# Reaching Past the Low Hanging Fruit

*Todd Heberlein*

Net Squared, Inc.

todd@NetSQ.com

SANS 99

10 May 1999

# Acknowledgements

Dan Teal

Ricardo Anguiano

Kevin Ziese

Matt Bishop

Karl Levitt

Cisco

UC Davis Security Lab

Fred Cohen

Dick O’Brien

Mike Dean

Rome Labs’ IW Teams

Jerry Hamilton

Marvin Christensen

IA Team

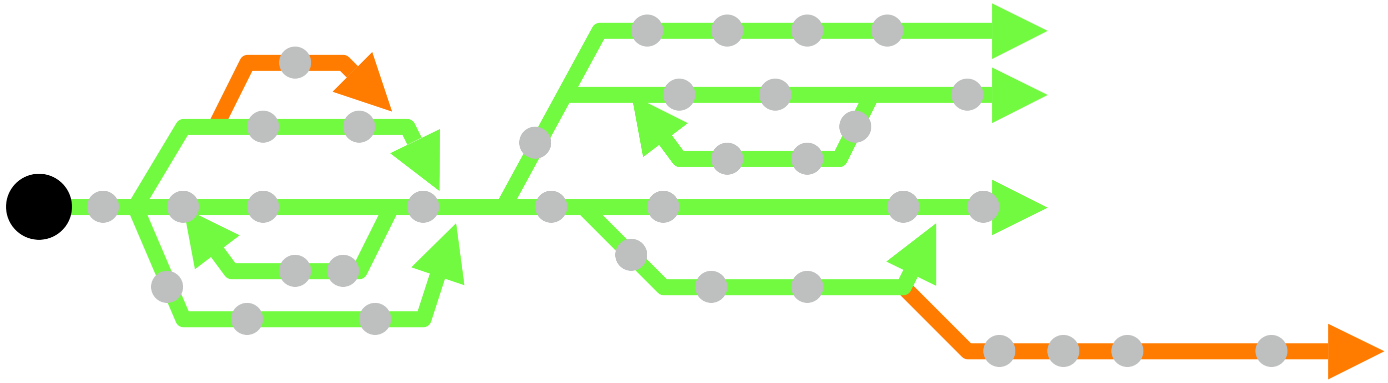
# Overview

- Detecting new attacks
  - sequence-based
  - StackGuard
  - specification-based
- Forensics
  - Need to understand what may or may not be an attack
  - Correlation: finding and understanding the subtle data
- Scaling
  - thousands of signatures
  - larger, more distributed attacks
  - Reduction through integration
- Accelerating the tempo

# Detecting New Attacks

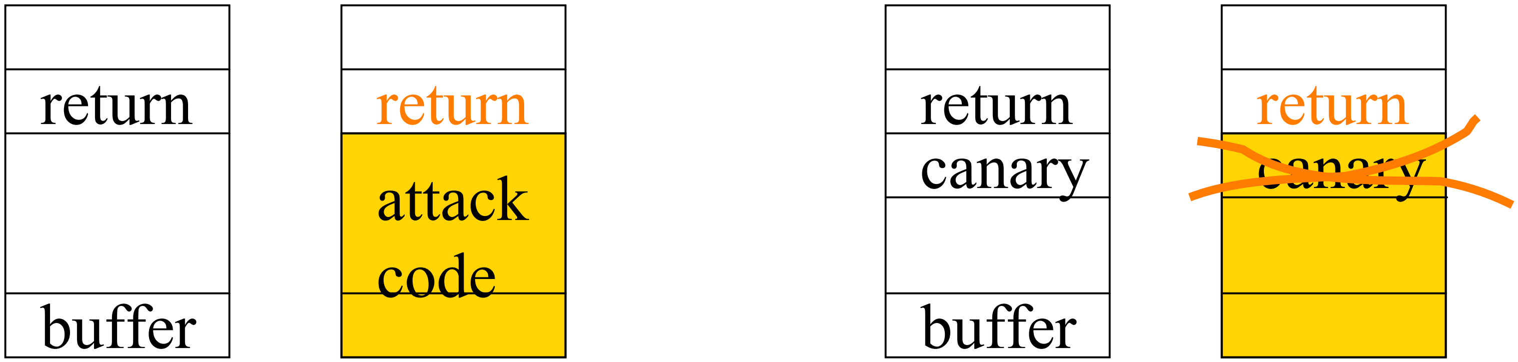
- Generally easier from the host (opinion!)
- Generic signatures
  - illegal transition to root
- Sequence-based detection
  - Profiling programs, not people
- StackGuard
- Specification-based detection
- Forensics, data mining, discovery

# Sequence-based ID



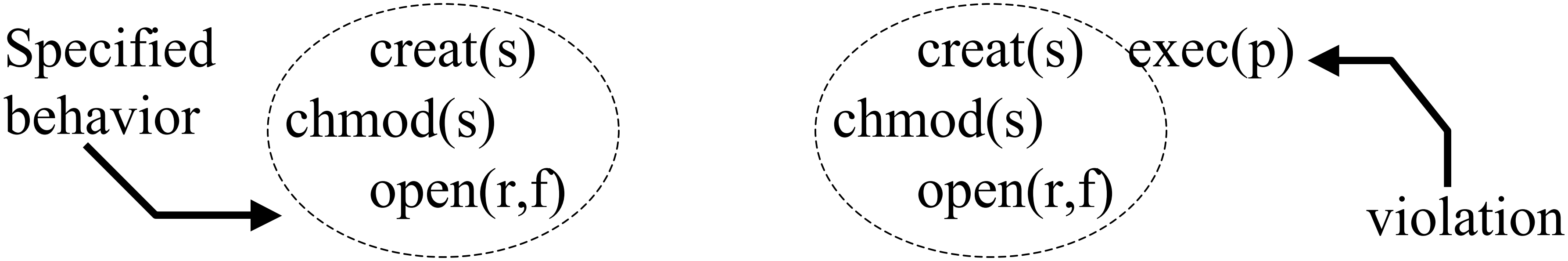
- Profile a **program**
- Profile based on model of execution path
  - sequences of system calls **learned**
- University of New Mexico
  - http://www.cs.unm.edu/~immsec/html-misc/ids.html
- Reliable Software Technologies
  - aghosg@rstcorp.com

# StackGuard



- Many of today’s attacks involve buffer overflow
  - Overflow buffer, insert code, reset return address
- StackGuard places a canary between buffers and return address pointers
  - Overflow will corrupt canary
  - Overflow is detected, reported, halted
- http://www.cse.ogi.edu/DISC/projects/immunix/StackGuard/

# Specification-based ID



Specified behavior

creat(s)
chmod(s)
open(r,f)

creat(s) exec(p)
chmod(s)
open(r,f)

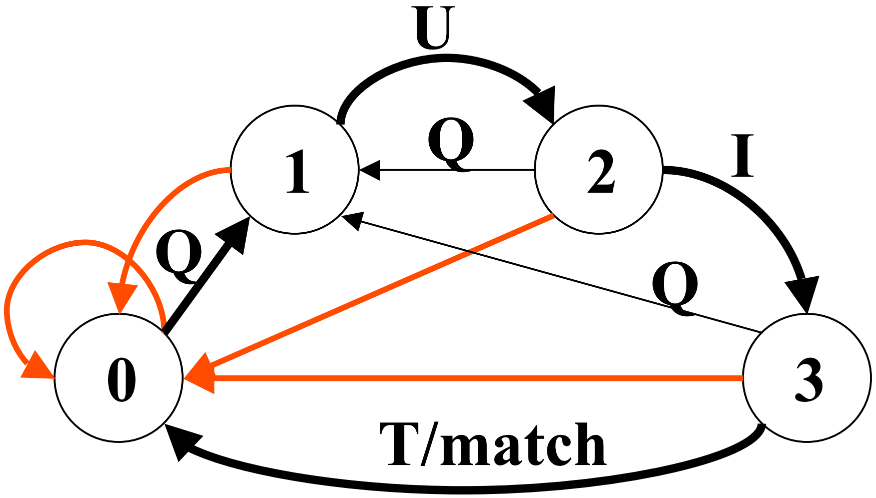
violation

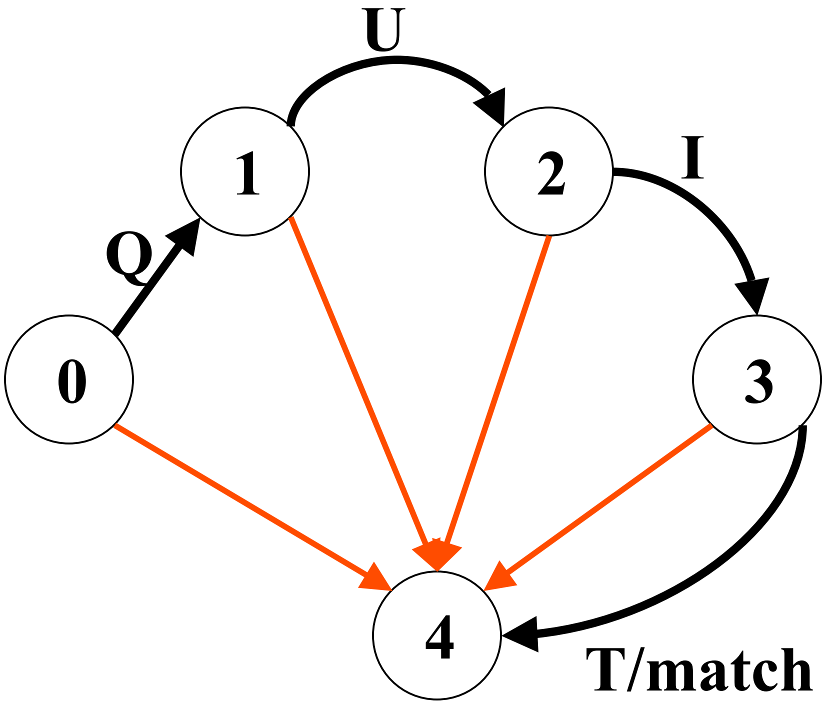
- Define/specify what a **program** should do
  - focus on network and privileged programs
- Detect programs exceeding their specification
- Approach is being incorporated into wrappers (FreeBSD, NT, Solaris)
- Publications:
  - http://seclab.cs.ucdavis.edu/papers/pdfs/ck-mr-kl-97.pdf
  - http://seclab.cs.ucdavis.edu/~ko/papers/thesis.pdf

# Forensics: Understanding and Discovering Attacks

- Mistakes to prime your thinking
  - The FTP Sweep
  - 10 million connection DOS
  - Sendmail’s mysterious QUIT
  - Warez that wasn’t
- Correlation
  - Finding related activity
  - Beyond random attacks: is the semiconductor industry under attack?

# QUIT vs. QUIT





I QUIT yes

QUIT yes

I QUIT NO

QUIT yes

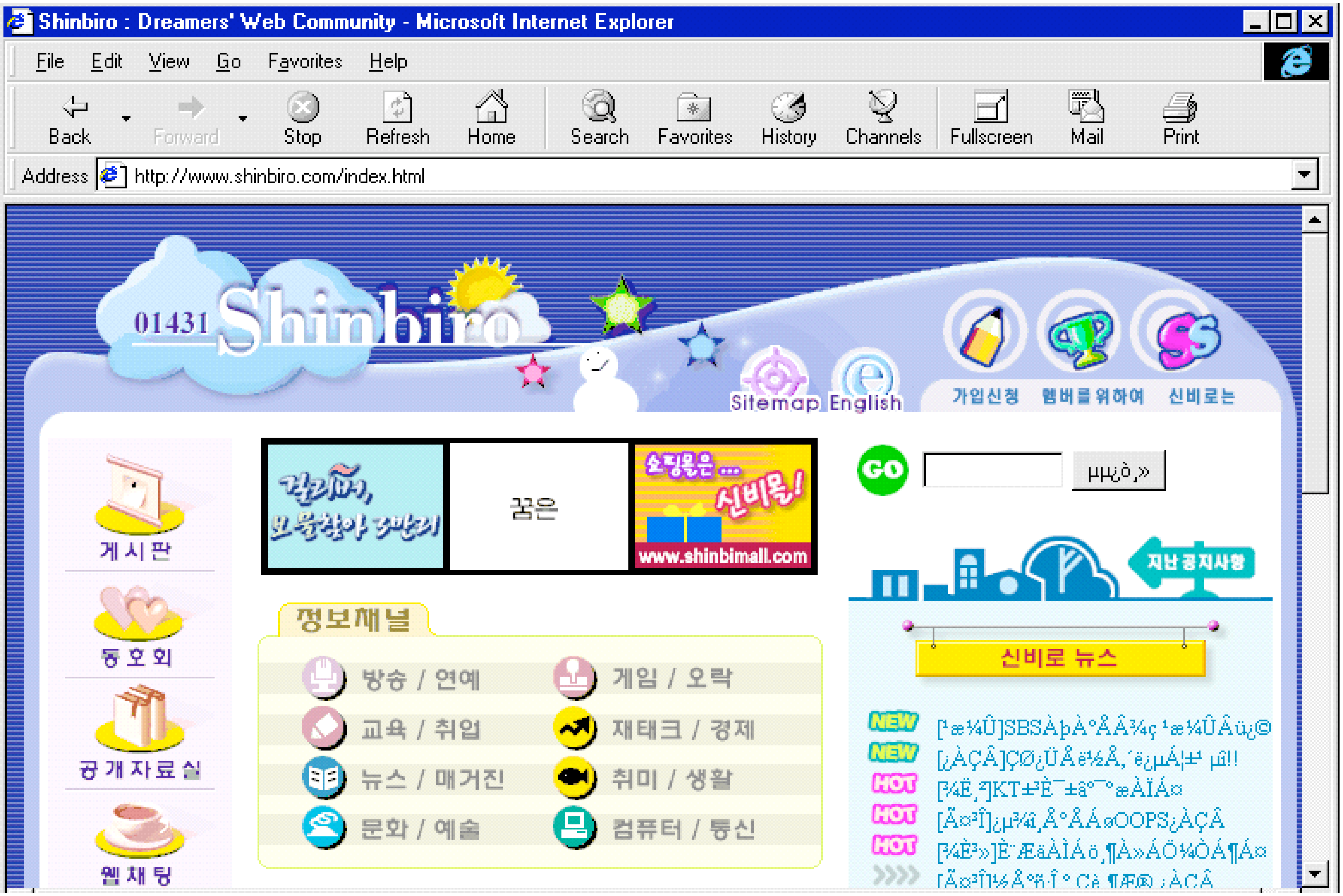
# Warez Attack?

```
--------------------------------------------------------
2531844  170.236.61.27  --> 167.103.221.216 (1404 -> 21)
from: 19:02:47 ( 7/23/1998)  to: 19:17:38 ( 7/23/1998)
client flags: SA R    server_flags: SA
        ---- FTP ---------------------------------------
        USER: anonymous
        PASS: xxxxxxxxx
        RETR: /!!!__µå_Ã À__î°¸_Å_ß ÇÕ´Ï´Ù!!!.txt
              /Mpeg-°¡¿ä/[ÀÌ_ÂÈ ] ÃµÀÏµ¿_È MV-by ego.MPG
        CWD:  /
              /Mpeg-°¡¿ä/
        FAILURES: 0

--------------------------------------------------------
2529427  170.236.61.27  -->  203.29.143.17  (1402 -> 80)
from: 19:01:36 ( 7/23/1998)  to: 19:01:38 ( 7/23/1998)
client flags: SAF     server_flags: SAF
--------------------------------------------------------
```

http://www.shinbiro.com/home.html

# Non-ASCII Character Sets



[¹æ¼Û]SBSÀþÀ°ÅÂ¾ç ¹æ¼ÛÂü¿©

[¿ÀÇÂ]ÇØ¿ÜÅë½Å¸´ë¿µÁ¦±¹ µî!!

[¾Ë¸²]KT±³È¯±â°¯°æÀÏÁ¤

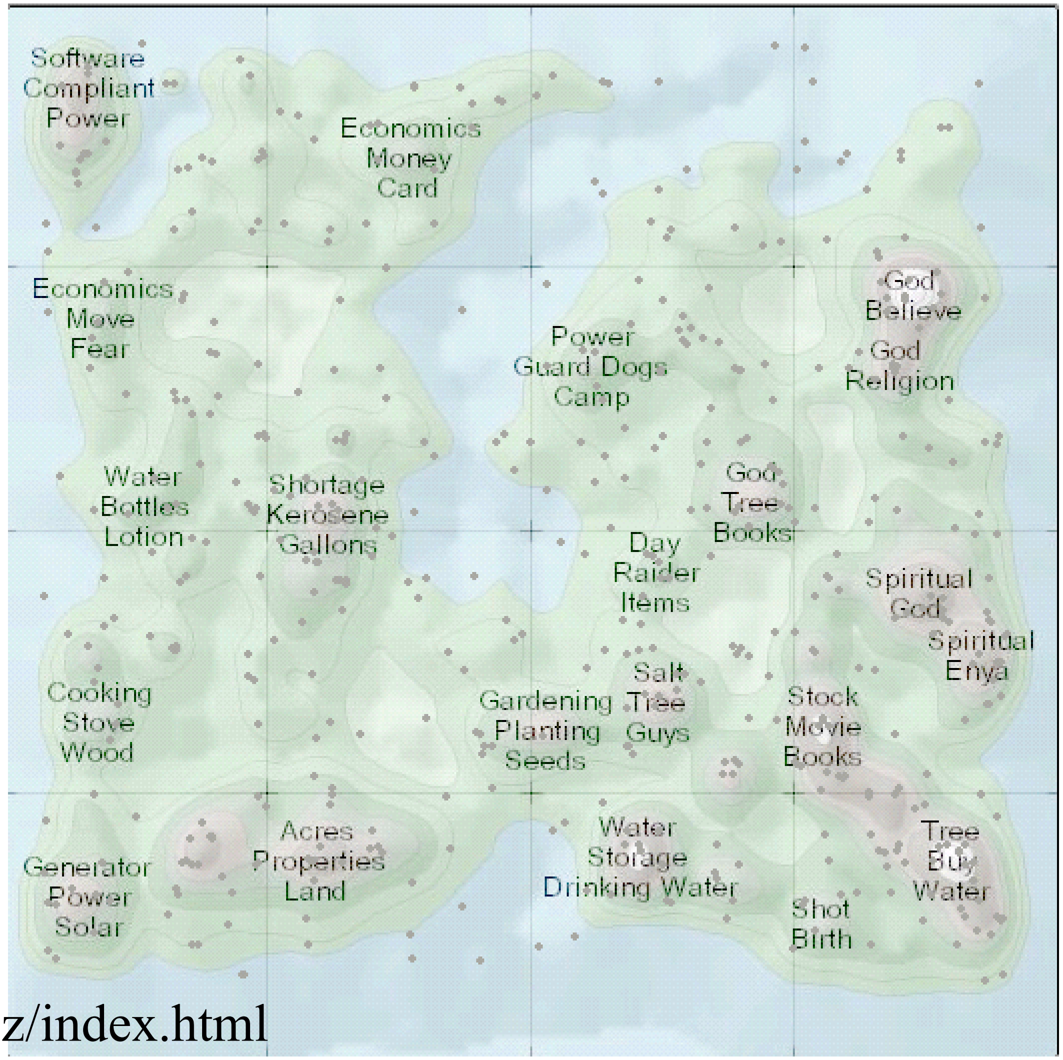
[Ã¤³Î]¿µ³ú¸Å°ÅÁøOOPS¿ÀÇÂ

[¾È³»]È¨ÆäÀÌÁö¸¶À»ÁÖ¼ÒÁ¶Á¤

[Ã¤³Î]½Å°ñ·Î°Ç¶ÆÆ®¿ÀÇÂ

# Themescape

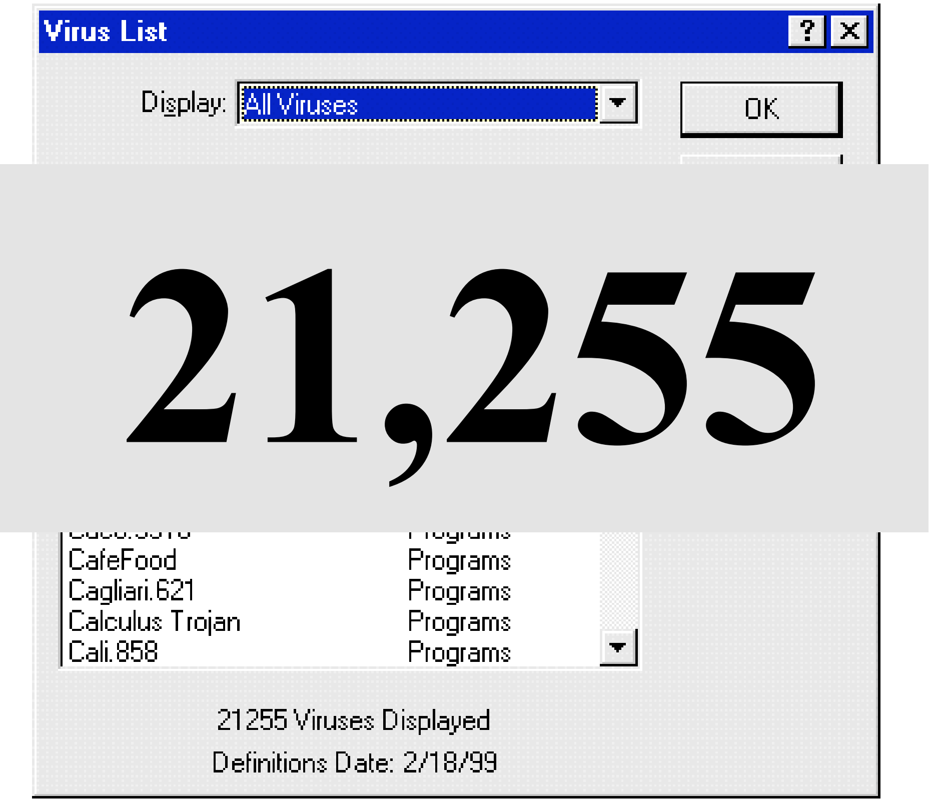
- Themescape discovers clusters of related data sources
- NSA applied similar tools (parentage/acquaintance) to session data from a large DOD break-in
- Pacific Northwest National Laboratory is developing visualization tools



**http://demo.cartia.com**

http://multimedia.pnl.gov:2080/infoviz/index.html

# Tens of Thousands of Signatures



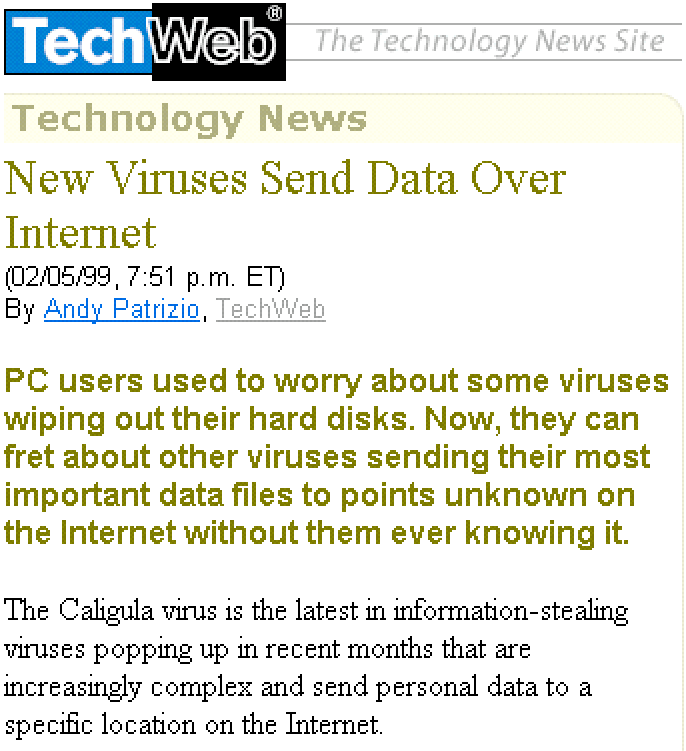
Display: All Viruses

# 21,255

| | |
|---|---|
| CafeFood | Programs |
| Cagliari.621 | Programs |
| Calculus Trojan | Programs |
| Cali.858 | Programs |

21255 Viruses Displayed

Definitions Date: 2/18/99



Technology News

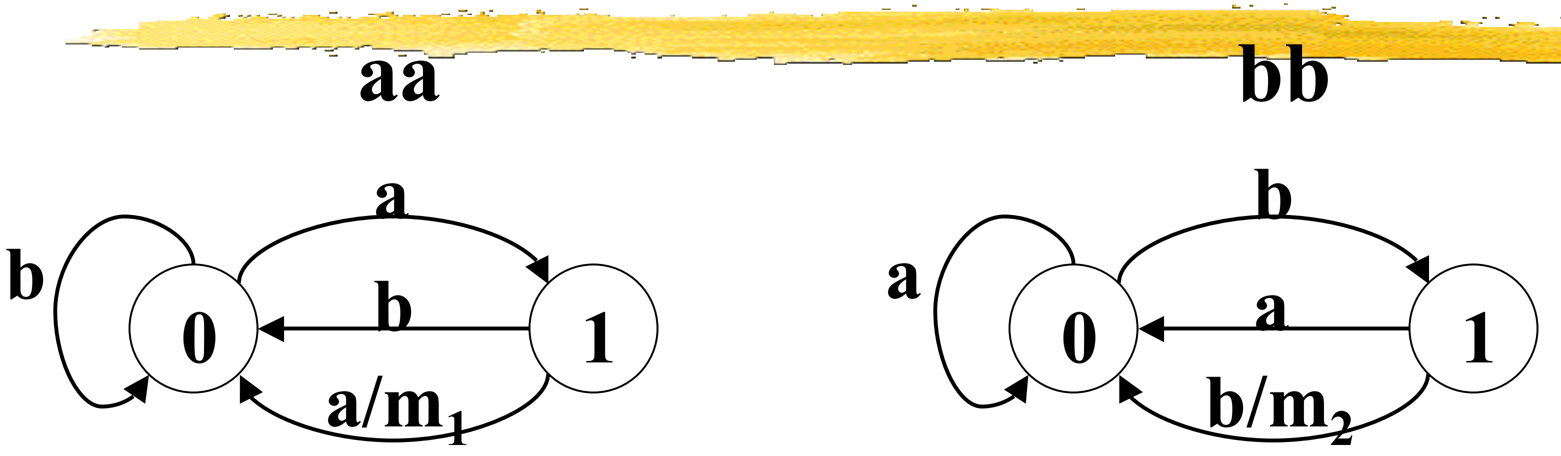
## New Viruses Send Data Over Internet

(02/05/99, 7:51 p.m. ET)
By Andy Patrizio, TechWeb

**PC users used to worry about some viruses wiping out their hard disks. Now, they can fret about other viruses sending their most important data files to points unknown on the Internet without them ever knowing it.**

The Caligula virus is the latest in information-stealing viruses popping up in recent months that are increasingly complex and send personal data to a specific location on the Internet.

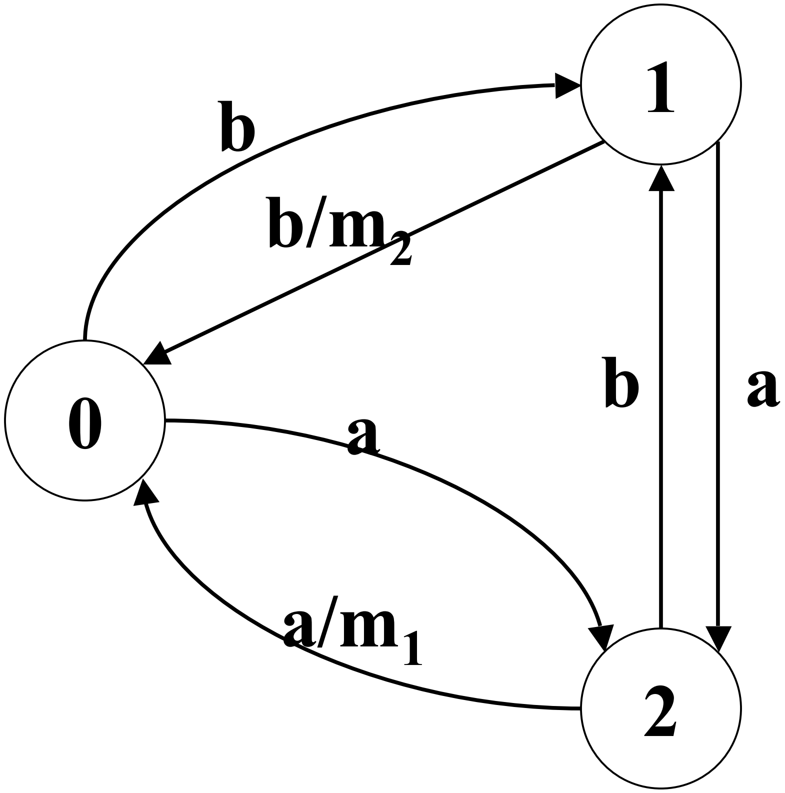
# Scaling Through Signature Compression



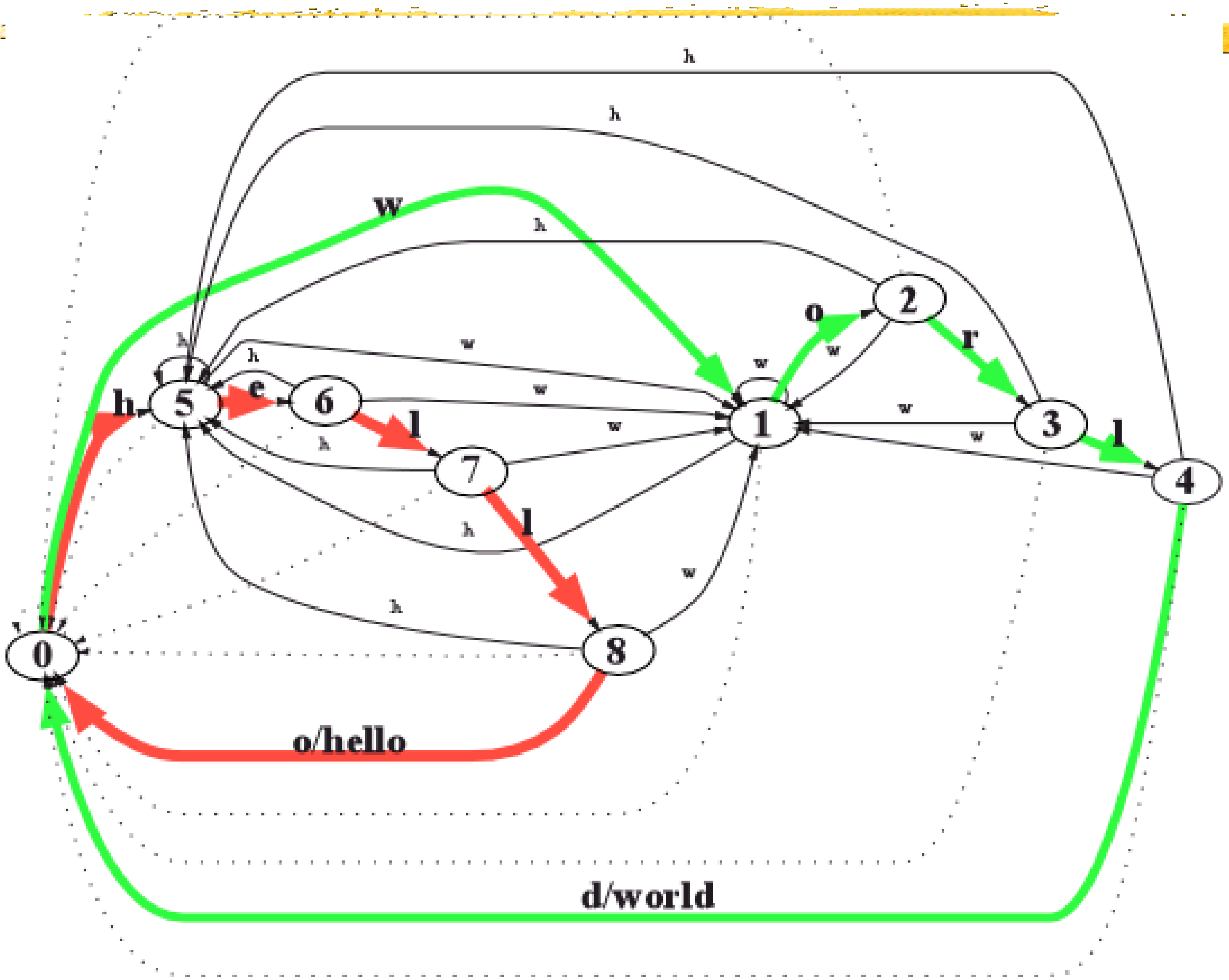
- Moving from a few tens of signatures to a tens of thousands of signatures
- If the signature can be represented by a regular expression or finite state machine, you can use cross-products to merge signatures

# Merged Signatures

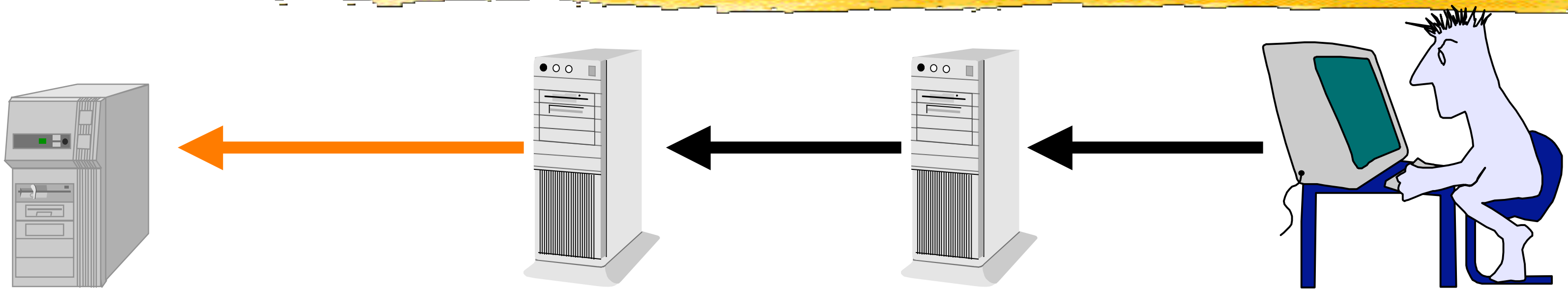
|   | a | b |
|---|---|---|
| 0 | 2 | 1 |
| 1 | 2 | 0/$m_2$ |
| 2 | 0/$m_1$ | 1 |



# Hello X World Signature



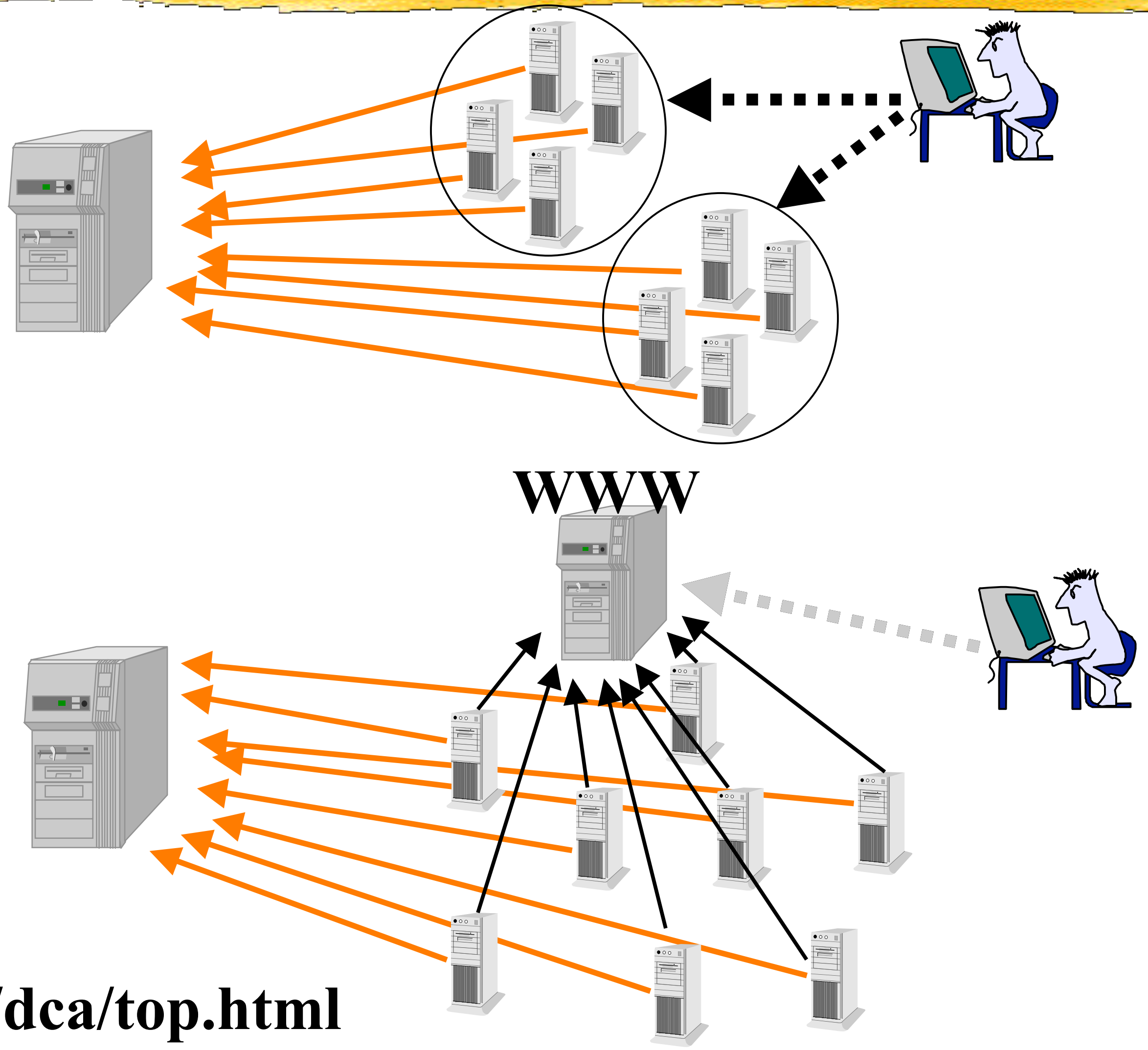
# The Changing Threat Model



- The original vision of the intruder
- Someone establishes a presence in your system
- Umbilical cord back to the original intruder
- Cuckoo’s egg model
- trace back, hack back, thumbprint back

# Distributed Attacks

- Smurf Attacks
- Distributed Coordinated Attacks
  - WWW attacks
  - Mailing lists
- Who do you block?
- How do you find the source?

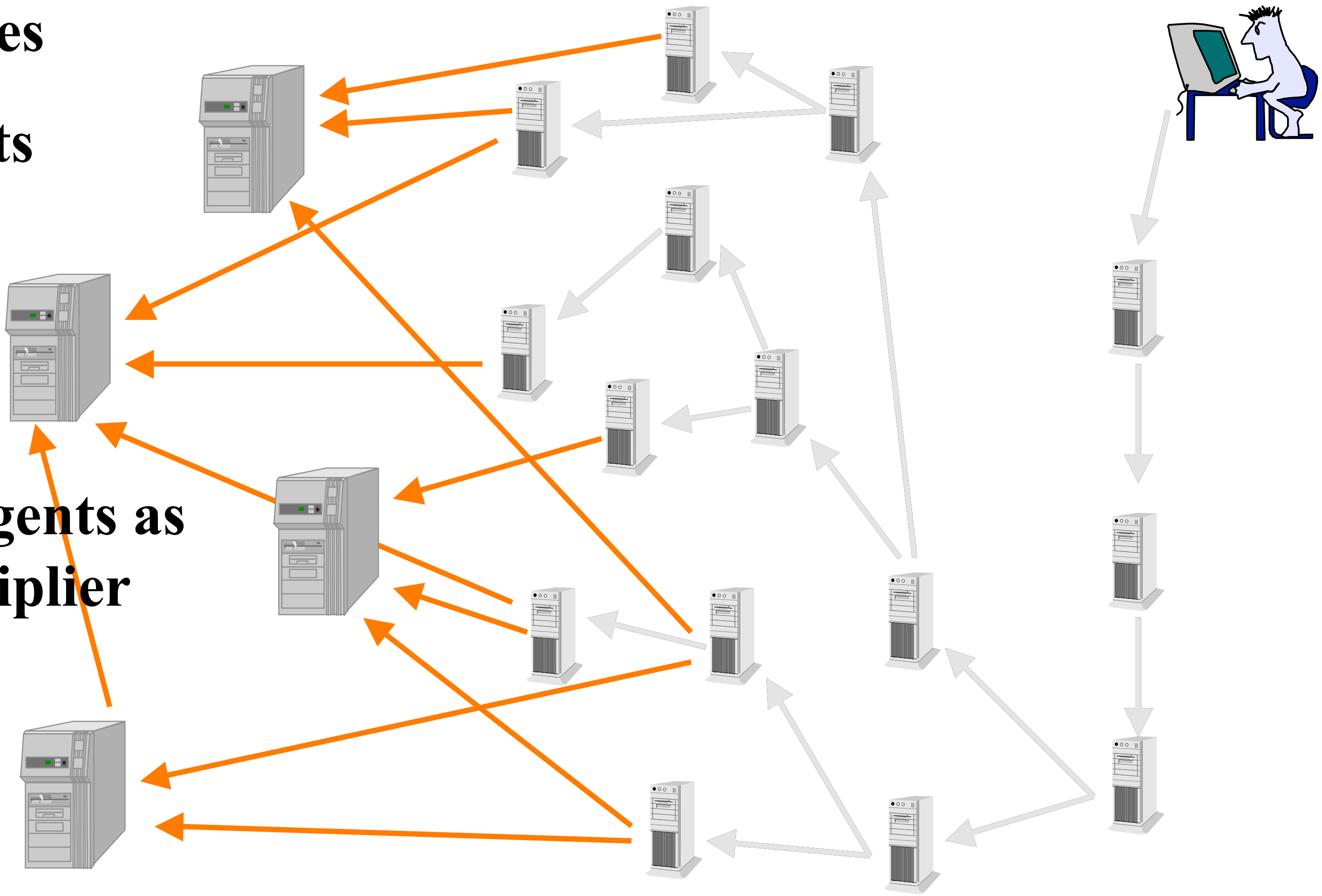


**http://all.net/books/dca/top.html**

# The Agent War

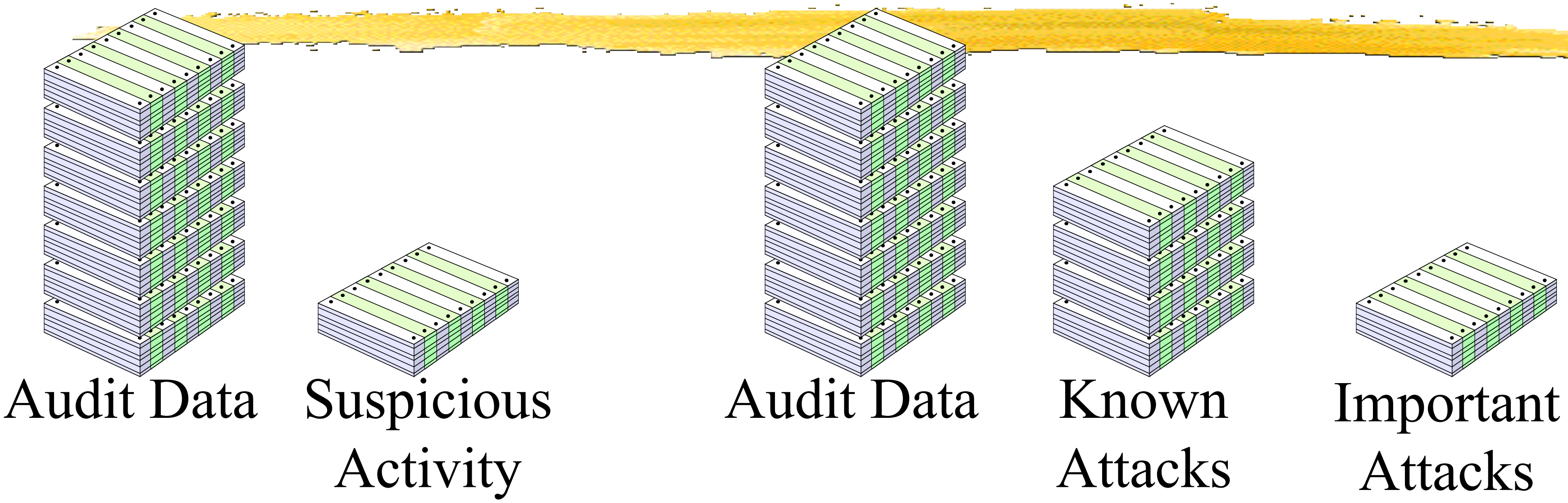
10,000 sources

10,000 targets



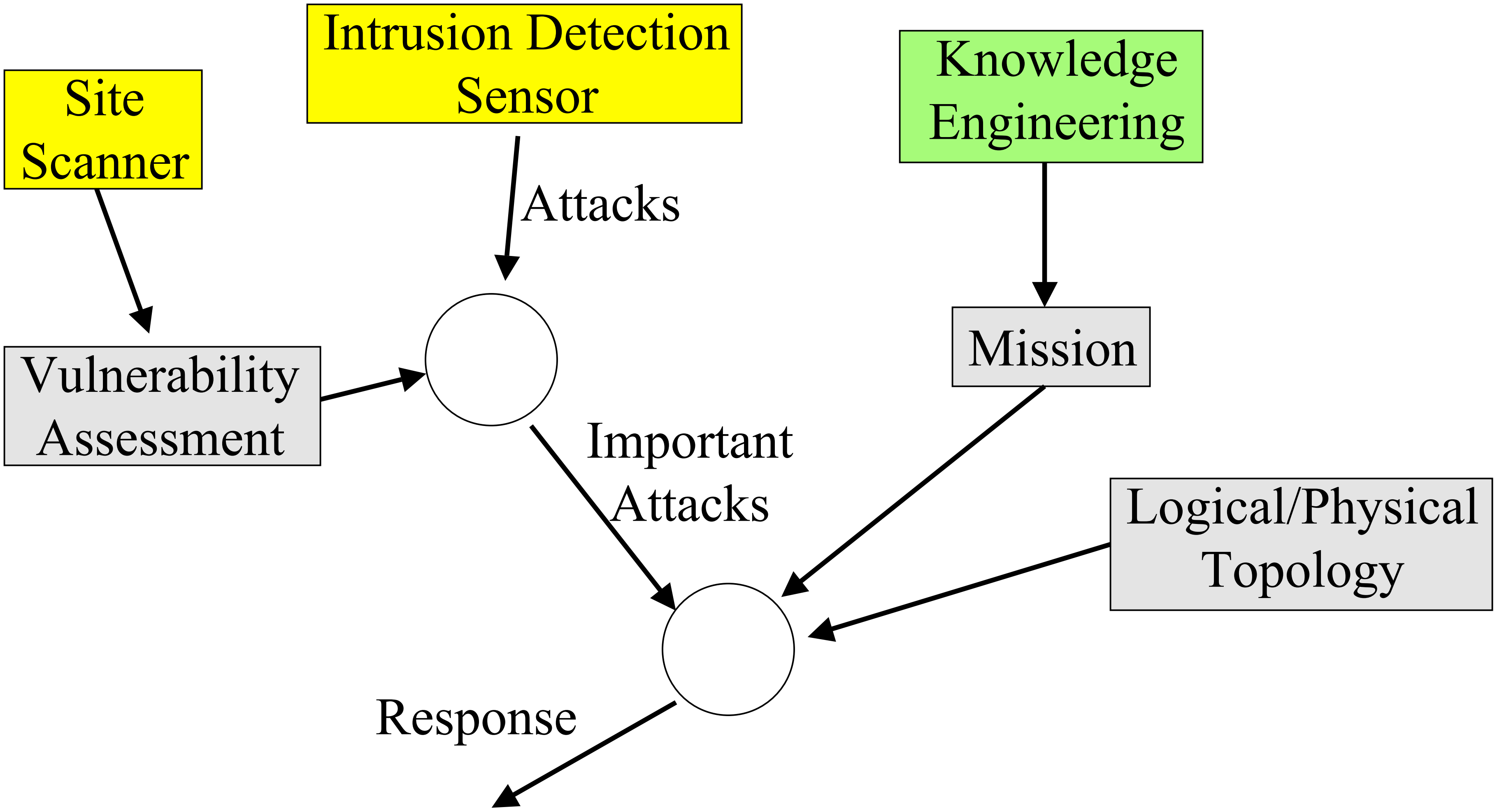
Intelligent Agents as
a Force Multiplier

# Scaling Through Attack Reduction

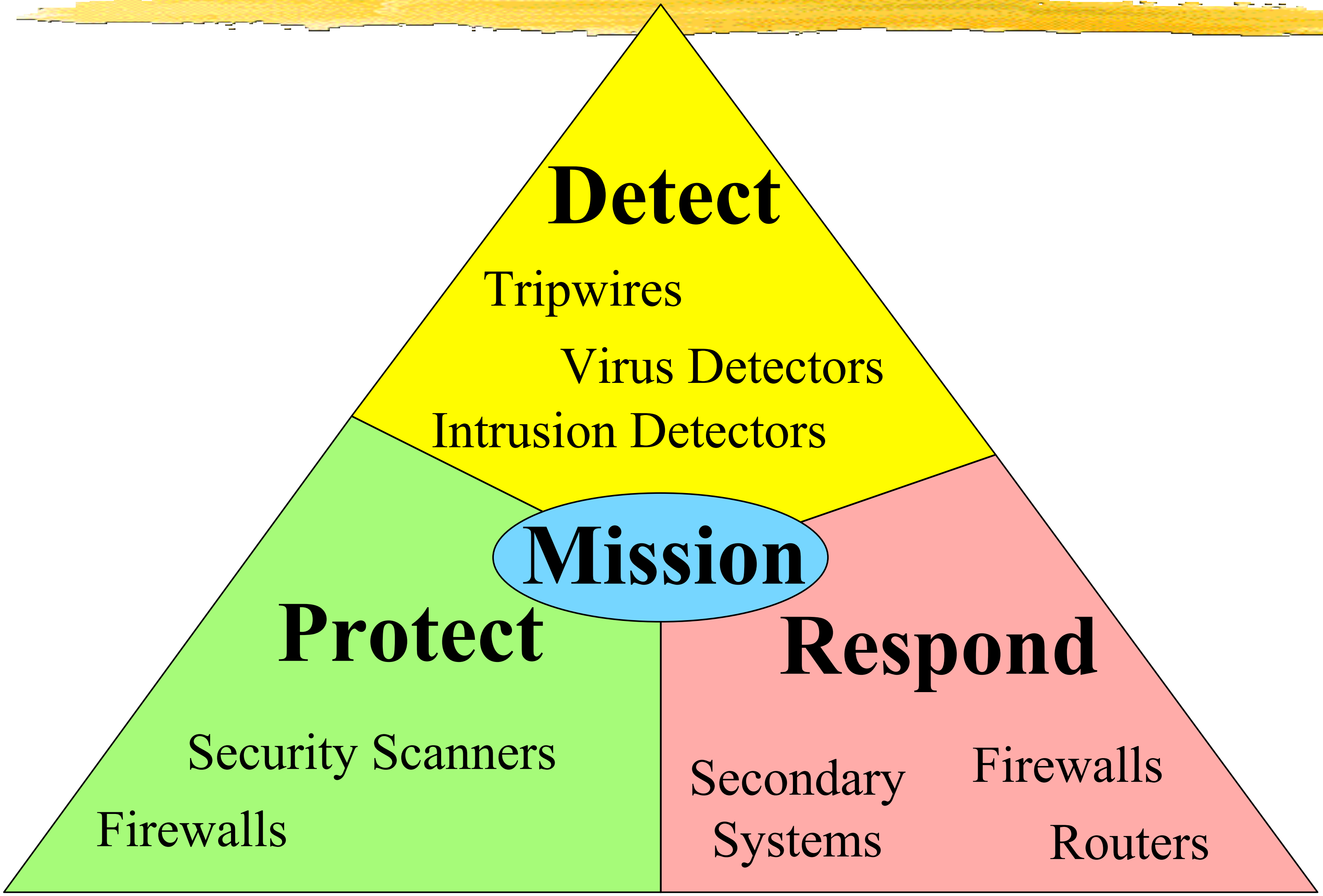


- Intrusion detection used to be called “audit reduction”
- Today, even the number of obvious attacks can be overwhelming
- Need to reduce to the important attacks

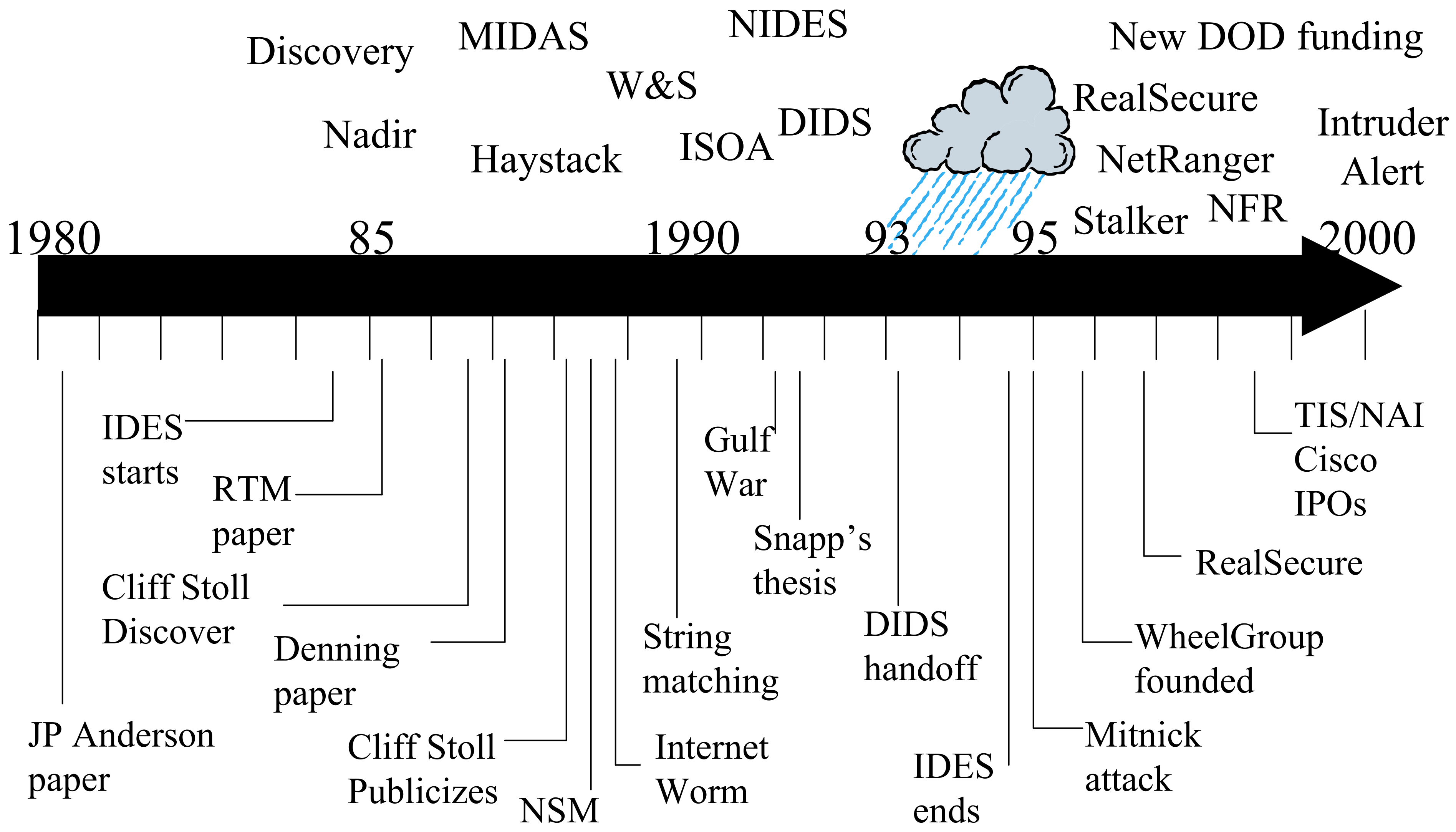
# Expanding the Picture



# Scaling Through Integration



# Timeline



Discovery

Nadir

MIDAS

Haystack

W&S

NIDES

ISOA

DIDS

RealSecure

NetRanger

Stalker

NFR

New DOD funding

Intruder Alert

1980

85

1990

93

95

2000

JP Anderson paper

IDES starts

RTM paper

Cliff Stoll Discover

Denning paper

Cliff Stoll Publicizes

NSM

Internet Worm

String matching

Gulf War

Snapp's thesis

DIDS handoff

IDES ends

Mitnick attack

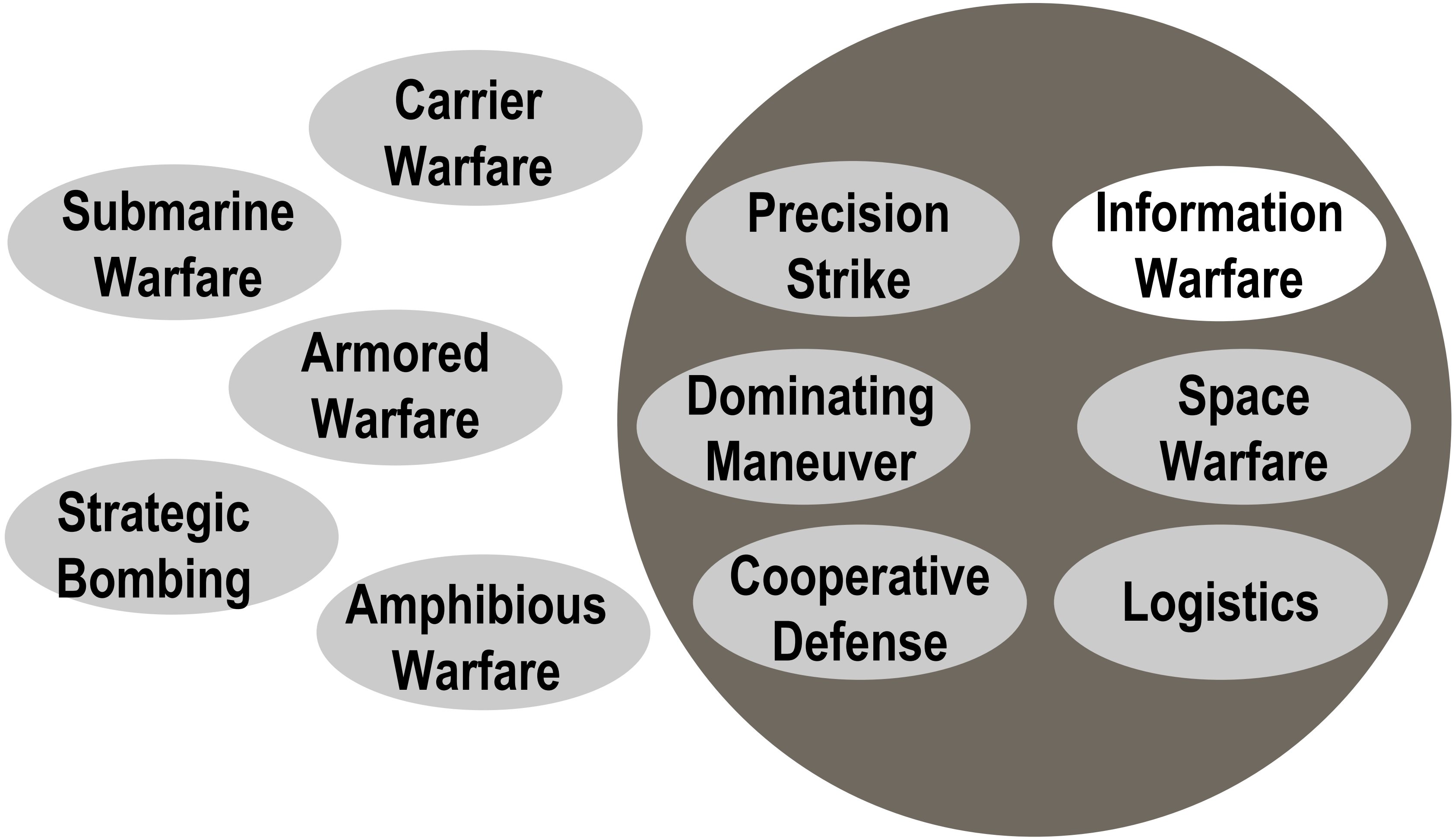
WheelGroup founded

RealSecure

TIS/NAI Cisco IPOs

Provided by DARPA

# Revolutions in Military Affairs



Carrier Warfare

Submarine Warfare

Armored Warfare

Strategic Bombing

Amphibious Warfare

Precision Strike

Information Warfare

Dominating Maneuver

Space Warfare

Cooperative Defense

Logistics

World War II

Emerging RMA

Provided by DARPA

# OODA Loops: Time & Command

*Civil War*

**Observe: Dispatch**
**Orient: Days**
**Decide: Weeks**
**Act: Months**

*World War II*

**Observe: Radio/wire**
**Orient: Hours**
**Decide: Days**
**Act: Weeks**

*Gulf War*

**Observe: Near real**
**Orient: Minutes**
**Decide: Hours**
**Act: Days**

*Tomorrow*

**Observe: Real time**
**Orient: Continuous**
**Decide: Immediate**
**Act: Hours**

# Information Pillar

*Information has been one of the pillars of our national strategy...*

*Now it is the dominant feature*

VADM Cebrowski, J6

# Summary

- We’ve made tremendous advancement in detecting intruders, but there are still many challenges.
  - Detecting new/original attacks
  - Understanding attacks
  - Scaling for asymmetric warfare
    - size & number of attacks
    - accelerating the OODA loops
- The war is coming, the clock is ticking