

# What's Happening in DNS Security?

Ed Lewis

APTLD in Manila

February 23, 2009

# Abstract

- The security (plus stability and resiliency) of the Domain Name System is once again a hot topic
- DNSSEC is one tool for securing DNS that is getting a lot of attention these days
- But DNSSEC is just one tool, it treats one of the major vulnerabilities
  - There are others to watch

# Structure of the talk

- Security is naturally a reactive science
- The various attacks must be understood and separated from each other
  - Divide and Conquer
- In this presentation, after a few slides on attacks, slides on the treatments and other events coming this week at APTLD/APRICOT Manila

# DNS Weak Points

- Provisioning (or registration) system "games"
- Cache Poisoning
- Denial of Service / Distributed Denial of Service
  - Packet floods
  - Reflective attacks
  - Amplification attacks

# Provisioning Games

- **Goal:** to hide the true identity of the owner of a domain name
- **Reason:** to cover other malicious activity using the domain name
- **How:** Stolen credit cards, stealing registration passwords via phishing, convincing a domain registration entity to lower security standards

# Cache Poisoning

- **Goal:** Putting misleading data into a mid-network DNS server (Cache)
- **Reason:** To direct clients to wrong addresses, e.g., a phishing site.
- **How:** Cache is fooled with a forged answer
  - This path seemed closed but was "re-opened" last summer via a new technique which is now exploited (attempted) regularly.

# (Distributed) Denial of Service

- A class of attacks rooted on the use of the User Datagram Protocol as a sub-element of the DNS
  - Packet Floods
  - Reflective Attacks
  - Amplification Attacks

# Packet Floods

- **Goal:** To prevent other packets from traveling to and from a network element
- **Reason:** To eliminate a legitimate service
- **How:** For "DoS" a source emits packets, for "DDoS" many sources emit packets, usually with false source addresses towards the target
  - In a DDoS, the attack may not be noticed other than at the targeted victim's site

# Reflective Attacks

- **Goal:** Send a packet to a name server to get it to reply to some other address
- **Reason:** Gives the appearance that the name server is the source of the attack
- **How:** Falsified source address. An attacker at address Z sends "Query from X to Y" and name server replies "Response from Y to X", sent to X (not Z). X is the "victim."

# Amplification Attacks

- **Goal:** Use the DNS to supply more bytes than the attacker sends
- **Reason:** Knock off a legitimate service
- **How:** Same as reflective attack but the response sent by the name server to X has more bytes than the query sent by Z (the attacker)
  - This attack "rides" on top of a reflective attack

# Treatments

- (Repeating) The taxonomy of attacks are
  - Provisioning/Registration
  - Cache Poisoning
  - Denial of Service
    - Packet Flood
    - Reflective
    - Amplification

# Provisioning/Registration

- Registration protocols on secure transport are important and do one part of the job
- But there is a human operator element
  - Procedures have to be strong and followed
  - "Please make a change, buddy" has to be denied
- Recent attack on this followed a phishing attack where credentials were presumably stolen

# Cache Poisoning

- DNSSEC
- APRICOT has a DNSSEC track on February 25<sup>th</sup>
- In short, DNSSEC is getting more deployment attention since the vulnerability was described by Dan Kaminsky last summer but DNSSEC still needs time to deploy
- Many server operators haven't heeded calls to "update, update, update" software

# Packet Floods

- The nature of UDP, the common reply to this is "BCP 38!"
  - A "Best Common Practice" that ISPs should follow, they should drop all packets leaving their network with a source address that is obviously false
- Active, reactionary defenses including dropping traffic from/to attacking nodes, firewall rules, packet scrubbers

# Reflective Attacks

- First these need to be detected. Usually a community or industry-wide effort because attacker may use many intermediate name servers and focus all false source to a particular victim.
- There's little about DNS that can be changed, the attacker is exploiting permissive UDP routing (source address) and firewalls allowing essential DNS traffic through

# Amplification Attacks

- Recent attack used the fact that BIND and other servers will respond to a "lame query" with a referral to the root. The response is an order of magnitude larger than the query, benefitting the attacker
- Preventing the use of the root referral in response to a lame query
  - <https://www.dns-oarc.net/oarc/articles/upward-referrals-considered-harmful>

# A note about the (D)DoS

- The technical root cause is reliance on UDP
  - But UDP is essential to the DNS "mission"
- DNS is (pretty much) unique among protocols because it is global and uses UDP
  - Many global protocols (HTTP, SSH, VPN) use TCP
  - Many UDP using protocols are local use
- These facts are the reason the DoS-class problems persist (but there are treatments)

# A recent event

- Global DNS Security, Stability, and Resiliency Symposium
  - February 3 & 4, 2009, at Georgia Tech Univ. (US)
  - <http://www.gtisc.gatech.edu/icann09.html>
- Further evidence of the growing concern about DNS Security
  - Starting with DNSSEC
  - Continuing into all other areas

# End of Slide marker

- That's the end of this presentation's material
- Chair, what's next? ;)