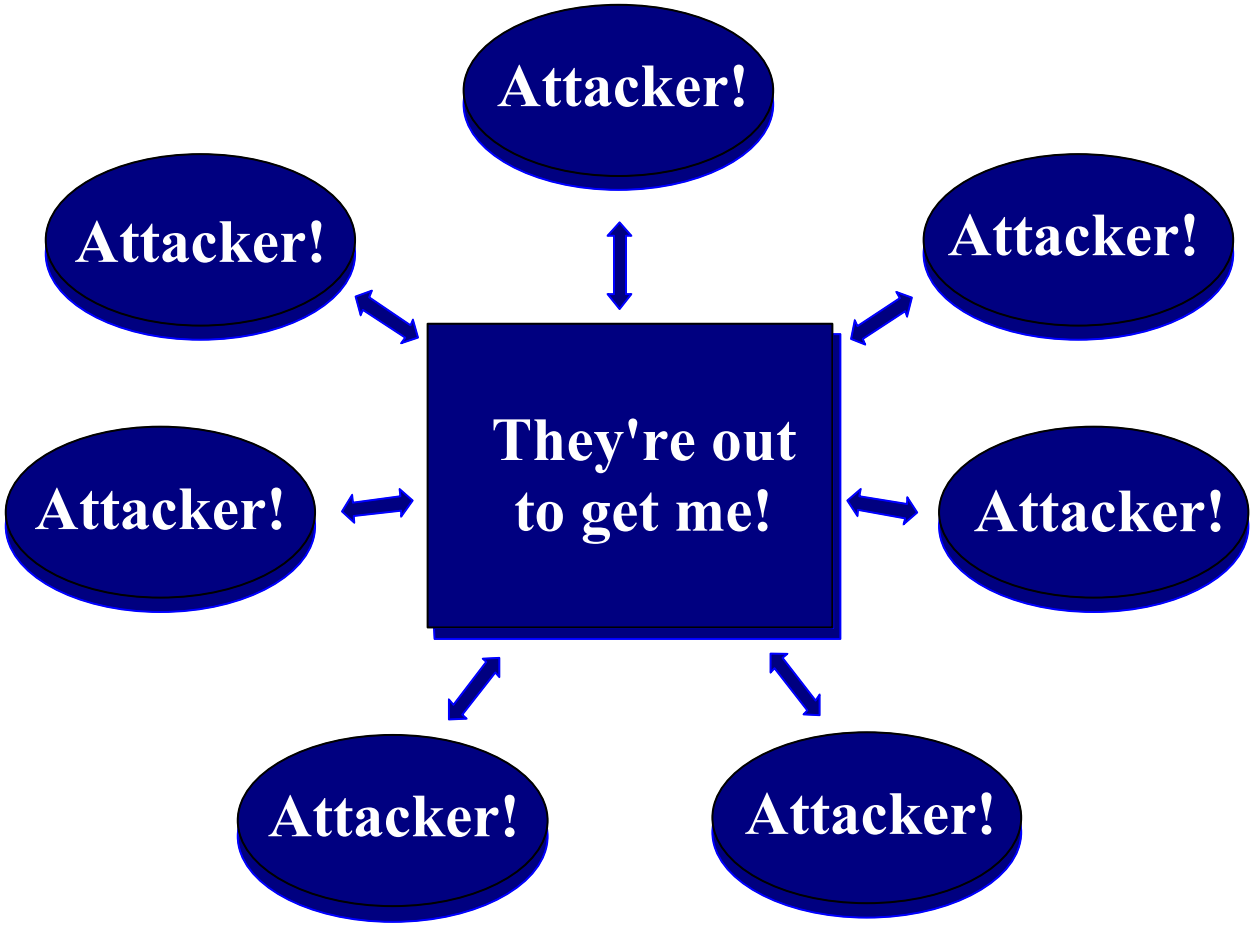
The FBI/States won't pursue

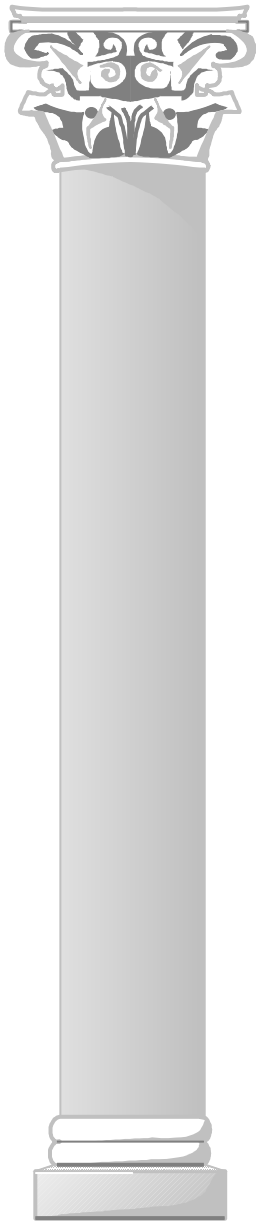




The view from all.net

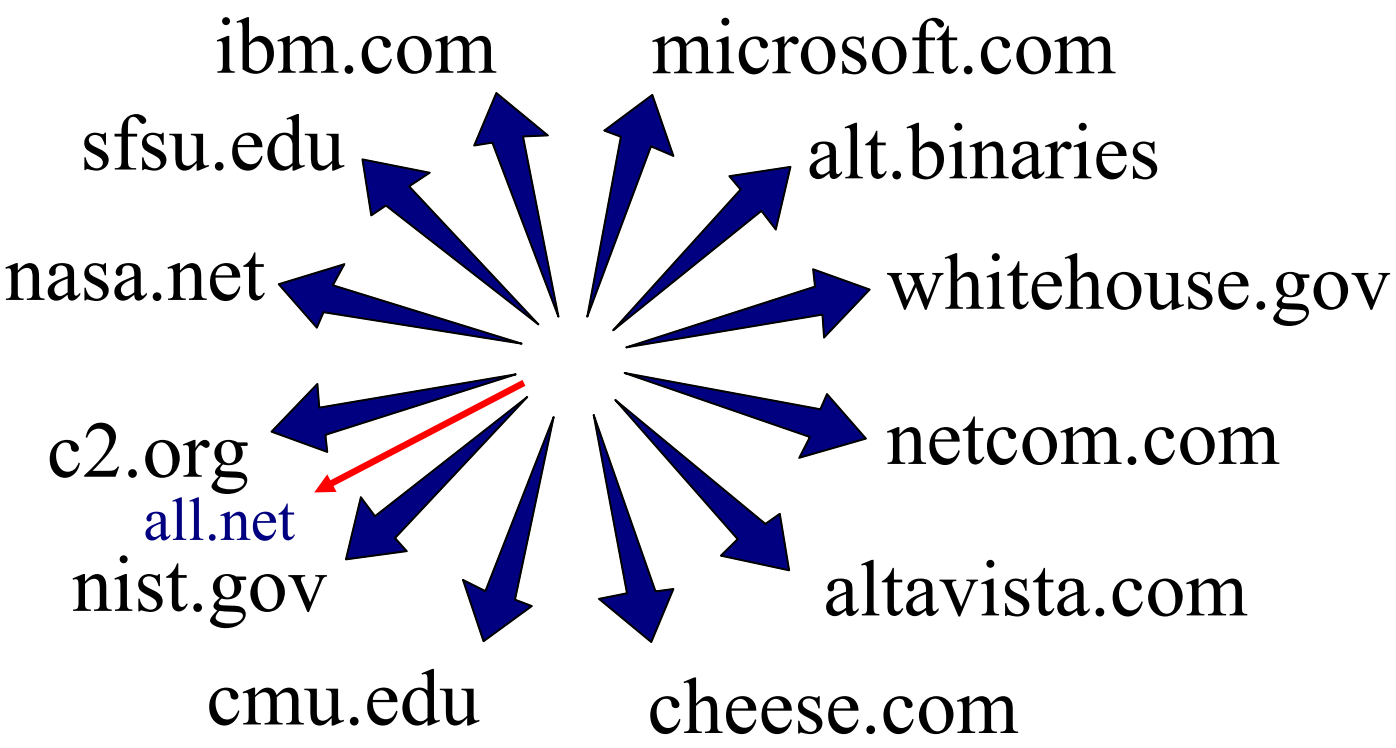
The world's out to get me!





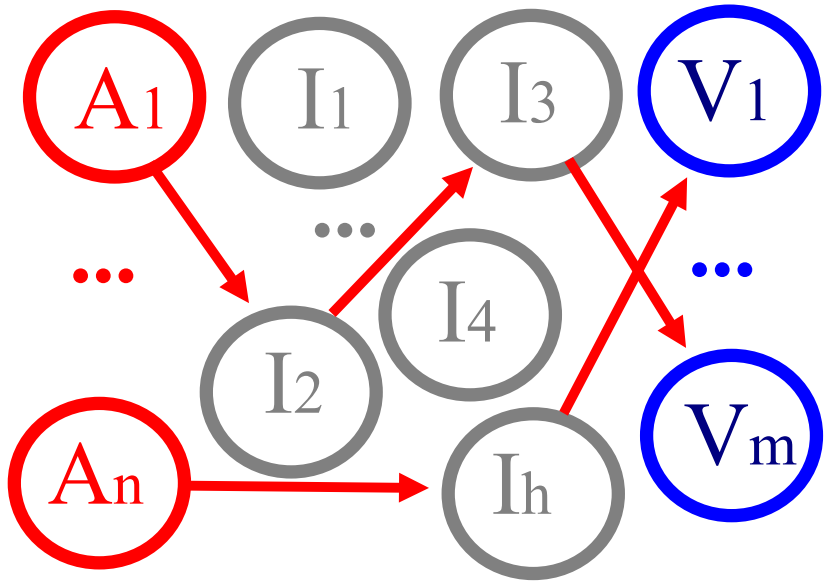
The view from each intermediate

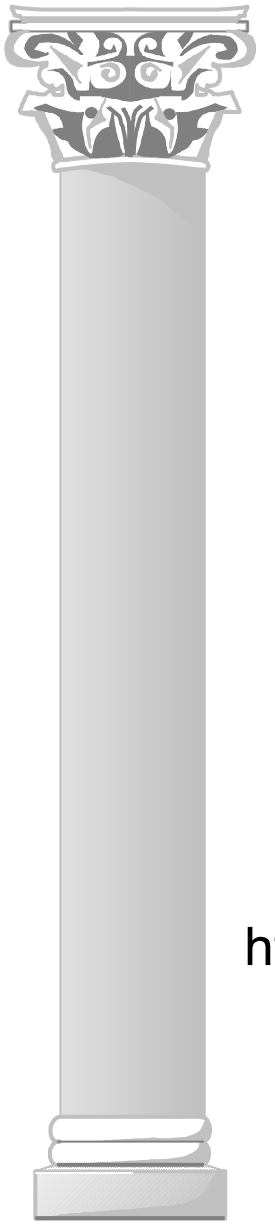
I visited a lot of Web sites
I never even heard of all.net before
Why would all.net say I attacked them?



Some other DCA examples*

Password guessing DCA
DCA through a firewall
A multi-hop DCA
A virus as a DCA

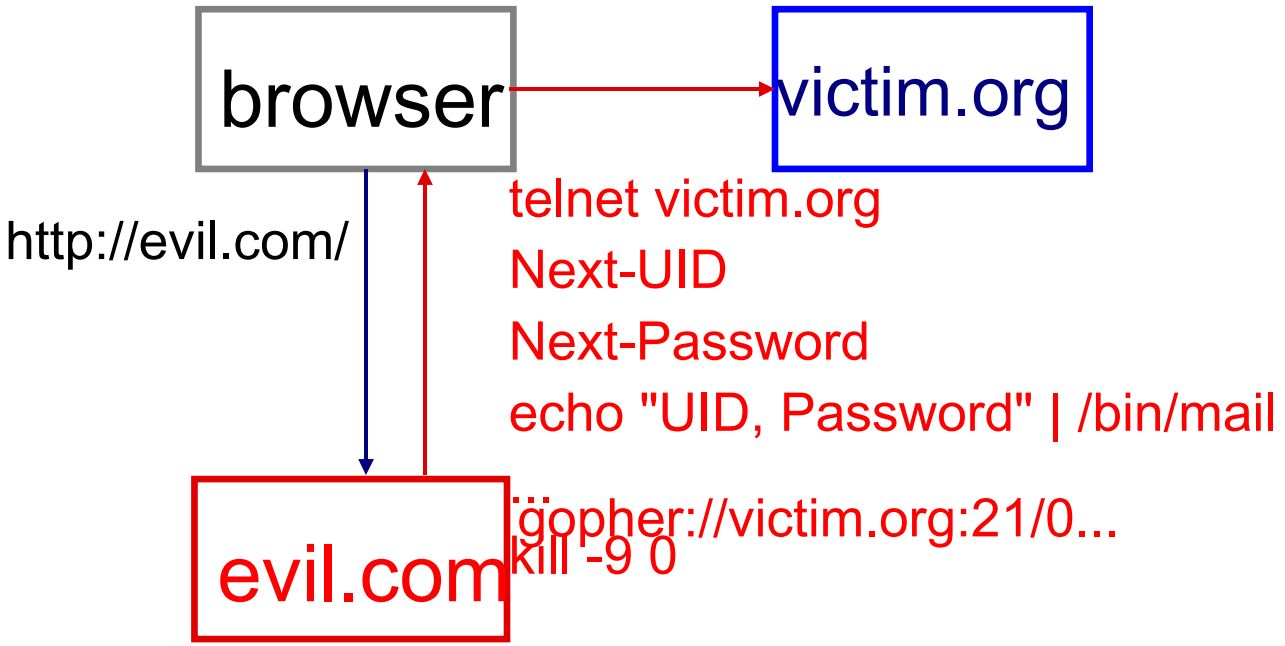




A password guessing DCA

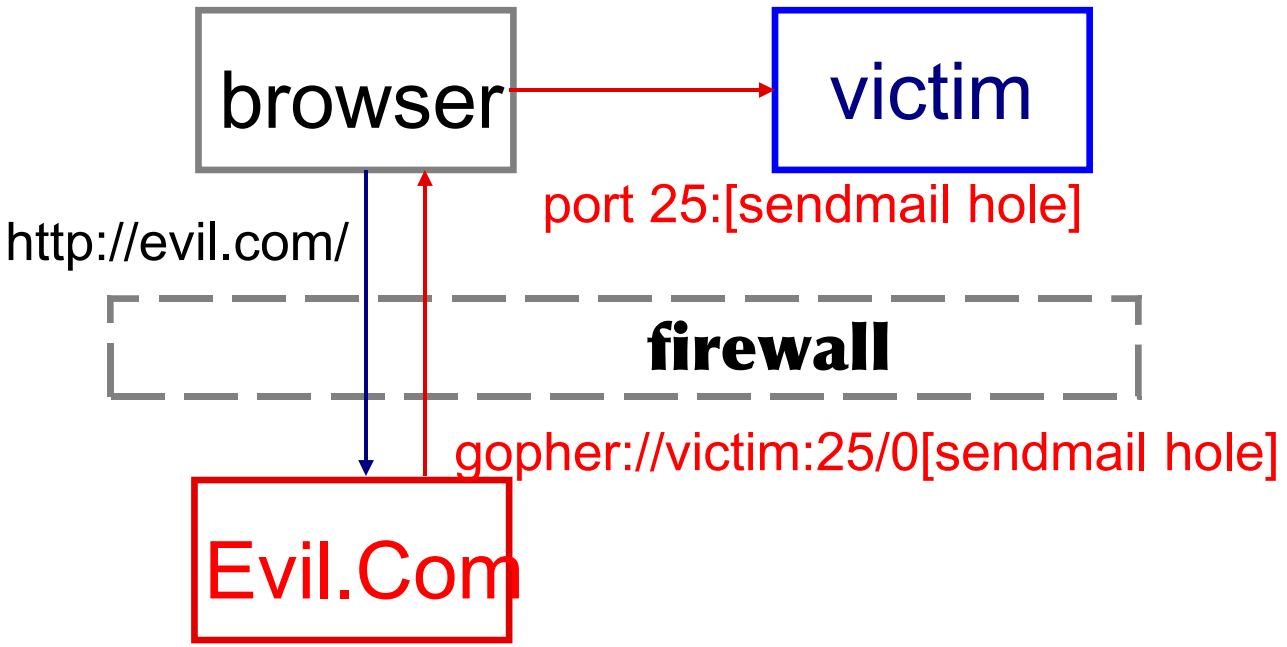
DCA password guessing attack:=

- Display Web Page;
- Get browser to guess next (UID,Password)
  command victim to email (UID,Password) to a usenet newsgroup via an anonymous remailer service



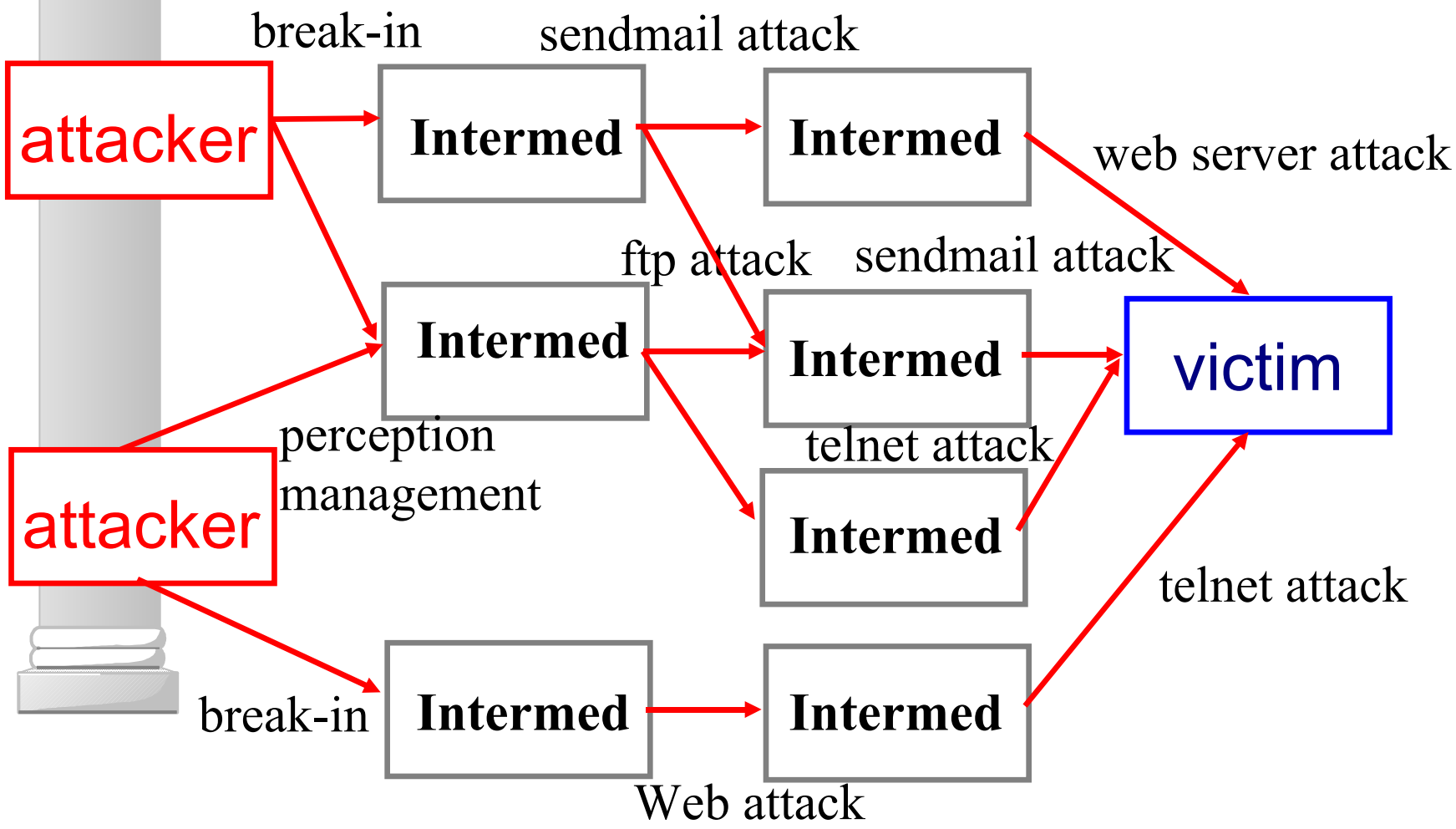
DCA sendmail through firewall

Exploits content of URLs
Only sent to target sites
Attack launched from inside firewall
Bypassed all firewalls in tests



A multi-hop DCA

Multiple attackers, techniques, and paths



A virus as a DCA

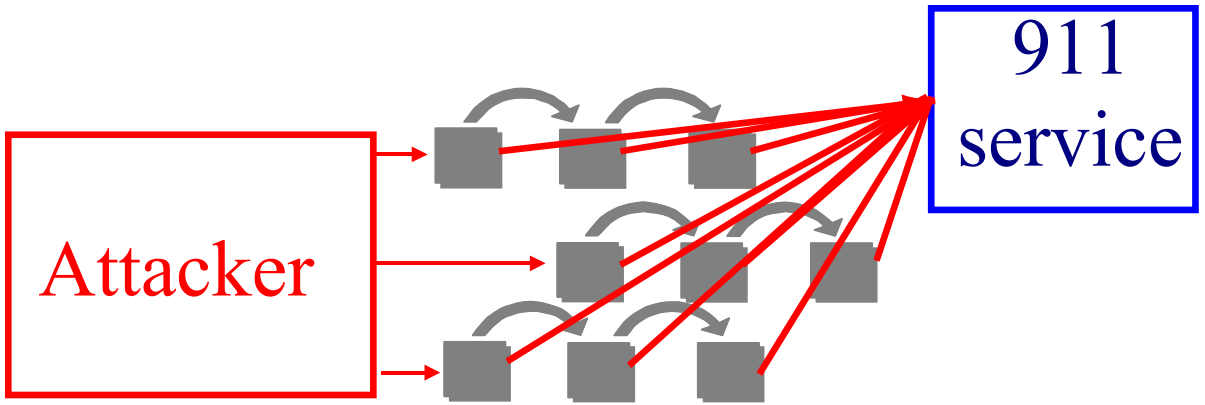
DCA Virus:=

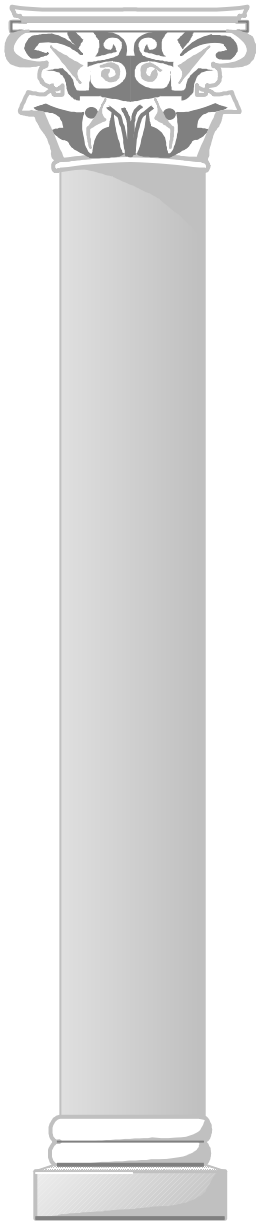
- Reproduce
- If (date > 1999/1/1) dial 911 on modem

Distributed automatically and widely

Coordinated as to time and victim

Disrupts 911 emergency services





Some other variations

One-per-site DCA:=

- if (! intermediary-exploited-this-week)
  then attack victim via intermediary
  otherwise provide normal services

Probabilistic DCA:=

- if (pseudo-random-integer <IP-address)
  then attack victim via intermediary
  otherwise provide normal services

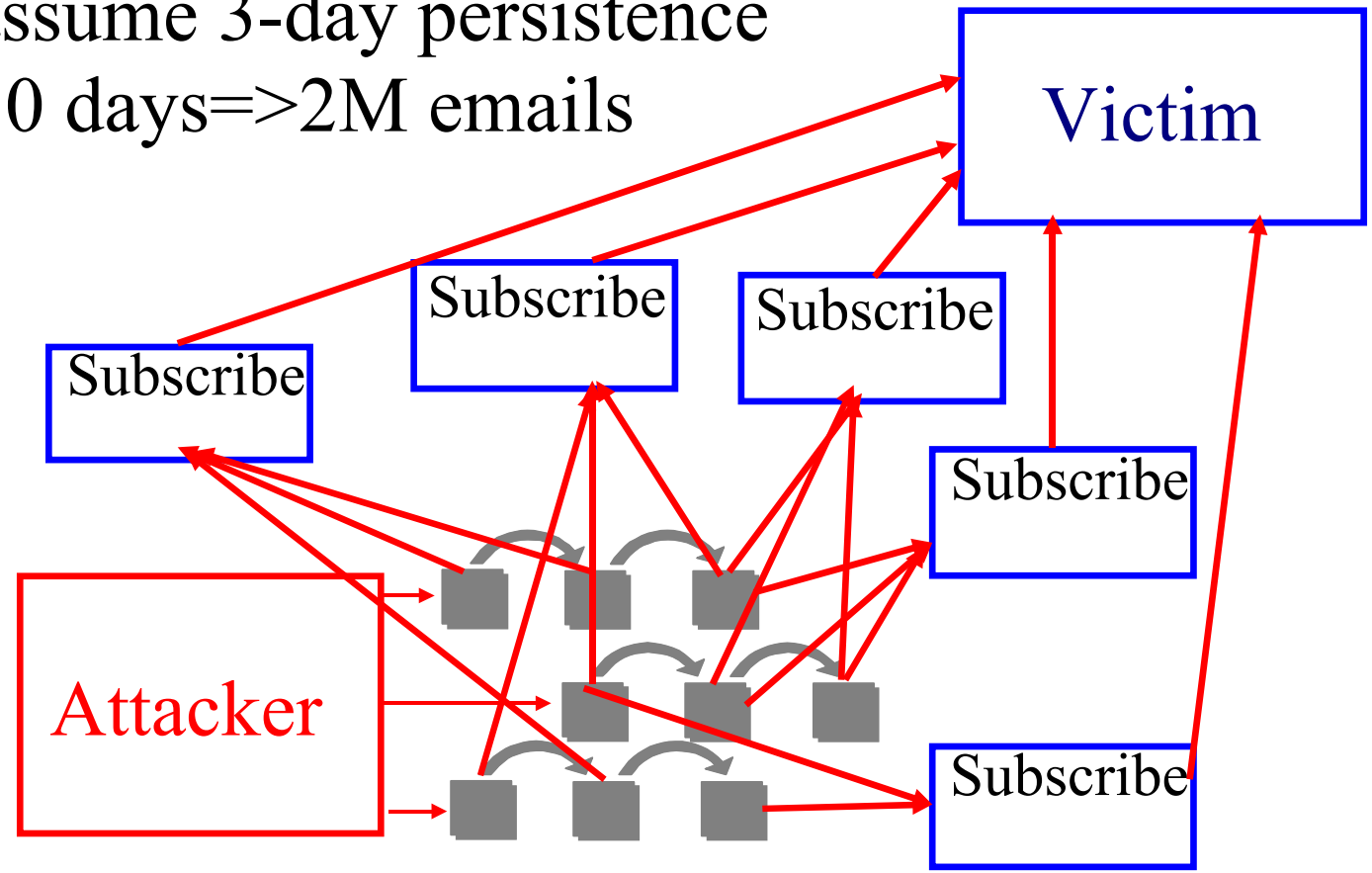
Email SPAM as a DCA:=

- for all X in Internet-mailing-lists
  sign-up victim to mailing list X

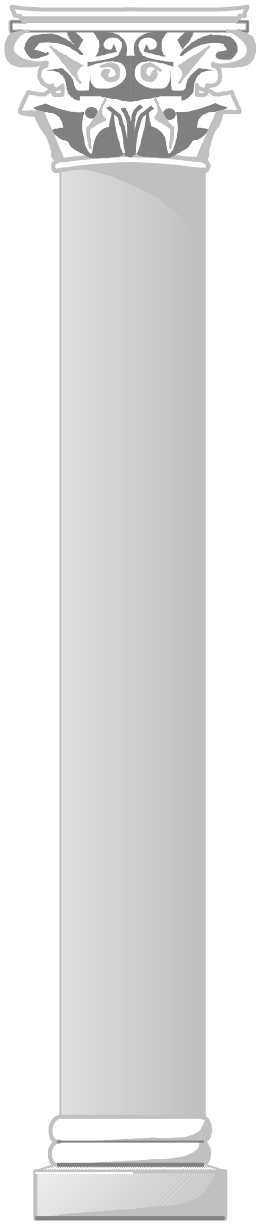
Forged IP address DCA

The superspam DCA

1 attacker
500 intermediaries per day
3 victims, 3 lists/intermediary
10 mailings/list/day
45,000 more emails each day
assume 3-day persistence
30 days=>2M emails



A PM DCA



May 31, 100 ftp attempts/hour

8 AM - Autoresponder to FTP turned on

- based on traffic, expected time to track down the source was computed at about 8 hours.
- about 7 hours later, the first useful response came in, by 12 hours we knew most of it.

8 PM - The ftp's were caused by PM

- an announcement that we were a "Warez" site
- publication in IRC forums and posting to lists

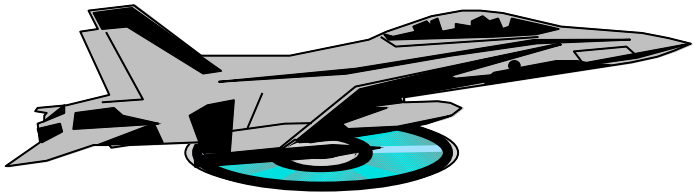
9 PM Counter-PM initiated

- A message to participants:

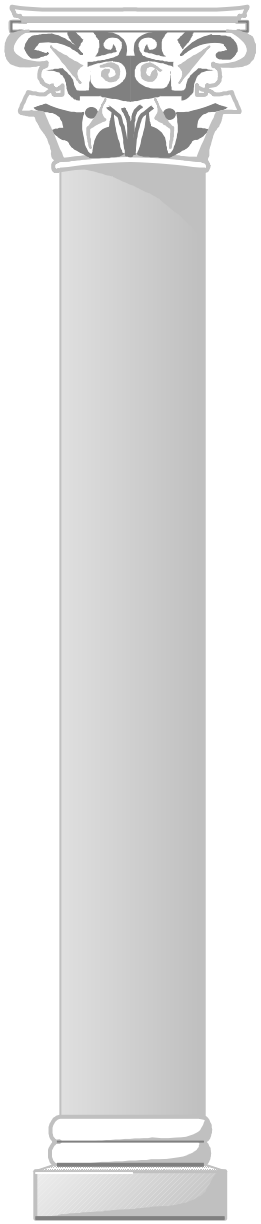
  no Warez here - we logged your entry - we reported to your admin - we CC'd the SPA

9AM June 1 - levels down to 2/hr

DCAs as IW weapons



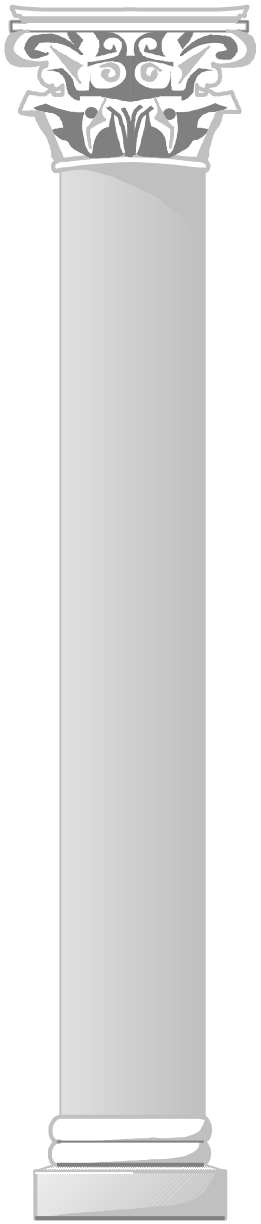
Easily controlled
Pinpoint targetable
Effect often easily measurable
Hard to trace
Easy to demonstrate causation
Plausible deniability (if careful)
Excellent for deceptions
Hard to selectively block
Often achieve deep penetration



DCAs and deception

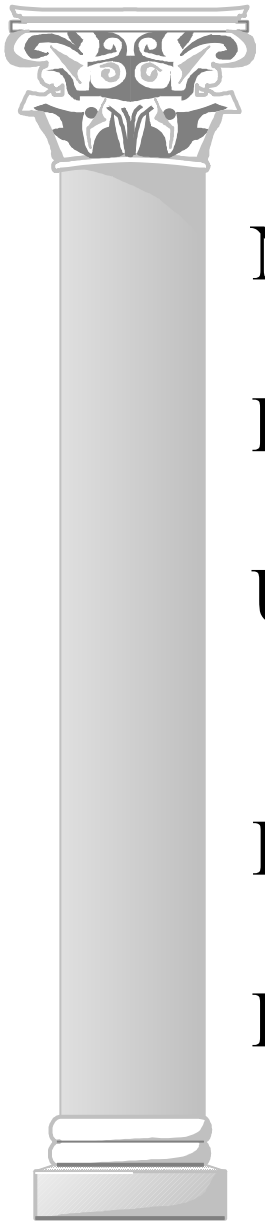
Jim Dunnigan and Albert A. Nofi (95)
Victory and Deceipt - Morrow and Co.

- Concealment
- Camouflage
- False and Planted Information
- Reuses
- Displays
- Demonstrations
- Feints
- Lies
- Insight



DCA damage

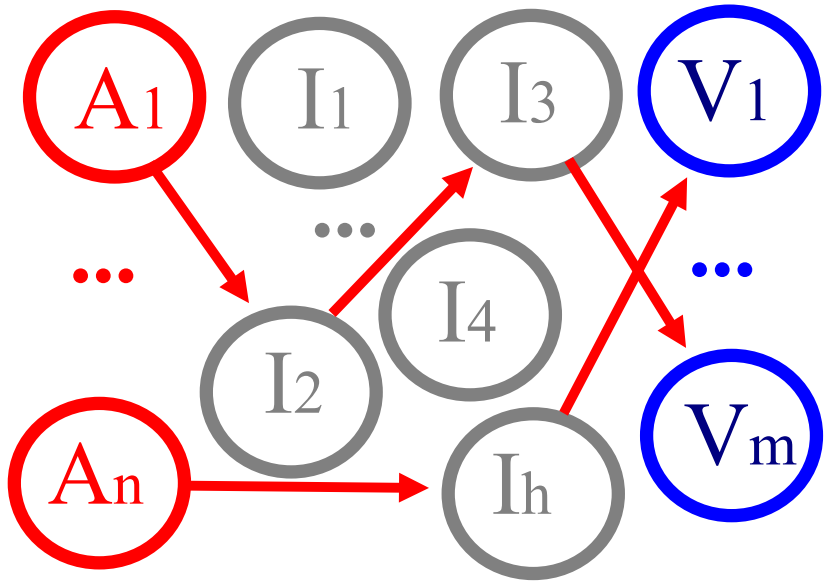
Denial of services often pretty easy
Computational leverage is substantial
Exhaustive search of attack space
Open-loop exploit of arbitrary attacks
Bypasses attacker-specific defenses
Consume limited protective resources
Perception management and deception
Systems and protection fail under stress
- DCAs tend to stress them



Enabling Technologies

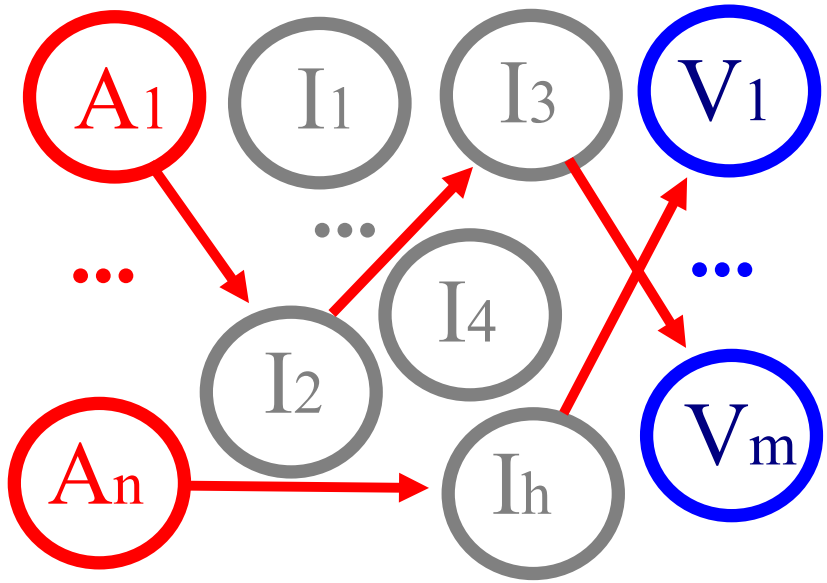
- Networking
  - Ethernets, Intranets, Internet, Cable-LAN, ...
- Remote execution and open access
  - Gopher, Web, Java, Postscript, Word, MIME, ...
- Uncontrolled Internet environment
  - New services on arbitrary ports with inadequate definition or notification create noise
- Insecure ISPs
  - target rich intermediate environment
- DC programs
  - Intelligent agents, Net crawlers, Virus-like DCs

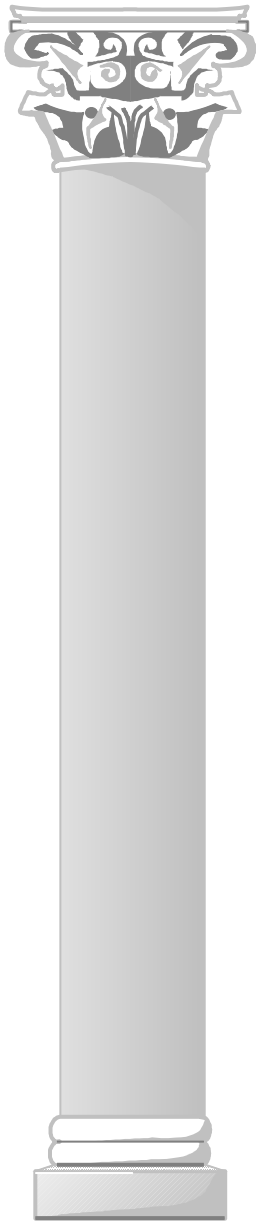
DCAs - Summary to here



DCA Protection*

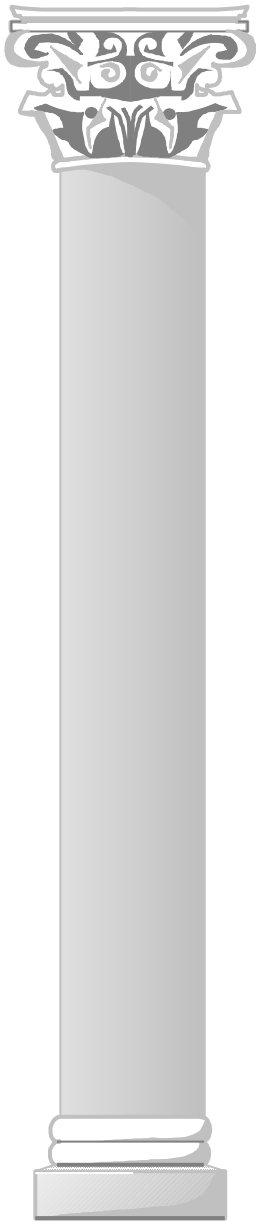
Prevention
Detection
Tracking DCAs down





DCA Prevention

- Disable enabling technologies
  - No Way
- Eliminate vulnerable intermediaries
  - No Way
- Private Inter-Networks
  - Increasingly used in industry
  - Limits sources and protocols
  - Allows additional authentication
  - Allows far easier tracking to source



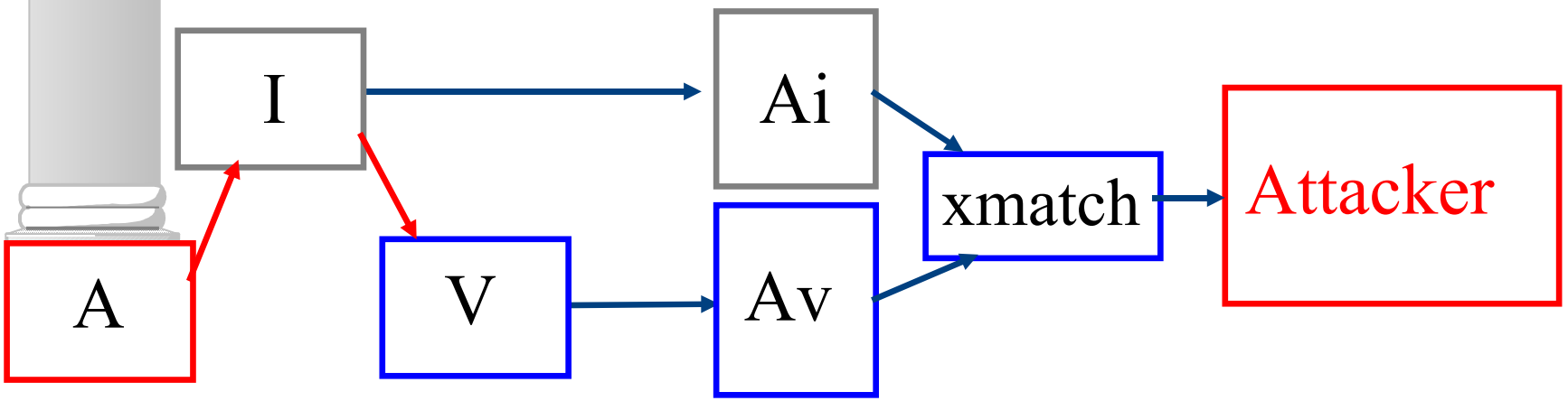
Detection

- Dramatic changes in event rates
  - typical of naive attacks and deceptions
  - reflexive control to increase thresholds
  - coordinated attacks =>coordinated defenses
- Zero-tolerance detection strategy
  - every event is important
  - resource exhaustion
  - automated response is necessary
- Crossmatched audit analysis
  - coordinates analysis of different sources
  - example results at http://all.net/

Tracking down a DCA

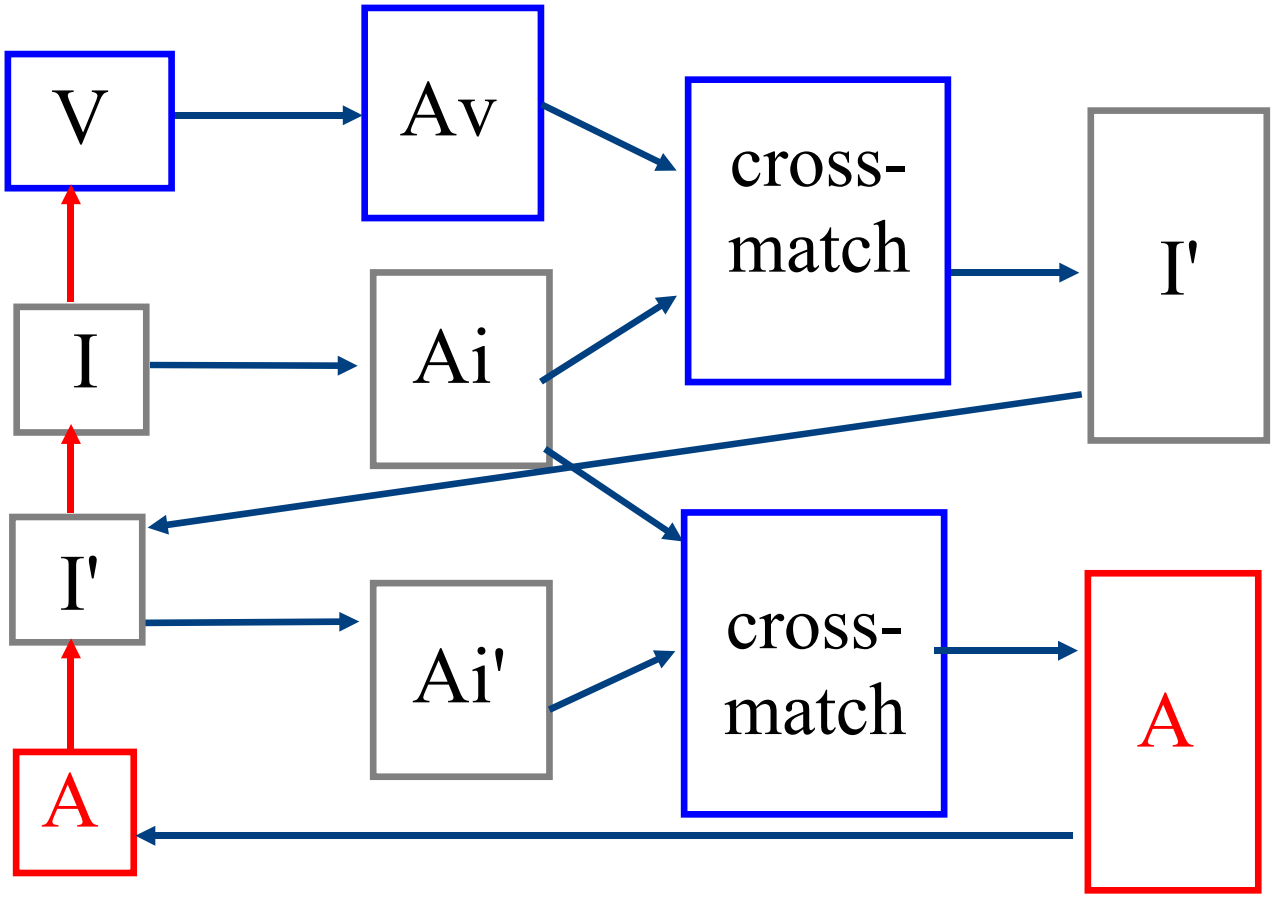
Zero-tolerance approach
Automated real-time response
1 in 125 sites responded usefully
Cross-match audit trails=> attacker
1-intermediary, 4 hours mean-time
2-intermediaries - same scenario

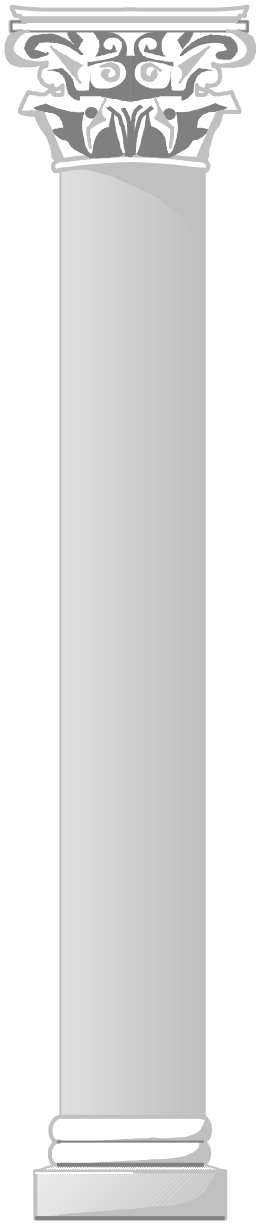
- 1 in 125^2 sites get 2-links = 15,625 sites
- 500 sites/day => 31+ days to track down



Tracking multi-hop DCAs

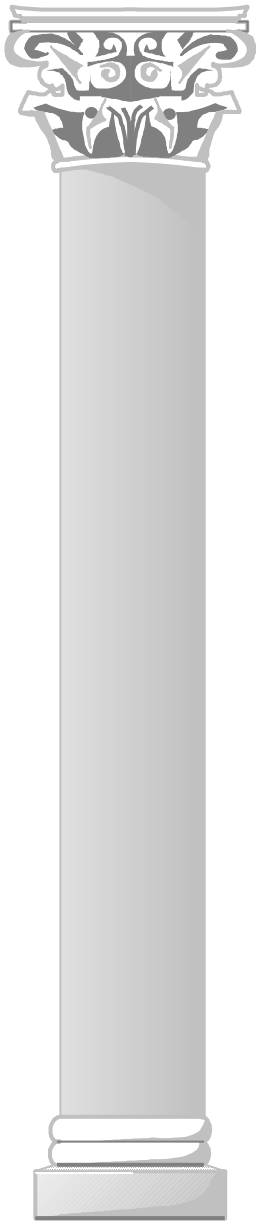
You need a full path back to the source





Some other properties of DCAs

- Indirect link between attacker and target
  - Tracking requires intersite coordination
- High attack rate - low contribution/site
  - Each intermediary may have only 1 instance
  - Intermediaries are often unaware
- Tacking exponential w/hops
  - till Internet space is exhausted
- Most DCAs have been open loop
  - closed loop feasible with Java, etc.
  - closing the loop may lead back to attacker



Theoretical limits

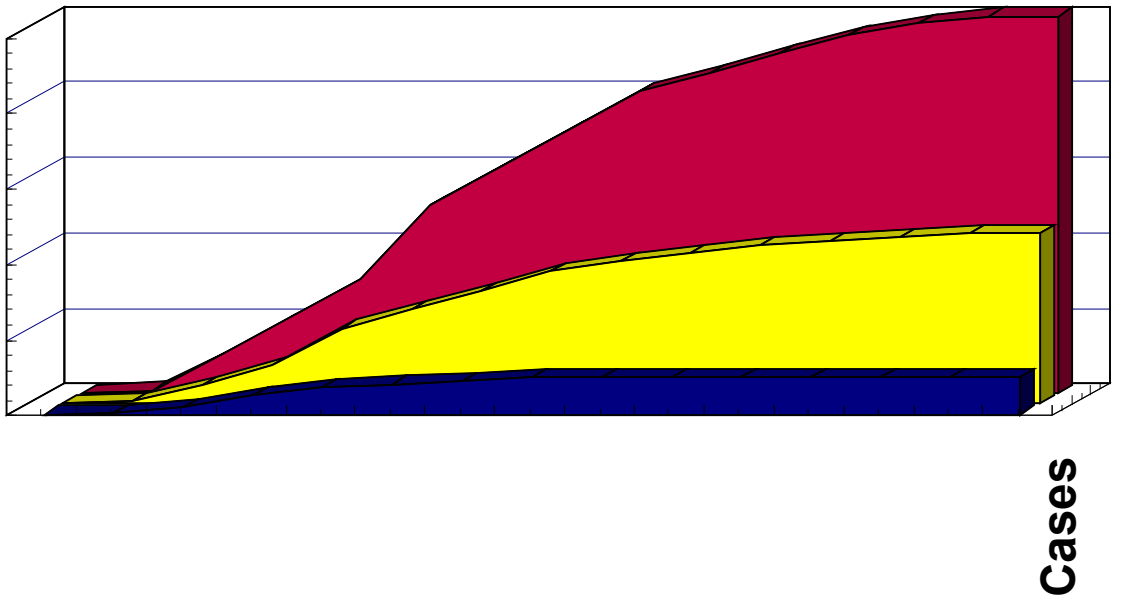
Without strong integrity, and with increased networking, DCAs are essentially unstoppable.

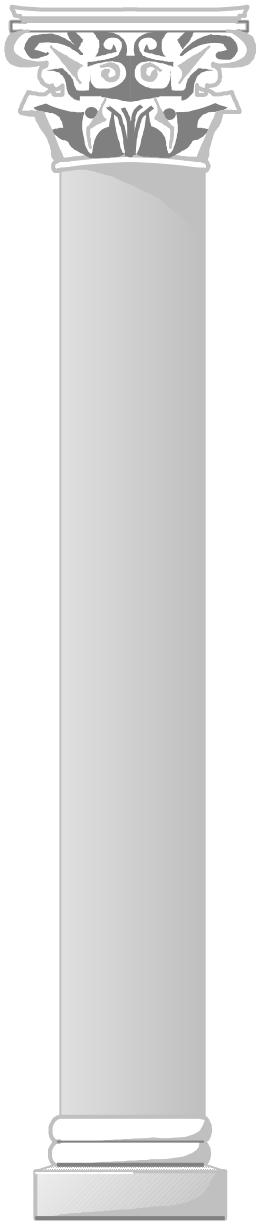
Tracking to source quickly becomes as hard as searching the whole world - without traceability (a.k.a. source authentication) things get bad fast.

Networking+Vulnerabilities=>DCAs

All of these are increasing quickly

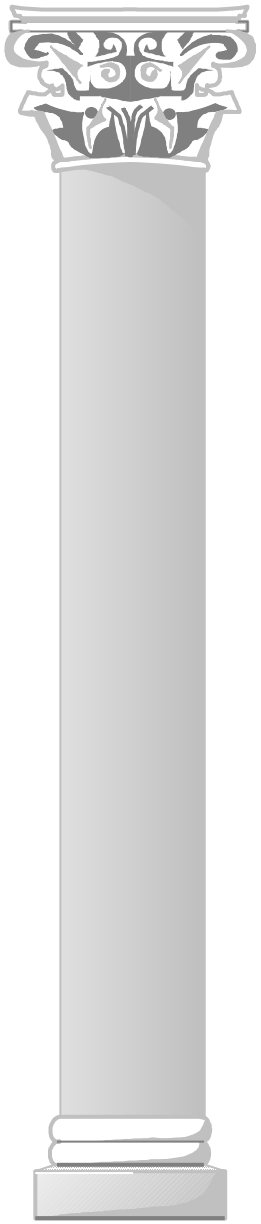
Some speculation on DCAs





Enabling Technologies

New vulnerabilities increasing(t)
Intermediaries increasing(t)
Connectivity increasing(t)
Network-based access increasing(t)
Remote and traveling computing...
Home-based businesses and computing...
Telecommuting and trust distribution
Virtual businesses and constant work flux



Summary

DCAs are here to stay
Things will get worse
They may never get better
DCA's will be very good IW weapons
Defenses at the NII level will be critical to national defense and success
Audit trails are the best hope for tracking down DCA attackers
The need to cross-correlate audit trails will lead to substantial legal challenges

Don't Forget

Fill out your course evaluation form
Have a great day!