Distributed Denial of Services

2012-11-15

San Francisco Electronic Crimes Task Force

Dr. Fred Cohen
CEO – Management Analytics (non-government)
President - California Sciences Institute (501(c)(3))
CEO – Fred Cohen & Associates (government only)

Management Analytics

Outline

- The (recent) history of distributed coordinated attacks
- The state of distributed denial of services today
- Countermeasures
- Questions / Comments?

65% of organizations experience three DDoS attacks a year

Posted on 14 November 2012.

BOOKMARK ...

Despite the increasing sophistication and severity of cyber attacks, a survey of more than 700 senior IT professionals reveals that organizations are surprisingly unarmed to deal with today's threat landscape, according to the Ponemon Institute and Radware.

http://www.net-security.org/secworld.php?id=13949

Management Analytics

History

- 1996: A Note On Distributed Coordinated Attacks
  - all.net > Research > Technical Safeguards > 1996:...
- 1996: A presentation at CSI and elsewhere
- 2008: A Presentation at ISOI and elsewhere
- 2012: So what has changed since then?
- Approach:
  - Show the slides from 1996 / 2008
  - Look for the differences

Management Analytics

Ancient History

- The history of war and conflict involves (Sun Tzu ~500BC)
  - Denial of limited resources (arguably the main strategy)
    - "Now, when your weapons are dulled, your ardor damped, your strength exhausted and your treasure spent, other chieftains will spring up to take advantage of your extremity. Then no man, however wise, will be able to avert the consequences that must ensue."
  - The conflict between speed/skill and bulk
    - "If he is in superior strength, evade him. If your opponent is of choleric temper, seek to irritate him. Pretend to be weak, that he may grow arrogant. If he is taking his ease, give him no rest. If his forces are united, separate them. Attack him where he is unprepared, appear where you are not expected."

Management Analytics

20th century history

- Denial of services is not new
  - WW-II – degradation of German supply chain
    - Bombing of bsll bearing plants and dams
  - First computer "bug" denied service (bio caused computer)
    - Literally a moth (or some such thing) cause HW failure
  - ARPAnet intended to reduce DoS (increase availability) even under nuclear attack
    - 1974: DISN and other network protocols to reduce DoS
  - Power outages and cascade failures
    - East coast power cascade failure
    - AT&T cascade failures in telephone services
    - West coast power cascade failure
    - Dial-in denial of service to a city power supply

Management Analytics

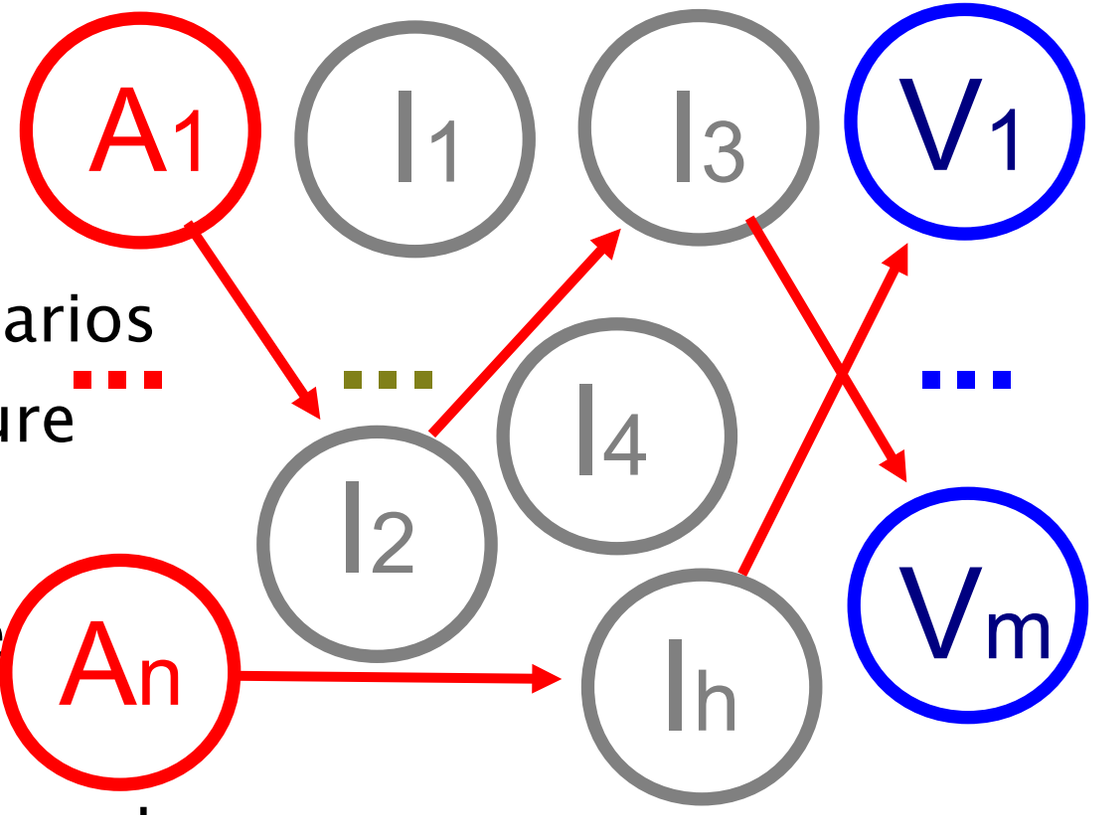
20th century history

- Denial of services is not new
  - Computer viruses as DoS
    - 1981: Xerox worm accidentally denied services
    - 1983-89: seminal virus theoretical work and experiments
    - 1988: First widespread virus (Morris worm)
  - Gulf war – degradation of Iraqi critical infrastructure
    - 1992: Defensive Information Warfare - Information Assurance
  - President's Commission / Critical Infrastructure Protection
    - 1996-2000: Critical infrastructures reviewed
      - Water, Power, Gas and Oil, Telecommunications, etc.
    - Interdependency analysis and denial of services
      - The tragedy of the commons well understood

Management Analytics

1996-2012

- A theory developed in response to a practical use
  - A distributed coordinated attack on all.net
  - A theoretical framework was developed based on a model
  - Analysis showed
    - How to track it down
    - Theoretical limits
    - Alternative attack scenarios
    - Challenges for the future
  - Mathematical analysis
    - Force on force defense
    - Move faster
    - Adaptive defenses followed



Management Analytics

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
- √ = 2008
- √ = Today

Management Analytics

1996-2012: DCAs as IW weapons

- Have these properties been realized?
  - Easily controlled (2010 – still problematic – e.g., StuxNet)
  - Pinpoint targetable (2010 – still problematic – e.g., StuxNet)
  - Effect easily measurable (2012 – obvious ones measurable)
  - Hard to trace (2012 – 3-6 months detected published)
  - Demonstrated causation (2012 – Still problematic)
  - Plausible deniability (2012 – Still feasible – but getting harder)
  - Used for deceptions (Widespread in BotNets since early 2000s)
  - Hard to selectively block (Since 1996)
  - Achieve deep penetration (Since early 2000s in BotNets)

Management Analytics

1996-2012 - Damage done?

- In IW?
  - Denial of services (Starting in the late 1990s)
  - Computational leverage (2012 - Barely realized - openly)
  - Open-loop exploits (Early 2000s in botnets)
  - Bypass defender-specific defenses (2010 StuxNet example)
  - Consume limited protective resources (Not yet as a decoy)
  - Perception management and deception (Still limited use)
    - Note that social media has emerged and memes are being used this way – technology for automating this as a for of DCA us under development
  - Stress failures of other protection and systems (Not yet)

Management Analytics

Outline

- The (recent) history of distributed coordinated attacks
- The state of distributed denial of services today
- Countermeasures
- Questions / Comments?

Management Analytics

Modern examples of DCAs for DDoS

- "StuxNet" and related industrial control systems (ICS) DCAs
  - StuxNet was the first widely publicized case vs. Iranian nuclear fuel enrichment facilities
  - Resulting in significant delays in their nuclear program
  - Initially denied by the US, but then self-attributed
  - Since then several ICS focused attacks have been undertaken by a variety of (some unknown) parties
- "Shamoon" and ARAMCO
- The 2012 attacks on US banks
- Some comments

Management Analytics

Modern examples of DCAs for DDoS

- “StuxNet” and related industrial control systems (ICS) DCAs
- "Shamoon" and ARAMCO
  - "More than 30,000 computers that it infected (at ARAMCO) were rendered useless, and had to be replaced," - (Reuters 2012-10-11)
    - … a "wiper," coded to self-execute, which replaced crucial system files with an image of a burning U.S. flag. It also overwrote all the real data on the machine with what he called garbage data.
- The 2012 attacks on US banks
- Some comments

Management Analytics

Modern examples of DCAs for DDoS

- “StuxNet” and related industrial control systems (ICS) DCAs
- "Shamoon" and ARAMCO
- The 2012 attacks on US banks
  - 2012-10-04 in a call to US Bank, they could not access their own systems or tell whether EFTs would work.
  - 2012-10-04 in a call to Wells Fargo, site was inaccessible for Internet banking – customers told to try tomorrow.
  - 2012-10-04 Chase bank – also under attack was fully accessible from Web and iPhone, and had a planned and announced outage over the weekend to update systems.
  - …
- Some comments

Management Analytics

Modern examples of DCAs for DDoS

- “StuxNet” and related industrial control systems (ICS) DCAs
- "Shamoon" and ARAMCO
- The 2012 attacks on US banks
  - "The compromised servers were outfitted with … DDoS tools that allowed the attackers to unleash network packets based on the UDP, TCP, HTTP, and HTTPS protocols. These flooded the banks' routers, servers, and server applications-layers 3, 4, and 7 of the networking stack-with junk traffic. Even when targets successfully repelled attacks against two...” - Dan Goodin 2012-10-03 arstechnica.com
  - Encryption worsened the problem...
- Some comments

Management Analytics

Modern examples of DCAs for DDoS

- "StuxNet" and related industrial control systems (ICS) DCAs
- "Shamoon" and ARAMCO
- The 2012 attacks on US banks
- Some comments
  - These are only the most obvious and well known cases
  - Similar attacks have been around for a long time
  - As we openly move toward the notion of information warfare the frequency and intensity is likely to rise
  - As we have created and continue to create high levels of interdependency on information infrastructure, it becomes the obvious focus of attack
  - DoS has long been known to create problems for encryption and other protective methods

Management Analytics

Modern capabilities for DCA/DDoS

- In addition to fully automated (viral) methods...
  - Packages using Metasploit or similar (e.g., CoreSecurity)
  - Integrated into parallel attack frameworks
  - With teams operating multiple parallel plan executions
  - Include substantial planning and execution capabilities
  - A commander can TODAY
    - Plan and order break-ins to many systems under positive control (or without it if desired)
    - Use those systems to break into other systems (reaching the transitive closure of the overall attack graph)
    - Command any/all "owned" systems to
      - Deny services to other systems/networks
      - Gather data on operational status of systems under attack
      - Shut down and/or damage/destroy/corrupt themselves

Management Analytics

Outline

- The (recent) history of distributed coordinated attacks
- The state of distributed denial of services today
- Countermeasures
- Questions / Comments?

Management Analytics

Technology issues (1996)

- Enabling technologies:
  - Still getting more of them
    - Networking / Remote execution and open access / Uncontrolled Internet / Insecure ISPs / DC programs / Trust distribution / Mobile computing / Many devices
- Prevention?
  - Disable enablers? Not likely
  - Eliminate or secure vulnerable intermediaries: Perhaps key ones
  - Private Inter-Networks: Some
  - Fault intolerance: The Commons
- Detection:
  - Detect dramatic changes in event rates - YES
  - Coordinated defenses – Yes
  - Zero tolerance detect? No
  - Better audit analysis? Yes
  - Honeynets and similar? Yes
- and Response:
  - More bandwidth/horsepower
  - Load leveling and balancing
  - Rapidly flexible addressing
  - Infrastructure adaptation
  - Multi-step access processes
  - Track-back and sever

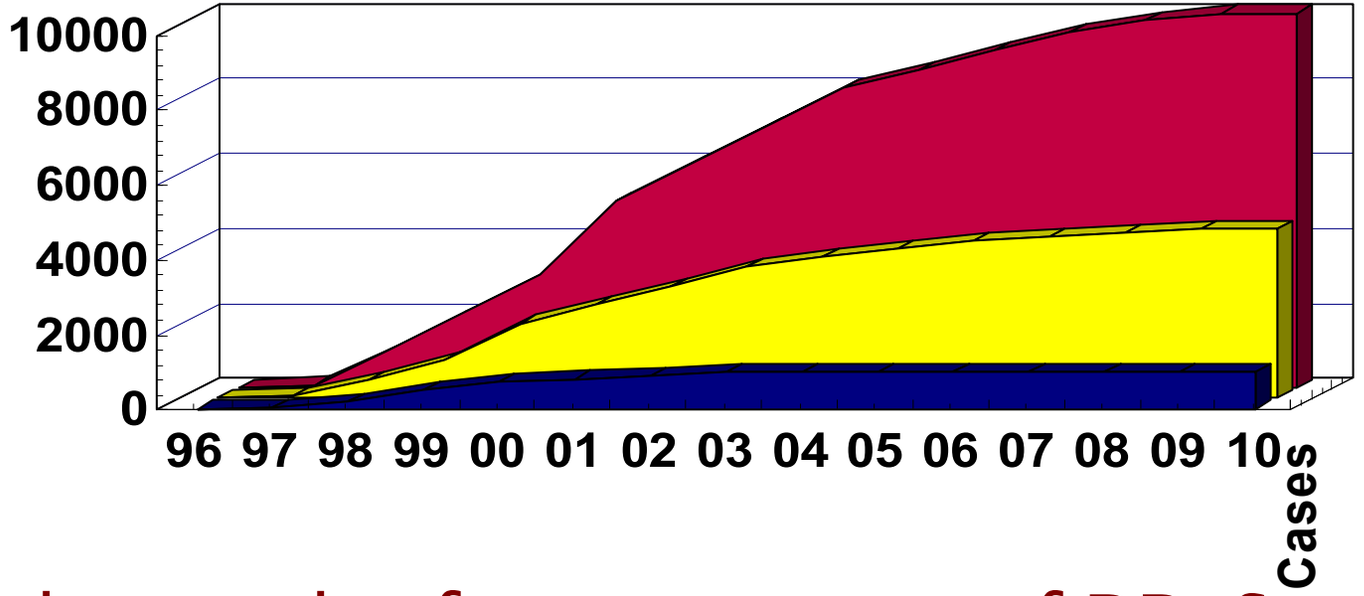
Management Analytics

Theoretical limits (1996 - today)

- Theory has not changed – identified factors remain:
  - Without strong integrity, and with increased networking, DCAs cannot be prevented from existing in the world.
    - But they can be managed as risks and kept from effecting critical infrastructure resources
  - Tracking to source quickly becomes as hard as searching the whole world - without traceability (a.k.a. source authentication) things get bad fast.
    - Some nation-states are getting very good at this
  - Networking+Vulnerabilities => DCAs
    - Rapid detection, adaptation, and response provide a managed approach to defense
- All of the critical factors are still increasing quickly

How far off was I in 1996?

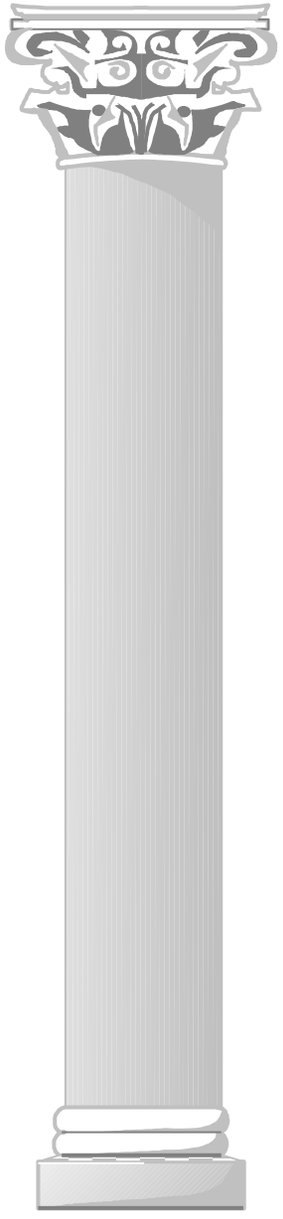
- 2008:
  - A few hundred cases per year of the use of DCAs?
  - 4,000 targets of DCAs in 2008?
  - A million intermediaries in 2008?



  - 2012:
  - Hundreds-thousands of cases per year of DDoS
  - Hundreds to thousands of large-scale target sets
  - Potentially 10 million intermediaries per instance (although)

Management Analytics

The retro slide still applies



Summary (additions)

- 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 (2008)
- An active defense industry is emerging and governments under IW and related banners will rapidly expand their uses and defenses

Management Analytics

Management / Technical Issues

- Prevention/Detection and Response
  - Eliminate or secure vulnerable intermediaries
    - Trustworthy systems in key points
    - Higher surety platforms (e.g., special purpose systems, bootable CD platforms, remote terminal servers, etc.)
  - Private Inter-Networks
    - DoD has a fully private (physically separated) network
  - Fault intolerance
    - Build adequate bandwidth / capacity to handle full load
- Critical infrastructures and enterprises CAN do this
- But management is going the opposite direction
- Trading off increased efficiency for decreased effectiveness

Management Analytics

Management / Technical Issues

- Prevention/Detection and Response
  - Detect dramatic changes in event rates
    - Widely done today at many levels (behavioral anomaly)
  - Coordinated defenses
    - Limited capabilities are available today – some emerging
  - Zero tolerance detection
    - Limited by unwillingness to characterize and lock down
  - Better audit analysis
    - Limited utility in DDoS today – rapid response too slow
  - Deception methodologies
    - Limited by management perception of challenges
    - Technology not pushed till recently (social issues)

Management Analytics

Management / Technical Issues

- Prevention/Detection and Response
  - More bandwidth/horsepower
    - But this reduces the financial advantage of the commons
    - Most management is not interested in spending on this
  - Load leveling and balancing
    - Used to a limited extent largely locally
    - Some regional / global services emerging
  - Rapidly flexible addressing
    - Not widely adopted and marginal technology today
    - Integrated with load-level and balancing when used
    - Risky for management to adopt as a strategy today

Management Analytics

Management / Technical Issues

- Prevention/Detection and Response
  - Infrastructure adaptation
    - Ultimately, we need to rearchitect infrastructures to deal with this set of attack methodologies
    - Management has been hesitant to pay the price of this adaptation without a clear understanding of benefits
  - Multi-step access processes
    - Multiple step access different infrastructure elements, you don't know the next till you get past the last, and sequences change over time and circumstance
    - Technology for this is not well applied see advertising
  - Track-back and sever (soft or hard)
    - Microsoft has tried this (soft) with some success
    - Only really works on fixed assets of attacks (or attackers)

Management Analytics

Outline

- The (recent) history of distributed coordinated attacks
- The state of distributed denial of services today
- Countermeasures
- Questions / Comments?

Management Analytics

Thank You

http://all.net/ - fc at all.net