Monitoring cache poisoning attacks

2008 OARC Workshop

Tsuyoshi TOYONO and Keisuke ISHIBASHI
NTT

Outline

- Motivation
- Issues on caching servers
- Monitoring tool: Methodology
- Monitoring results
- Data refinement
- Alert results
- Conclusion

Motivation

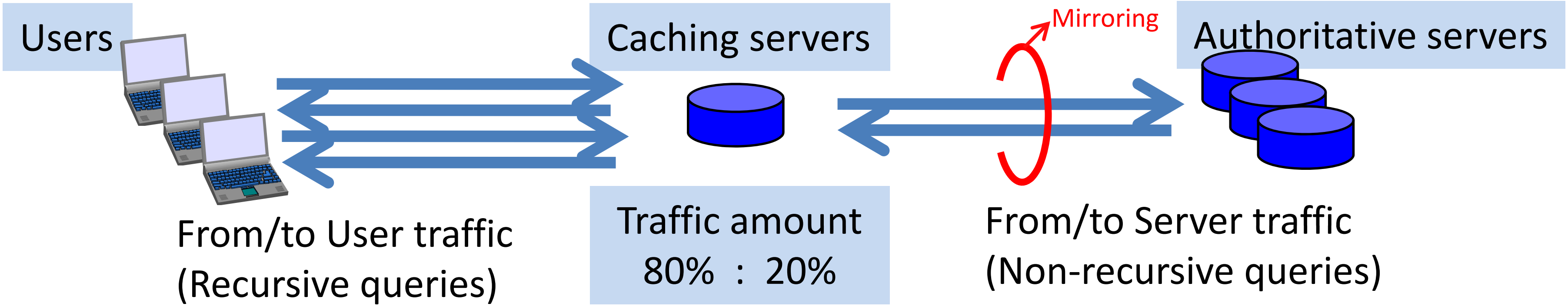
- Monitoring system of cache poisoning attack on caching server are required
  - Dan Kaminsky's attacks had been reported in July
- Real-time monitoring and alert system are required
- Monitoring tools shouldn't impact on performance of caching servers
  - It shouldn't impact customers usability
- It is important to monitor poisoning attacks on caching servers even if patches were applied

Issues on caching servers

- Large-scale caching servers are used by several million users
  - These servers handle tens of thousands of queries per second
- It’s difficult to capture full traffic and monitor in real-time due to huge amount of traffic

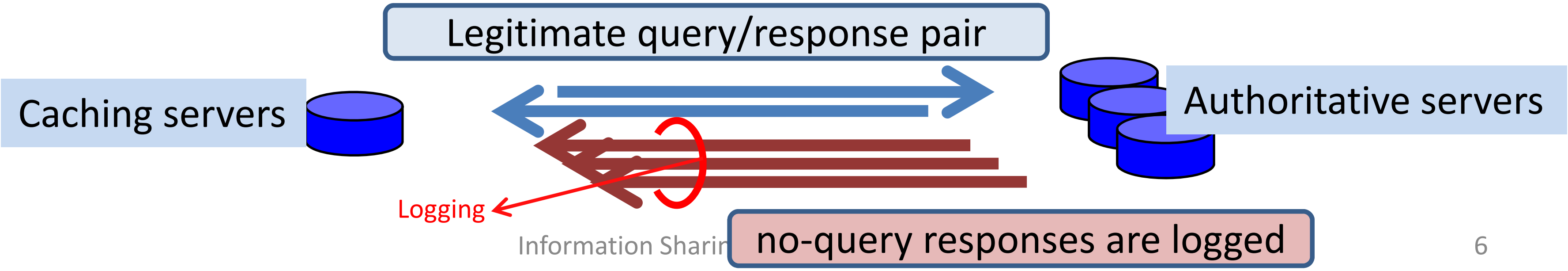
Our monitoring tool

- Concept: Simple and Light-weight
  - Monitoring “no-query” responses
    - If server is attacked, it will increase number of no-query responses
- Monitoring data
  - We use port mirroring and capture only server traffic on caching servers
    - Port mirroring does not affect actual server performance
    - It can merge multiple caching servers’ traffic

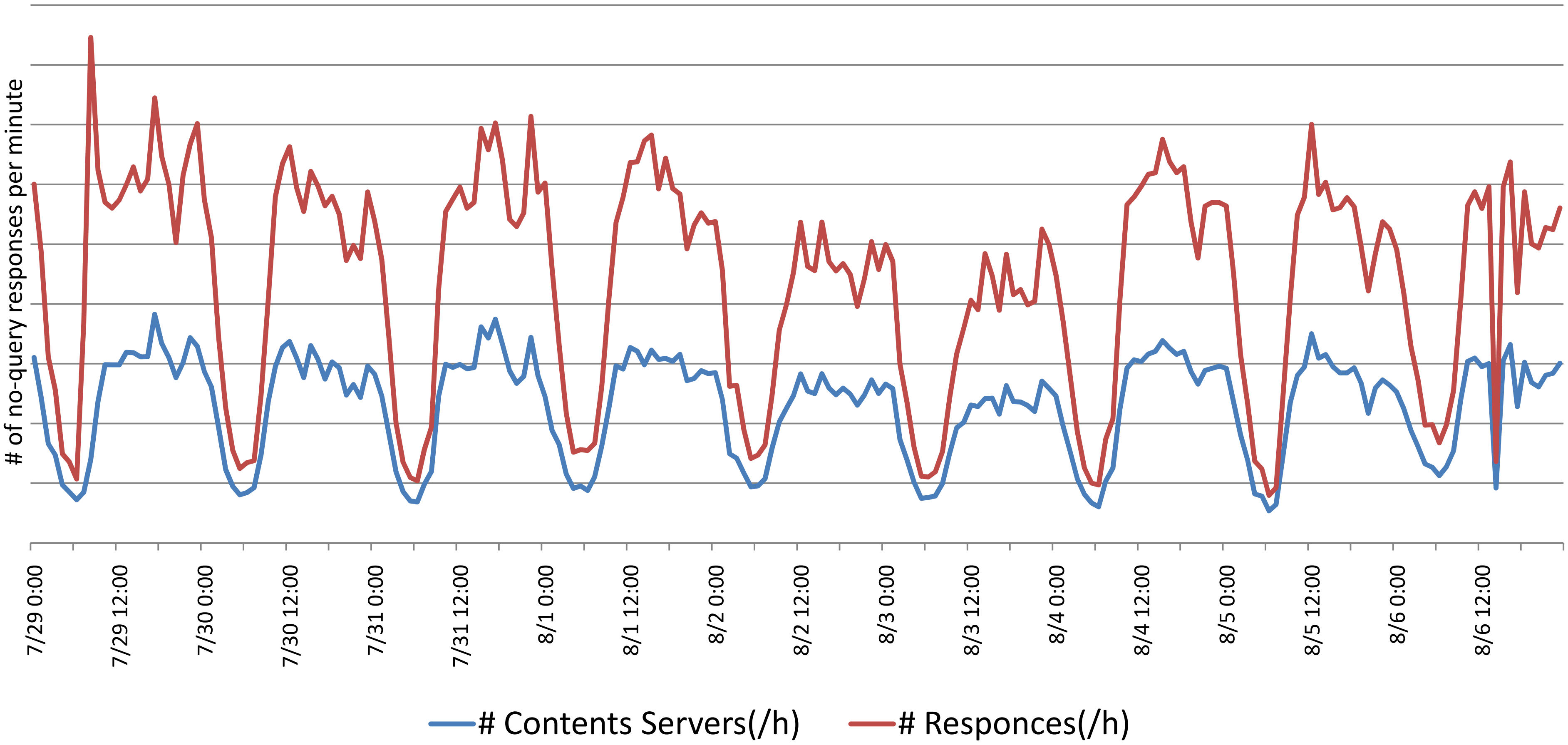


Methodology

- Monitoring no-query responses from authoritative servers
  - Query-response pair by checking 5-tuple matches in the past 2 minutes
    - {Src, Dest} IP address, {Src, Dest} Port, TXID(DNS Transaction ID)
  - Using "bloom filter"
    - Bloom filter checks existence of query/response pair using only a few bits
    - Light computational load, less memory used
- If a response don't match any query, it's a no-query response
- All no-query responses are detected and logged



Number of no-query responses



- No-query response time series are similar to those of all user traffic
- Caching servers received no-query responses constantly

Monitoring results

- Caching servers received no-query responses constantly
  - If server is attacked, it will increase the number of no-query responses rapidly
  - Our servers have not been attacked yet

- What are these constant no-query responses?
- Close analysis of details of these responses

List of most no-query responses (Number of detection times)

	# of detection times	Server IP	Server Name	Whois result
1	2586 times	202.96.128.143	ns.guangzhou.gd.cn.	
2	2080 times	192.35.51.30	f.gtld-servers.net.	
3	1815 times	69.25.142.42	dns1.name-services.com.	
4	1574 times	192.41.219.11		NTT America, Inc.
5	1183 times	59.106.82.158		SAKURA Internet Inc.
6	1048 times	192.55.83.30	m.gtld-servers.net.	
7	1038 times	207.199.88.179	ns1.bindhost.net.	
8	1018 times	202.122.112.54		Shanghai Bennalong Network Technology Co.,LTD
9	1015 times	207.241.145.25	nydns2.about.com.	
10	940 times	207.241.145.24	nydns1.about.com.	

- Number of detections for 2 weeks
- Counting servers which sent no-query responses one or more times

List of most no-query responses (Number of responses/minute)

	Number of responses/min	Server IP	Server Name	Whois result
1	320 resps/min	202.101.103.54	dns2.xm.fj.cn.	
2	212 resps/min	64.56.191.105		International Digital Communications, Inc.
3	207 resps/min	64.56.191.104		International Digital Communications, Inc.
4	157 resps/min	202.96.128.143	ns.guangzhou.gd.cn.	
5	75 resps/min	70.86.196.66	nf3.no-ip.com.	
6	60 resps/min	64.34.166.157	server1.copleymotorcars.com.	
7	53 resps/min	133.176.220.31	rtprogw.rtpro.yamaha.co.jp.	
8	41 resps/min	211.133.249.144	pc1.netvolante.jp.	
9	31 resps/min	89.104.112.10		ALPHA-TELECOM
10	30 resps/min	203.81.56.74		BIZWEBASIA PTE LTD

- Servers sorted by the maximum number of no-query responses/minute

No-query responses (1/3)

- “ns.guangzhou.gd.cn.”
  - This authoritative server ALWAYS sends more than one responses per query

- 202.***.***.143 sent 5 responce[s]
  - qd: 1 an: 1 ns: 1 ar: 1
  - qname: 220.***.***.218.in-addr.arpa. qtype: 12
  - rname: dns.guangzhou.gd.cn. rtype: 1 ttl: 86400 rdata: 202.***.***.68

- A bug of some load balancer or L4 switch appliances ?

No-query responses (2/3)

- “f.gtld-servers.net.”
  - If the response packet have no “answer section” (no err/answer 0), this authoritative server sometimes sends two or three responses

- 192.**.**.30 sent 1 responce[s]
  - qd: 1 an: 0 ns: 2 ar: 2
  - qname: www.just***.com. qtype: 1
  - rname: ns13.***.com. rtype: 1 ttl: 172800 rdata: 64.***.***.117
  - rname: ns14.***.com. rtype: 1 ttl: 172800 rdata: 208.***.***.7
- 192.**.**.30 sent 2 responce[s]
  - qd: 1 an: 0 ns: 2 ar: 2
  - qname: ***corp.com. qtype: 15
  - rname: sedns.***.com. rtype: 1 ttl: 172800 rdata: 159.***.***.89
  - rname: swdns.***.com. rtype: 1 ttl: 172800 rdata: 159.***.***.89

No-query responses (3/3)

- “dns2.xm.fj.cn.”
  - This authoritative server sometimes sends large number of responses within a short time, but not continuously

- 202.***.***.54 sent 320 responce[s]
  - qd: 1 an: 1 ns: 2 ar: 2
  - qname: 198.***.***.202.in-addr.arpa. qtype: 12
  - rname: dns.xm.fj.cn. rtype: 1 ttl: 86400 rdata: 202. ***. ***.55
  - rname: dns2.xm.fj.cn. rtype: 1 ttl: 86400 rdata: 202. ***. ***.54
- 202.***.***.54 sent 319 responce[s]
  - qd: 1 an: 1 ns: 3 ar: 3
  - qname: dns.xm.fj.cn. qtype: 1
  - rname: xm.fj.cn. rtype: 1 ttl: 86400 rdata: 202. ***.***.55
  - rname: dns2.xm.fj.cn. rtype: 1 ttl: 86400 rdata: 202. ***. ***.54

  - A bug of some DNS software?

Alert system

- We have to refine monitoring logs to pick poisoning attacks
  - Caching servers received no-query answers constantly

- Refinement
  - The number of responses per second
  - The number of TXIDs
  - The number of QNAMEs
  - The number of Additional “A” or “AAAA” records

Data refinement for alert (1/2)

- The number of responses per second
  - Poisoning attack responses will be received within a short time
    - Need to reach caching server before RTT between caching server and legitimate authoritative server
  - [Running] We check whether or not the number of responses per second is over the fixed threshold
    - (ex) Most rapid server sent 320 responses per minute, but it not seemed to be an attack (only 5 responses per second)

Data refinement for alert (2/2)

- The number of TXIDs
  - if responses have same additional record but many different TXIDs, it seems to be an attack.
- The number of QNAMEs
  - If responses have many different QNAMEs of same domain suffix and these are NXDOMAINs, it may be an attack.
- The number of additional “A” (or “AAAA”) records
  - If responses have multiple additional “A” records for same NS, it seems to be an attack.
    - Of course there are cases such as DNS round robin

Alert results

- Results of 2 months monitoring
  - The number of alert which is over the threshold of no-query responses per second
    - Only 3 times
  - Maximum no-query responses from one server
    - 51,735 responses/day (= 0.6 responses per second)

Future work

- Detecting low-rate long-term attacks
  - this system can’t alert long-term attacks which have low-rate responses per second
    - monitoring tool already logs, but difficult to find from large logs
    - Probably we can detect such attacks by using QNAME checking and Additional “A” record checking

Conclusion

- We introduce cache poisoning monitoring system on caching server
  - It can apply to large-scale DNS traffic
- Our servers have not been attacked yet.
- However, caching servers received no-query responses constantly
  - seems to be some bug of load balancing hardware or DNS software
- It is important to monitor such attacks on caching servers even if patches were applied