Transaction oriented DNS flow analysis (WIP)

Shigeya Suzuki / Bill Manning
WIDE Project
USC/ISI & Keio University + Auto-ID Labs Japan

CAIDA Workshop 2006 @ISI, March 17th 2006

Topics

- Current on-going work @ISI
- DNS Flow profile
- Strategy and Tools
- Applicability to Amplifier Attack

Current on going works

(1) ONS (Object Naming System) over DNSSec
(2) DNSSec Operational Considerations
(3) Considerations on autonomous operations
    - Name decoupling from external authority
    - Friend/Foe determination
    - (Packet origination check)
(4) Traffic analysis on some of heavily loaded DNS servers
(5) DNS Cache effectiveness
(6) (... and little more not related to DNS)

Current on going works

(1) ONS (Object Naming System) over DNSSec
(2) DNSSec Operational Considerations
(3) Considerations on autonomous operations
    - Name decoupling from external authority
    - Friend/Foe determination
    - (Packet origination check)
(4) Traffic analysis on some of heavily loaded DNS servers
(5) DNS Cache effectiveness
(6) (... and little more not related to DNS)

Transaction oriented DNS flow analysis

- Intent to see what's happening in transaction/session oriented view
- Want to see how change of profile (protocol or anomalies) cause:
  - Resource consumption
  - Response delay
  - Or other properties

Example: DNS Cache Effectiveness

- Take dump of the traffic of the server of interest
- Extract transaction in the packet flow
- Co-relate these transaction into sessions
  - Possibly fill in gaps, which created by "cache hit"
- Compare "real" sessions and "cache-less" sessions and see which part of the RR caching is effective or not, etc.

Example: Estimation of effects of DNSSec Deployment

- Take dump of the traffic of the server of interest
- Extract transaction in the packet flow
- Co-relate these transaction into sessions
  - Possibly fill in gaps, which created by "cache hit"
- Insert extra DNSSec transactions as necessary
- Modify(fallback) to EDNS0, if necessary
- Compare "current" sessions and "DNSSec-aware" sessions and see how they're different

So... I need tools!
- Design Guideline -

- Use "pcap" as data source
- Possibly run 'on the fly' basis
- Analyze large amount of data in relatively short amount of time
- Build as a framework: create set of classes to
  - handle packets/frames/flow
  - find and relate transactions/sessions
  - "pcap" file and device bridge
  - .. and other utilities
- Possibly store part of information to SQL database or data mining oriented DBs for analysis

Current version

- Implemented in C++, for better performance
  - 7.9mil packets, 80sec @CoreDuo 2.0G
- Accept dump files, but designed to accept live pcap feeds
- On memory data only, with "light" abstraction layer
- Set of classes for packet/frames

- Not a command line tool. Just set of libraries

DNS Flow profile differences

- What's the difference between:
  A. "Normal" DNS flow
  B. "Well behaved" DNSSec flow
  C. Flow under some type of attack like Amplifier attack
- How we can distinguish B and C?

"Normal" DNS Flow

- Request Packet
  - Question to Ask
- Reply Packet
  - Question, Answer, Auth section, Additional Section
- Amount of flow in each direction is very similar

"Well Behaved" DNSSec Flow

- Request Packet
  - Question to ask
- Reply Packet
  - Question, Answer, Auth, Additional
  - Auth and Additional will contain DNSSec specific RRs such as RRSIG, NSEC, DS,

- Amount of data replied is a lot bigger
- If zone manager installed extra keys. it will cost more too
- signature lifetime/TTL affect situation too

Amplifier Attack Flow

- Request Packet
  - Question to Ask
- Reply Packets
  - Question, Answer, Auth section, Additional Section
- Amount of data replied is a lot bigger

Amplifier Attack

A. Set-up authoritative server with a zone which have a label with several long data (like TXT)
B. Find some recursive resolver
C. Find a victim
D. Send a query of the label made ready in (A) with ANY type request, to servers (B) above, with spoofed packet look like request from a victim (C)

- At most, x73 amplification performance. Some of these attack cause 10Gbps traffic.

http://www.us-cert.gov/reading_room/DNS-recursion121605.pdf

DNS flow profiling meaningful?

- Possibly, Yes
  - Operators want to know the trend of change from, for example, traffic engineering point of view
  - Core DNS server operators may have benefit from this

Extra topic:
How we can find Open Recursive Server?

- We need to find way to mitigate effect of amplifier attack - need to way to find Open Recursive Server
- Active
  - Send a query, check RA on or not
- Passive
  - Traffic analysis
  - Data analysis (RA flag, etc.)
- Unfortunately, all of these are incomplete

Next Steps

- We have a few set of DNS traffic dump in different characteristics. Apply the tool to these data to:
  - understand how DNS cache is effective
  - how deployment of DNSSec affect flow
  - Paper or report will be ready before summertime
- Plan to continuously improve this tool, and make them available publicly, possibly during FY2006