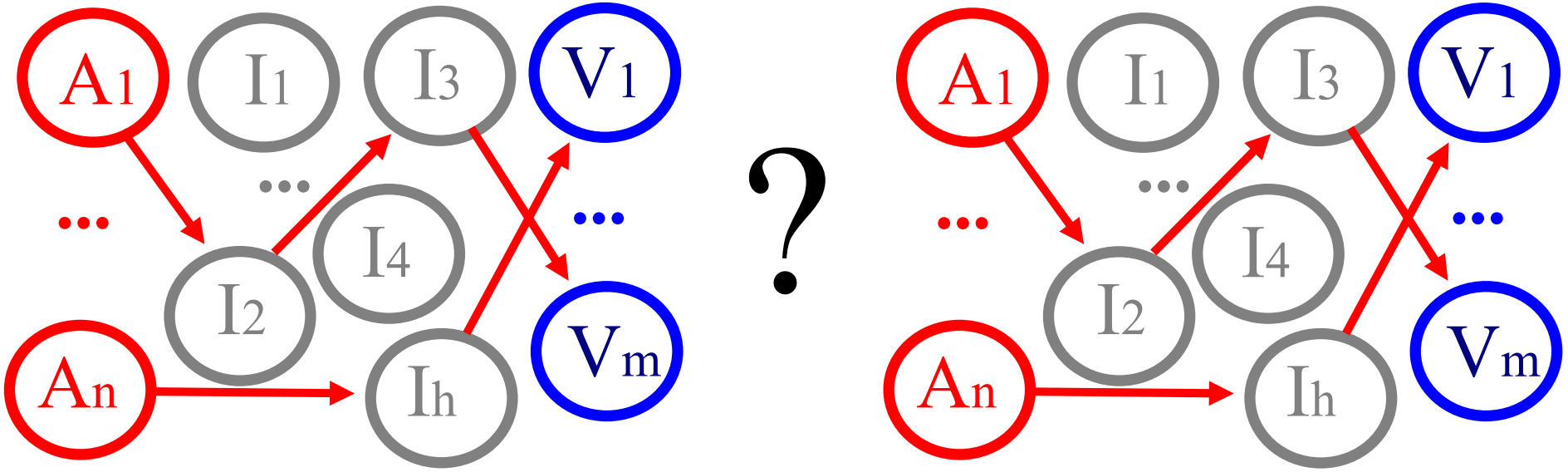
DCAs Then and Now

Distributed Coordinated Attacks

Then and Now

Fred Cohen
CEO – Fred Cohen & Associates
President – California Sciences Institute



Outline

- Background
  - Of the speaker
  - Of the talk
- Definitions
  - Have they changed?
- Examples
  - Have they been realized?
  - Is there anything new?
- DCAs in IW
  - What has been realized?
  - What has not?
  - What did I miss?
- DCA Defenses
  - Here, there have been changes!!!
- Summary & Conclusions
  - Questions & Comments

Background of the Speaker

- Some career accomplishments
  - MS Information Science, Ph.D. EE
  - First examined “Computer Viruses” and defenses
  - First defined “Information Assurance” as used today
  - Critical infrastructure protection starting in 1992
  - 30+ years of research, development, consulting in the information protection arena
  - 150+ professional papers, 10+ books, hundreds of presentations and talks, and on and on
- President: “California Sciences Institute”
  - Non-profit post-graduate educational institution

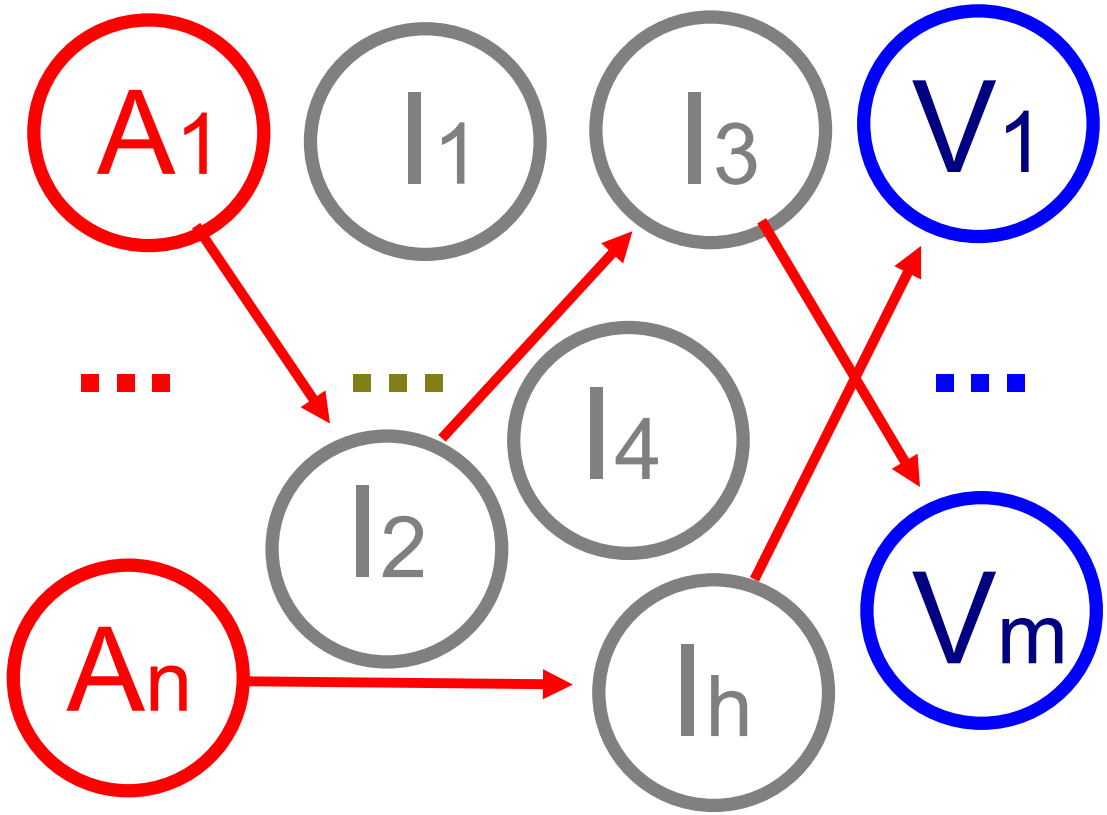
Background of the Talk

- 1996: A paper (all.net > Library > Technical Safeguards > 1996: A Note On Distributed Coordinated Attacks)
- 1996: A presentation at CSI and elsewhere
- 2008: So what exactly has changed since then?
- Approach:
  - Show the slides from 1996
  - Look for the differences
  - For this I will need your help!

Outline

- Background
  - Of the author
  - Of the talk
- Definitions
  - Have they changed?
- Examples
  - Have they been realized?
  - Is there anything new?
- DCAs in IW
  - What has been realized?
  - What has not?
  - What did I miss?
- DCA Defenses
  - Here, there have been changes!!!
- Summary & Conclusions
  - Questions & Comments

Has this picture changed?



Outline

- Background
  - Of the author
  - Of the talk
- Definitions
  - Have they changed?
- Examples
  - Have they been realized?
  - Is there anything new?
- DCAs in IW
  - What has been realized?
  - What has not?
  - What did I miss?
- DCA Defenses
  - Here, there have been changes!!!
- Summary & Conclusions
  - Questions & Comments

Has this been done yet?

- √Web-based FW bypass
- √Password guessing DCA
- √DCA through a firewall
- √A multi-hop DCA
- √A virus as a DCA
- √911 DCA
- One-per-site DCA
- Probabilistic DCA
- √Email SPAM as a DCA
- Forged IP address DCA
- Super-spam DCA
- Perception management DCA

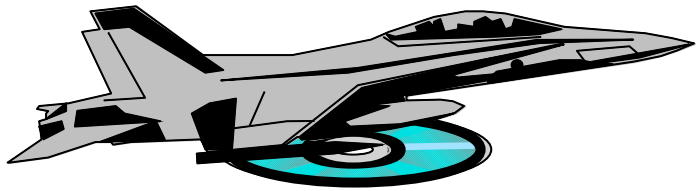
What else has been done?

Outline

- Background
  - Of the author
  - Of the talk
- Definitions
  - Have they changed?
- Examples
  - Have they been realized?
  - Is there anything new?
- DCAs in IW
  - What has been realized?
  - What has not?
  - What did I miss?
- DCA Defenses
  - Here, there have been changes!!!
- Summary & Conclusions
  - Questions & Comments

DCAs as IW weapons

- Have these properties been realized? Examples?
  - Easily controlled
  - Pinpoint targetable
  - Effect easily measurable
  - Hard to trace
  - Demonstrated causation
  - Plausible deniability
  - Used for deceptions
  - Hard to selectively block
  - Achieve deep penetration



Has this damage been done?

- In IW? - Provide example
  - Denial of services
  - Computational leverage
  - Open-loop exploits
  - Bypass attacker-specific defenses
  - Consume limited protective resources
  - Perception management and deception
  - Stress failures of other protection and systems

What did I miss?

- Other IW examples of DCAs?
  - –

Outline

- Background
  - Of the author
  - Of the talk
- Definitions
  - Have they changed?
- Examples
  - Have they been realized?
  - Is there anything new?
- DCAs in IW
  - What has been realized?
  - What has not?
  - What did I miss?
- DCA Defenses
  - Here, there have been changes!!!
- Summary & Conclusions
  - Questions & Comments

Technology issues

- Enabling technologies:
  - Still getting more of them
    - Networking - Remote execution and open access - Uncontrolled Internet environment - Insecure ISPs - DC programs – Trust distribution – Mobile computing
- Prevention?
  - Disable enablers? - No
  - Eliminate vulnerable intermediaries – No
  - Private Inter-Networks
    - Some
- The real breakthroughs:
  - Detection:
    - Detect dramatic changes in event rates - YES
    - Coordinated defenses – Yes
    - Zero tolerance detect? No
    - Better audit analysis? Yes
  - And
    - Honeynets and similar
    - Others?

Theoretical limits

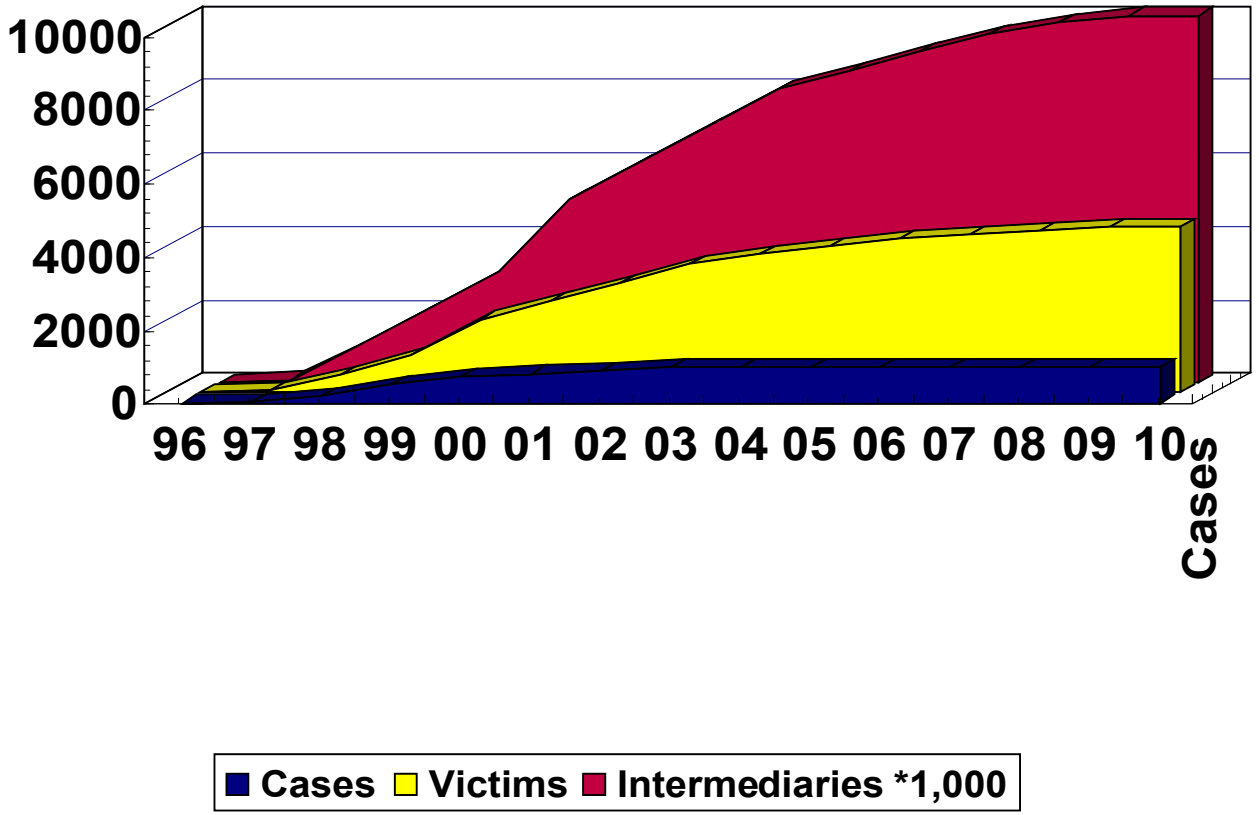
- They have not changed:
  - Without strong integrity, and with increased networking, DCAs are essentially unstoppable.
  - Tracking to source quickly becomes as hard as searching the whole world - without traceability (a.k.a. source authentication) things get bad fast.
  - Networking+Vulnerabilities => DCAs
- All of these are still increasing quickly

Outline

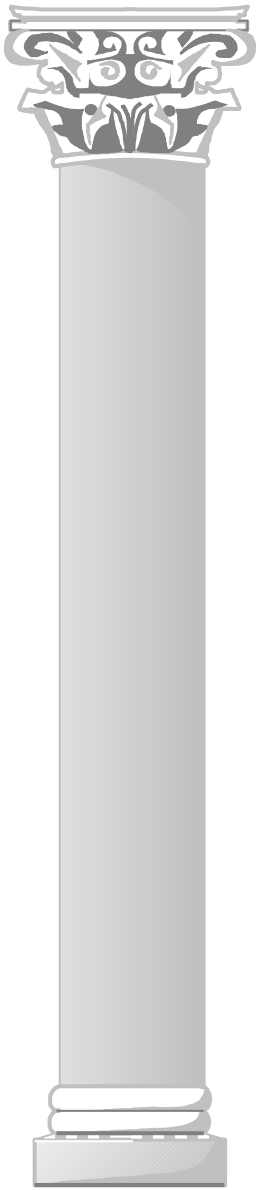
- Background
  - Of the author
  - Of the talk
- Definitions
  - Have they changed?
- Examples
  - Have they been realized?
  - Is there anything new?
- DCAs in IW
  - What has been realized?
  - What has not?
  - What did I miss?
- DCA Defenses
  - Here, there have been changes!!!
- Summary & Conclusions
  - Questions & Comments

How far off was I?

- 2008:
  - A few hundred cases per year of the use of DCAs?
  - 4,000 targets of DCAs in 2008?
  - A million intermediaries in 2008?



The retro slide still applies



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

Thank You

Questions?
Discussion?!

Dr.Cohen at Mac.Com
http://all.net/