DNS
How Simple Things Can Go Wrong

April 16, 2018

Davide Papini

Elettronica S.p.a.

ABOUT ME

- Research & Innovation **@Elettronica S.p.a.**
- Postdoc **@ISG Royal Holloway, UK** on ML applied to cyber situational awareness.
- Ph.D. **@Danmarks Tekniske Universitet**:
  - → "Attacker Modeling in Ubiquitous Computing Systems"
  - → External stay at **COSIC, KU Leuven**
- M.Sc. Telecommunication Engineering **@Politecnico di Milano**:
  - → Erasmus **@Danmarks Tekniske Universitet**
  - → Master Thesis on "Anomaly Based Wireless Intrusion Detection Systems"

AGENDA

- What is DNS
- DNS attacks
- Botnets and DNS

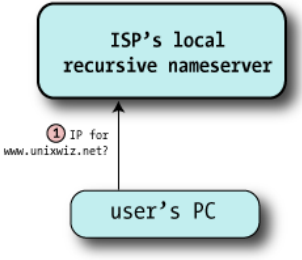
DOMAIN NAME SYSTEM

DOMAIN NAME SYSTEM (DNS)

Essential infrastructure for the Internet.

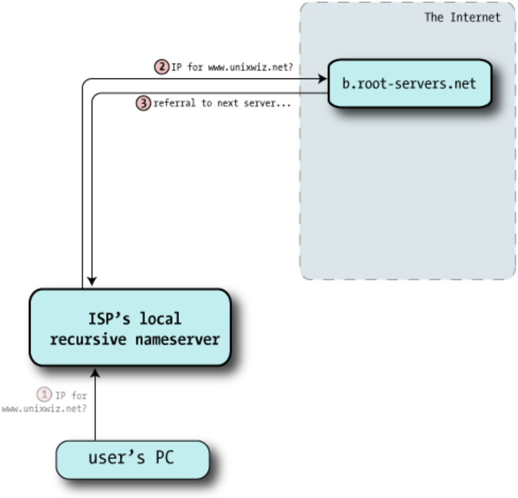
- Maps host names to IP addresses
  → and vice versa.
- Originally designed for a friendly environment;
  → hence only basic authentication mechanisms.
- Some serious attacks reported in recent years.
- We will look at those attacks and at available countermeasures.

HOW DOES IT WORK



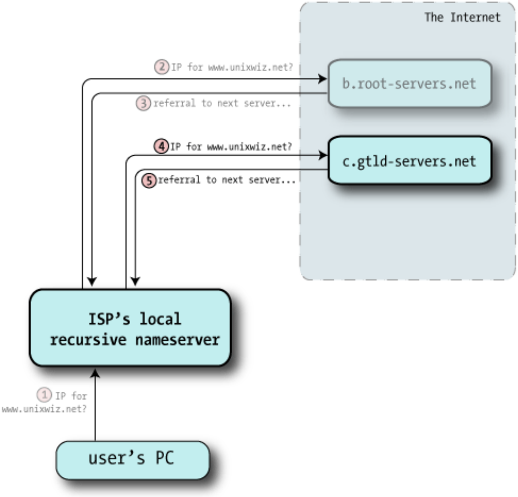
Courtesy of http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html

HOW DOES IT WORK


The Internet
2 IP for www.unixwiz.net?
b.root-servers.net
3 referral to next server...
ISP's local recursive nameserver
1 IP for www.unixwiz.net?
user's PC

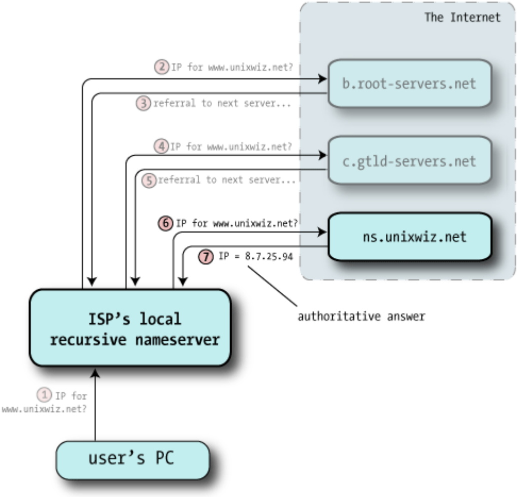
Courtesy of http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html

HOW DOES IT WORK


The Internet
b.root-servers.net
c.gtld-servers.net
2 IP for www.unixwiz.net?
3 referral to next server...
4 IP for www.unixwiz.net?
5 referral to next server...
ISP's local recursive nameserver
1 IP for www.unixwiz.net?
user's PC

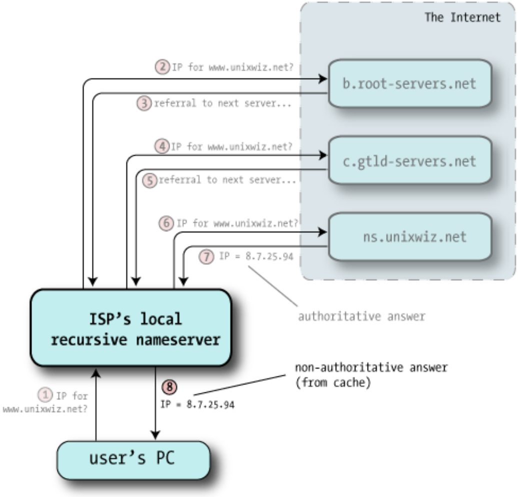
Courtesy of http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html

HOW DOES IT WORK


The Internet
b.root-servers.net
c.gtld-servers.net
ns.unixwiz.net
ISP's local recursive nameserver
user's PC
1 IP for www.unixwiz.net?
2 IP for www.unixwiz.net?
3 referral to next server...
4 IP for www.unixwiz.net?
5 referral to next server...
6 IP for www.unixwiz.net?
7 IP = 8.7.25.94
authoritative answer

Courtesy of http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html

HOW DOES IT WORK


The Internet
b.root-servers.net
c.gtld-servers.net
ns.unixwiz.net
2 IP for www.unixwiz.net?
3 referral to next server...
4 IP for www.unixwiz.net?
5 referral to next server...
6 IP for www.unixwiz.net?
7 IP = 8.7.25.94
authoritative answer
ISP's local recursive nameserver
non-authoritative answer (from cache)
1 IP for www.unixwiz.net?
8 IP = 8.7.25.94
user's PC

Courtesy of http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html

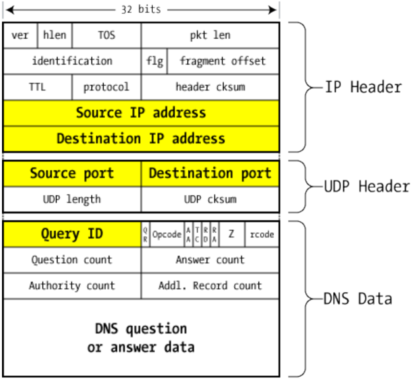
DOMAIN NAME SYSTEM (DNS)

- Distributed directory service for domain names (host names) used for:
  - → look up IP address for host name, host name for IP address.
  - → anti-spam: Sender Policy Framework uses DNS records.
  - → basis for same origin policies applied by web browsers.
- Various types of resource records e.g. A, AAA, NS, MX, CNAME.
- Host names and IP addresses collected in zones managed by authoritative name servers.

DNS INFRASTRUCTURE

- 13 root servers; all name servers configured with the IP addresses of these root servers.
- Global Top Level Domain (GTLD) servers for top level domains: .com, .net, .cn, ...
  - → Can be more than one GTLD server per TLD.
  - → Root servers know about GTLD servers.
- Authoritative name servers provide mapping between host names and IP addresses for their zone.
  - → GTLD servers know authoritative name servers in their TLD.
- Recursive name servers pass client requests on to other name servers and cache answers received.

DNS PACKET



32 bits

ver | hlen | TOS | pkt len

identification | flg | fragment offset

TTL | protocol | header cksum

Source IP address

Destination IP address

IP Header

Source port | Destination port

UDP length | UDP cksum

UDP Header

Query ID | QR | Opcode | AA | TC | RD | RA | Z | rcode

Question count | Answer count

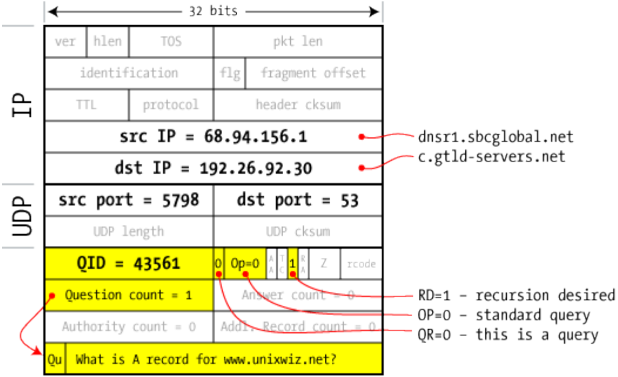
Authority count | Addl. Record count

DNS question
or answer data

DNS Data

DNS packet on the wire

DNS PACKET: QUERY & RESPONSE



32 bits

IP

ver | hlen | TOS | pkt len

identification | flg | fragment offset

TTL | protocol | header cksum

src IP = 68.94.156.1

dst IP = 192.26.92.30

UDP

src port = 5798 | dst port = 53

UDP length | UDP cksum

QID = 43561 | 0 | Op=0 | AA | TC | 1 | RA | Z | rcode

Question count = 1 | Answer count = 0

Authority count = 0 | Addl. Record count = 0

Qu | What is A record for www.unixwiz.net?

dnsr1.sbcglobal.net

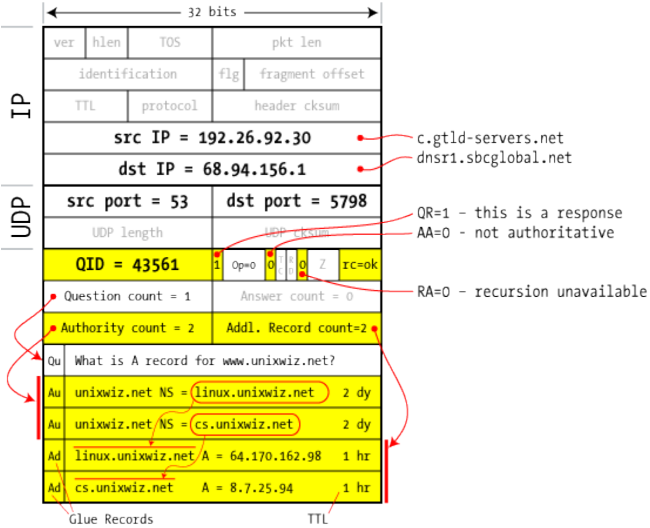
c.gtld-servers.net

RD=1 – recursion desired

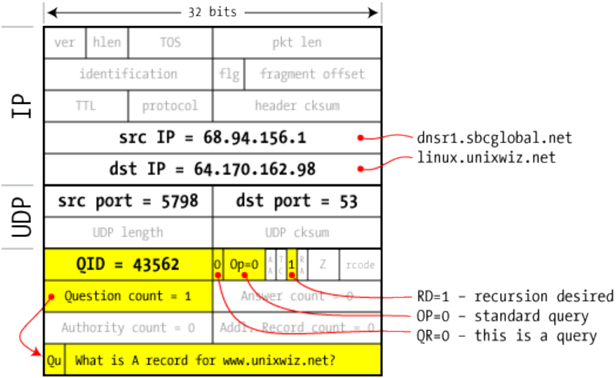
OP=0 – standard query

QR=0 – this is a query

DNS PACKET: QUERY & RESPONSE



DNS PACKET: QUERY & RESPONSE



32 bits

IP

ver | hlen | TOS | pkt len

identification | flg | fragment offset

TTL | protocol | header cksum

src IP = 68.94.156.1

dst IP = 64.170.162.98

UDP

src port = 5798 | dst port = 53

UDP length | UDP cksum

QID = 43562 | 0 | Op=0 | AA | TC | 1 | RA | Z | rcode

Question count = 1 | Answer count = 0

Authority count = 0 | Addl. Record count = 0

Qu | What is A record for www.unixwiz.net?

dnsr1.sbcglobal.net

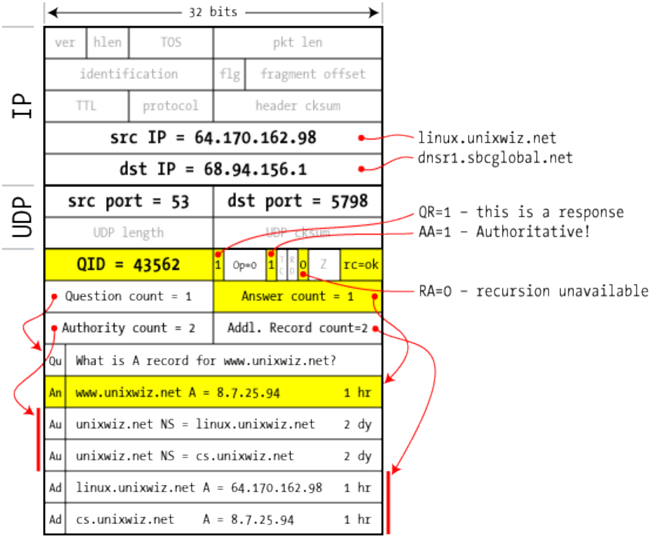
linux.unixwiz.net

RD=1 – recursion desired

OP=0 – standard query

QR=0 – this is a query

DNS PACKET: QUERY & RESPONSE



32 bits

IP

ver | hlen | TOS | pkt len

identification | flg | fragment offset

TTL | protocol | header cksum

src IP = 64.170.162.98

dst IP = 68.94.156.1

UDP

src port = 53 | dst port = 5798

UDP length | UDP cksum

QID = 43562 | 1 | Op=0 | 1 | TC | RD | 0 | Z | rc=ok

Question count = 1 | Answer count = 1

Authority count = 2 | Addl. Record count=2

Qu What is A record for www.unixwiz.net?

An www.unixwiz.net A = 8.7.25.94 1 hr

Au unixwiz.net NS = linux.unixwiz.net 2 dy

Au unixwiz.net NS = cs.unixwiz.net 2 dy

Ad linux.unixwiz.net A = 64.170.162.98 1 hr

Ad cs.unixwiz.net A = 8.7.25.94 1 hr

linux.unixwiz.net

dnsr1.sbcglobal.net

QR=1 - this is a response

AA=1 - Authoritative!

RA=0 - recursion unavailable

IP ADDRESS LOOKUP – SIMPLIFIED

1. Client sends request to its local recursive name server asking to resolve a host name (target).
2. Recursive name server refers request to one of the root servers.
3. Root server returns list of GTLD servers for the target's TLD; also sends glue records that give the IP addresses of those servers.
4. Recursive name server refers request to one of the GTLD servers.
5. GTLD server returns list of authoritative name servers for the target's domain, together with their IP addresses (glue records).

IP ADDRESS LOOKUP – SIMPLIFIED

6. Local recursive name server refers the request to one of the authoritative name servers.
7. Authoritative name server provides authoritative answer with IP address to local name server.
8. Local recursive name server sends answer to client.

CACHE & TIME-TO-LIVE

Simplified description left out an important aspect.

- Performance optimisation: when name server receives an answer, it stores answer in its cache.
- When receiving a request, name server first checks whether answer is already in its cache; if this is the case, the cached answer is given.
- Answer remains in cache until it expires; time-to-live (TTL) of answer is set by server.

What are the security implications of higher/lower TTL? Is it ok to trust the server?

E.g.: Long TTL = high security, low TTL = low security?

LIGHT-WEIGHT AUTHENTICATION

- Messages on Internet cannot be intercepted; attacker can only read messages forwarded to her.
- Anybody can pretend to be an authoritative name server for any zone.
- How does a recursive name server know that it has received a reply from an authoritative name server?
- Recursive name server includes a 16-bit query ID (QID) in its requests.
- Responding name server copies QID into its answer; applies also to answer from authoritative name server.
- Recursive name server caches first answer for a given QID and host name; then discards this QID.
- Drops answers that do not match an active QID.

AUTHENTICATION -- SECURITY?

- If query is not passed by mistake to the attacker, her chance to generate a valid fake answer is 2^{-16}.
- If

  → root servers entries at the local name server are correct,
  → routing tables in the root servers are correct,
  → routing tables in the GTLD servers are correct,
  → cache entries at recursive name server are correct,

  then the attacker will not see original query ID.
- Security relies on the assumption that routing from local recursive name server to authoritative name server is correct.
- Attack method: guess QID to subvert cache entries.

DNS CACHE ATTACKS

COMPROMISING AUTHENTICATION

- If routing to and from root servers and GTLD servers cannot be compromised, the attacker can only try to improve her chances of guessing a query ID.
- Some (earlier) versions of BIND used a counter to generate the QID.
- Cache poisoning attack.
  1. Ask recursive name server to resolve host name in attacker's domain.
  2. Request to attacker's name server contains current QID.
  3. Ask recursive name server to resolve host name you want to take over; send answer that includes next QID and maps host name to your chosen IP address.
  4. If your answer arrives before the authoritative answer, your value will be cached; the correct answer is dropped.

PREDICTABLE CHALLENGES

If you want to perform authentication without cryptography, do not use predictable challenges.

- More ways of improving the attack's chances:
  - → To account for other queries to the recursive name server concurrent to the attack, send answers with multiple QIDs within a certain range.
  - → To increase the chance that fake answer arrives before authoritative answer, slow down authoritative name server with a DoS attack.
  - → To prevent a new query for the host name restoring the correct binding, set a long time to live.

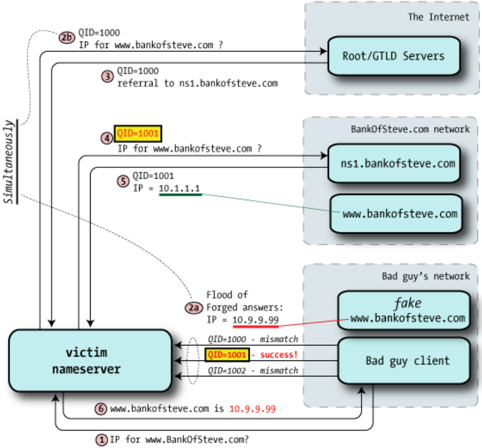
BAILIWICK CHECKING

- Performance optimization: name servers send additional resource records to recursive name server, just in case they might come useful.
- Might save round trips during future name resolution.
- Works fine if all name servers are well behaved.
- Do not trust your inputs: malicious name server might provide resource records for other domains, e.g. with IP addresses of its choice.
- Bailiwick checking: additional resource records not coming from the queried domain, i.e. records "out of bailiwick", not accepted by recursive name server.

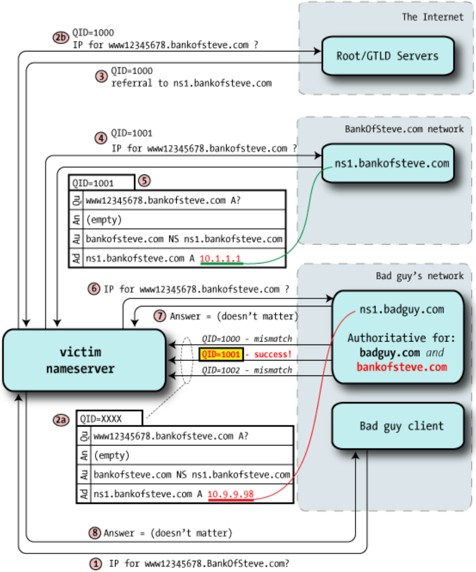
DNS ATTACK – NEXT TRY

- Attacker is in a race with authoritative name server.
- If authoritative answer arrives first, the attacker's next attempt has to wait until TTL expires.
- But attacker does not ask for www.foo.com but for a host random.foo.com that is not in recursive name server's cache; triggers a new name resolution request.
  - → Defeats TTL as a measure to slow down attacker;
  - → TTL not intended as a security mechanism!
- Authoritative name server for foo.com unlikely to have entry for random.foo.com.
- Returns an NXDOMAIN answer indicating that host doesn't exist.

DNS SIMPLE CACHE POISON



DAN KAMINSKY'S ATTACK (2008)



The Internet

Root/GTLD Servers

BankOfSteve.com network

ns1.bankofsteve.com

Bad guy's network

ns1.badguy.com

Authoritative for:
badguy.com *and*
bankofsteve.com

Bad guy client

victim
nameserver

① IP for www12345678.BankOfSteve.com?

2a

QID=XXXX	
Qu	www12345678.bankofsteve.com A?
An	(empty)
Au	bankofsteve.com NS ns1.bankofsteve.com
Ad	ns1.bankofsteve.com A 10.9.9.98

2b QID=1000
IP for www12345678.bankofsteve.com ?

③ QID=1000
referral to ns1.bankofsteve.com

④ QID=1001
IP for www12345678.bankofsteve.com ?

⑤

QID=1001	
Qu	www12345678.bankofsteve.com A?
An	(empty)
Au	bankofsteve.com NS ns1.bankofsteve.com
Ad	ns1.bankofsteve.com A 10.1.1.1

⑥ IP for www12345678.bankofsteve.com ?

⑦ Answer = (doesn't matter)

QID=1000 - mismatch

QID=1001 - success!

QID=1002 - mismatch

⑧ Answer = (doesn't matter)

DAN KAMINSKY'S ATTACK (2008)

1. Attacker sends requests for random.BankOfSteve.com to recursive name server.

DAN KAMINSKY'S ATTACK (2008)

1. Attacker sends requests for random.BankOfSteve.com to recursive name server.
2. Recursive name server refers request to authoritative name server for BankOfSteve.com.

DAN KAMINSKY'S ATTACK (2008)

1. Attacker sends requests for random.BankOfSteve.com to recursive name server.
2. Recursive name server refers request to authoritative name server for BankOfSteve.com.
3. Attacker sends answers for random.BankOfSteve.com with guessed QIDs,
   → and additional resource record for www.BankOfSteve.com (in bailiwick).

DAN KAMINSKY'S ATTACK (2008)

1. Attacker sends requests for random.BankOfSteve.com to recursive name server.
2. Recursive name server refers request to authoritative name server for BankOfSteve.com.
3. Attacker sends answers for random.BankOfSteve.com with guessed QIDs,
   → and additional resource record for www.BankOfSteve.com (in bailiwick).
4. If guessed QID is correct and attacker's answer wins race with NXDOMAIN.
   → Entry www.BankOfSteve.com is cached with a TTL set by attacker.

DAN KAMINSKY’S ATTACK (2008)

1. Attacker sends requests for random.BankOfSteve.com to recursive name server.
2. Recursive name server refers request to authoritative name server for BankOfSteve.com.
3. Attacker sends answers for random.BankOfSteve.com with guessed QIDs,
   → and additional resource record for www.BankOfSteve.com (in bailiwick).
4. If guessed QID is correct and attacker’s answer wins race with NXDOMAIN.
   → Entry www.BankOfSteve.com is cached with a TTL set by attacker.
5. Recursive name server will now direct all queries for www.BankOfSteve.com to attacker’s IP address.

KAMINSKY'S ATTACK ILLUSTRATED

http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html

SEVERITY OF ATTACK

- Very serious attack: attacker becomes name server for domains of their choice.
- Attack increases chance of guessing a QID correctly by trying many random host names.
- Reportedly success within 10 seconds.
- Many ways for triggering name resolution at recursive name server.
- Alternative attack strategy: send many faked name server redirects for www.BankOfSteve.com with guessed QID (version in Kaminsky's black hat talk).

MITIGATING DNS CACHE ATTACKS

COUNTERMEASURES

- Increase search space for attacker: run queries on random ports.

$$\underbrace{2^{16}}_{\text{Query ID}} \times \underbrace{2^{11}}_{\text{Source ports}} = 2^{27} = \mathbf{134\ million}$$

  → Attacker now must guess correct QID & port number.
- Restrict access to local recursive name server:
  → split name server (split-split name server).
- DNSSec:
  → cryptographic authentication using digital signatures;
  → give up on QID as a security feature.

SPLIT NAME SERVER

- Split the task of supporting local users who want to connect to the outside world from supporting remote users who want to connect to local hosts.

SPLIT NAME SERVER

- Split the task of supporting local users who want to connect to the outside world from supporting remote users who want to connect to local hosts.
  - → Recursive name server for internal queries to resolve (external) host names.

SPLIT NAME SERVER

- Split the task of supporting local users who want to connect to the outside world from supporting remote users who want to connect to local hosts.

  → Recursive name server for internal queries to resolve (external) host names.

  → Non-recursive authoritative name server for zone to resolve external queries for host names in zone

SPLIT NAME SERVER

- Split the task of supporting local users who want to connect to the outside world from supporting remote users who want to connect to local hosts.
  - → Recursive name server for internal queries to resolve (external) host names.
  - → Non-recursive authoritative name server for zone to resolve external queries for host names in zone
- Non-recursive DNS server facing external users does not cache resource records so there is no cache to poison.

SPLIT NAME SERVER

- Split the task of supporting local users who want to connect to the outside world from supporting remote users who want to connect to local hosts.
  - → Recursive name server for internal queries to resolve (external) host names.
  - → Non-recursive authoritative name server for zone to resolve external queries for host names in zone
- Non-recursive DNS server facing external users does not cache resource records so there is no cache to poison.
- No defence against local attackers.

DNSSEC

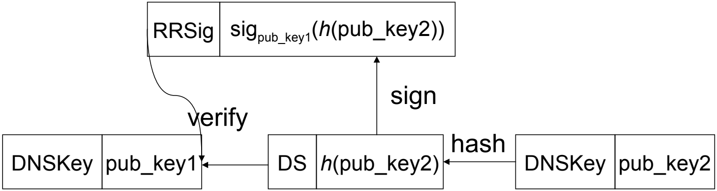
- DNS Security Extensions, protect the authenticity and integrity of resource records with digital signatures.
- Specified in RFC 2535 already in 1999.
- RFC 2535 superseded by RFCs 4033-4035 in 2005.
- Several new resource record types introduced:
  - → RRSIG resource records contain digital signatures of other resource records.
  - → DNSKEY resource records contain the public keys of zones.
  - → DS (Delegation Signer) resource records contain hashes of DNSKEY records.

By using a key from the DNSKEY record you can verify the signature contained in the RRSIG record.

DNSSEC – AUTHENTICATION

- Authentication chains built by alternating DNSKEY and DS resource records.
- Public key in a DNSKEY resource record used to verify the signature on the next DS resource record.
- Hash in the DS resource record provides the link to the next DNSKEY resource record, and so on.
- Verification in the resolver has to find a trust anchor for the chain (root verification key).

DNSSEC – AUTHENTICATION CHAIN

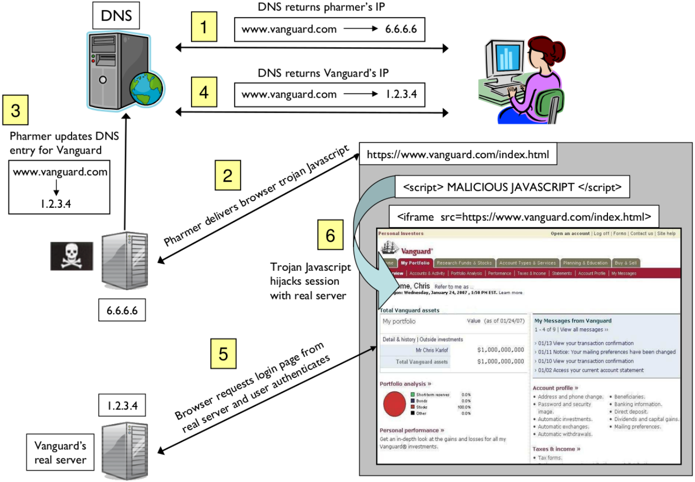


DNS REBINDING ATTACKS

DNS REBINDING

- Same origin policy: script in a web page can only connect back to the server it was downloaded from.
- To make a connection, the client's browser needs the IP address of the server.
- Authoritative DNS server resolves 'abstract' DNS names in its domain to 'concrete' IP addresses.
- The client's browser 'trusts' the DNS server when enforcing the same origin policy.
- Trust is Bad for Security!

DNS REBINDING ATTACK


DNS
1
DNS returns pharmer's IP
www.vanguard.com → 6.6.6.6
4
DNS returns Vanguard's IP
www.vanguard.com → 1.2.3.4
3
Pharmer updates DNS entry for Vanguard
www.vanguard.com
1.2.3.4
2
Pharmer delivers browser trojan Javascript
6.6.6.6
6
Trojan Javascript hijacks session with real server
5
Browser requests login page from real server and user authenticates
1.2.3.4
Vanguard's real server
https://www.vanguard.com/index.html
<script> MALICIOUS JAVASCRIPT </script>
<iframe src=https://www.vanguard.com/index.html>

Personal Investors Open an account | Log off | Forms | Contact us | Site help

Vanguard®

ome | My Portfolio | Research Funds & Stocks | Account Types & Services | Planning & Education | Buy & Sell

rview | Accounts & Activity | Portfolio Analysis | Performance | Taxes & Income | Statements | Account Profile | My Messages

ome, Chris Refer to me as ...
gon: Wednesday, January 24, 2007 , 1:50 PM EST. Learn more

Total Vanguard assets

My portfolio	Value (as of 01/24/07)
Detail & history | Outside investments	
Mr Chris Karlof	$1,000,000,000
Total Vanguard assets	$1,000,000,000

My Messages from Vanguard
1 - 4 of 9 | View all messages »

› 01/13 View your transaction confirmation
› 01/11 Notice: Your mailing preferences have been changed
› 01/10 View your transaction confirmation
› 01/02 Access your current account statement

Portfolio analysis »

🟩 Short-term reserves	0.0%
■ Bonds	0.0%
🟥 Stocks	100.0%
■ Other	0.0%

Personal performance »
Get an in-depth look at the gains and losses for all my Vanguard® investments.

Account profile »
- Address and phone change.
- Password and security image.
- Automatic investments.
- Automatic exchanges.
- Automatic withdrawals.
- Beneficiaries.
- Banking information.
- Direct deposit.
- Dividends and capital gains.
- Mailing preferences.

Taxes & income »
- Tax forms.

C.Carlos et al. Dynamic Pharming Attacks and Locked Same-origin Policies for Web Browsers, CCS07

DNS REBINDING ATTACK: DETAILS

- “Abuse trust”: Attacker creates attacker.org domain; binds this name to two IP addresses, to its own and to the target’s address.
- Client downloads applet from attacker.org; script connects to target; permitted by same origin policy.
- Defence: Same origin policy with IP address.

→ D. Dean, E.W. Felten, D.S. Wallach: Java security: from HotJava to Netscape and beyond, 1996 IEEE Symposium on Security & Privacy.

DNS REBINDING ATTACK: DETAILS

- Client visits attacker.org; attacker’s DNS server resolves this name to attacker’s IP address with short time-to-live.
- Attack script waits before connecting to attacker.org.
- Binding at browser has expired; new request for IP address of attacker.org, now bound to target address.
- Defence: Don’t trust the DNS server on time-to-live; pin host name to original IP address;
  - → J. Roskind: Attacks against the Netscape browser. in RSA Conference, April 2001.
  - → Duration of pinning is browser dependent.

DNS REBINDING ATTACK: DETAILS

- Attacker shuts down its web server after the page has been loaded.
- Malicious script sends delayed request to attacker.org.
- Browser's connection attempt fails and pin is dropped.
- Browser performs a new DNS lookup and is now given the target's IP address.
- General security issue: error handling procedures written without proper consideration of their security implications.

IS IT OVER?

- Next round — browser plug-ins, e.g. Flash.
- Plug-ins may do their own pinning.
- Dangerous constellation:
  - → Communication path between plug-ins.
  - → Each plug-in has its own pinning database. Some may have different/weaker pinning mechanisms.
- Attacker may use the client's browser as a proxy to attack the target.
- Defence (centralize controls): one pinning database for all plug-ins
  - → E.g., let plug-ins use the browser's pins.
  - → Feasibility depends on browser and plug-in.

BOTNETS AND DNS

BOTNET

- A botnet consists of bots (drones), i.e. programs installed on the machines of unwitting Internet users and receiving commands from a bot controller.
- Botnet attacks do not target communications links. You do not face an adversary in charge of the entire Internet — but you can no longer assume that the end points of links are safe harbours.

MATERIAL

- Schiavoni, Maggi, Cavallaro, and Zanero, ”Phoenix: DGA-based Botnet Tracking and Intelligence”
- Poster on ”Cerberus: Detection and Characterization of Automatically-Generated Malicious Domains”

ELT GROUP

- Elettronica S.p.a. Roma
- Elettronica GmbH Germany
- Cy4Gate S.r.l Roma

elt

ELT
Technologie für Innovation

CY4
GATE
CYBER EW & INTELLIGENCE
AN ELETTRONICA GROUP COMPANY

ELT GROUP

- Elettronica S.p.a. Roma
- Elettronica GmbH Germany
- Cy4Gate S.r.l Roma

We're hiring and looking for internships