Chapter 61
Domain Name System (DNS)

- **True Names have Power.**

> **“I will give you three days' time,” said he; “if by that time you find out my name, then shall you keep your child.”**
>
> **-- Rumpelstiltskin**

Copyright Information

- Some rights reserved / Einige Rechte vorbehalten
- Michael Kafka, René Pfeiffer, Sebastian Mayer
  C.a.T. Consulting and Trainings, Vienna, Austria
- You may freely use, distribute and modify this work under following agreement:
- Diese Arbeit darf frei genutzt, verbreitet und bearbeitet werden unter folgenden Bedingungen:

Authors must be referenced (also for modification)
Autoren müssen genannt werden (auch bei Bearbeitung)

Only for non commercial use
Nur für nichtkommerzielle Nutzung

Derivative work under same licence
Derivative Arbeit unter selber Lizenz

creative commons http://www.creativecommons.com

DeepSec Vienna 2007
7 Layers of Insecurity

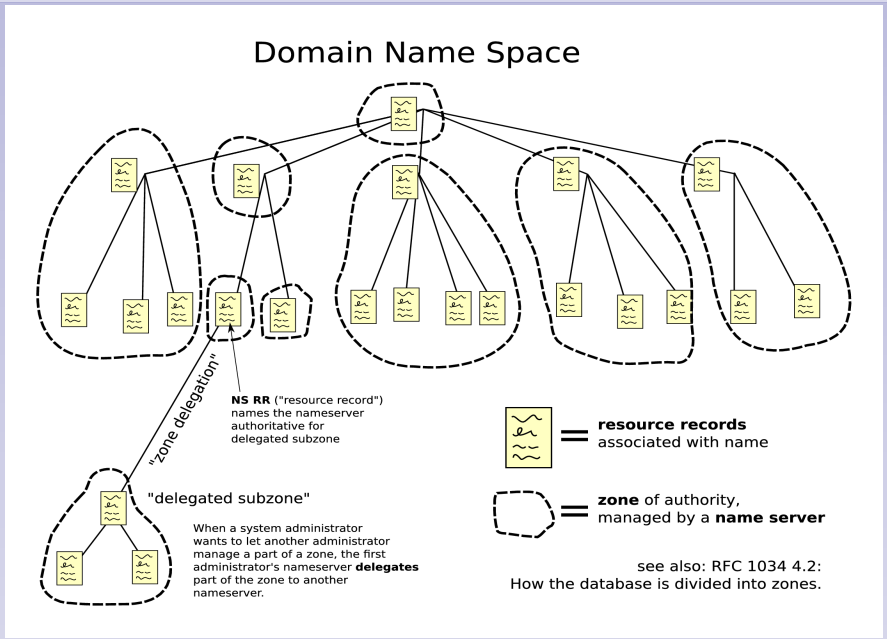
Chapter 61
Domain Name System

- Agenda
  - Role of DNS
    - Deployment
    - Protocol
  - DNS Software
  - DNS Reconnaissance
  - DNS Poisoning
  - DNSSEC

Role of DNS

- **Your Names are your Premium Resource.**

DNS Hierarchy



DNS Protocol

- DNS uses TCP and UDP on port 53
  - UDP for most queries and answers
  - TCP for information > 512 byte
- DNS uses records to order information
  - MX, A, NS, PTR, SRV, LOC, …
  - Answers have TTL
- 16 bit ID used to distinguish query/response
- DNS servers usually act as
  - *authority* exclusive or
  - *cache*

DNS Software

- **Well and Lesser Known Software.**

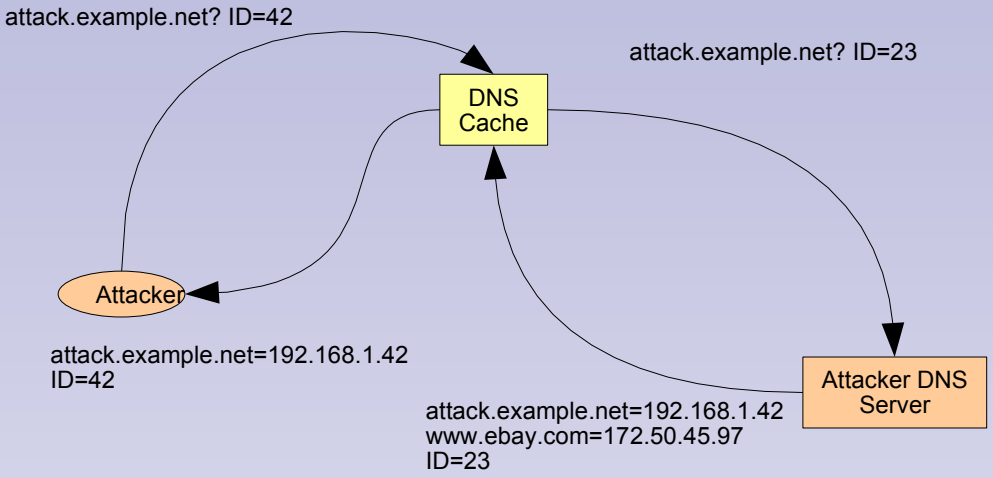
DNS Software

- BIND V4, V8 and V9
  - Please use V9 if you use BIND
- djbdns
- dnsmasq
- Posadis
- PowerDNS
- MaraDNS
- Microsoft® DNS Server
- NSD

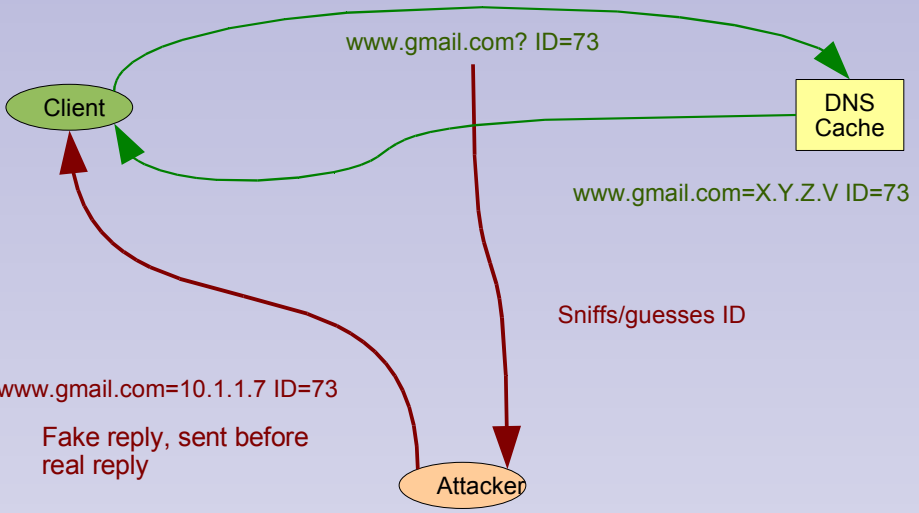
DNS Reconnaissance

- Interesting names attract attackers
  - *auth.example.net*, *radius.example.net*
  - *secure.example.net*
- "Split Horizon" DNS
  - Maintain external and internal zone
  - Separate views of your namespace
- Risk: medium
- Impact: low

DNS Cache Poisoning

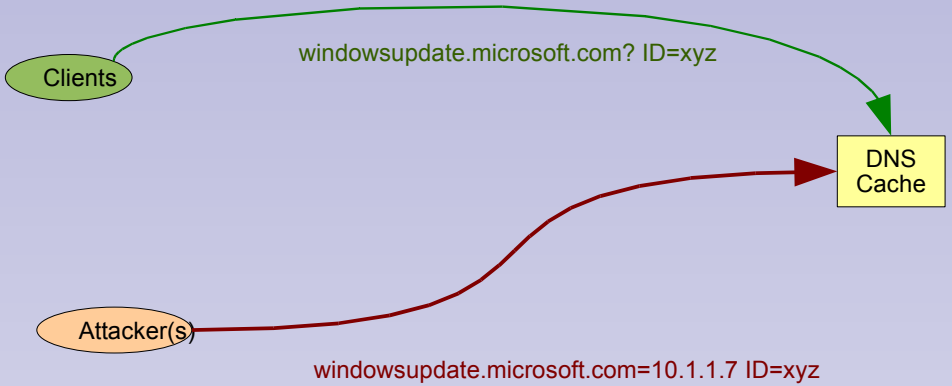


DNS Spoofing



DeepSec Vienna 2007
7 Layers of Insecurity

DNS Flooded Spoofing



DNS Spoofing Defence

- DNS software checks source/target ports
- Split DNS service according to roles
  - Authority servers don't resolve recursively
  - Cache servers are never a authority
  - Use distinct internal/external namespace
- Don't cache additional records
- Don't rely on DNS on critical systems
- Use TLS & certificates to check origin and destination

DNS Pinning

- Pinning is a defence used by browsers
- Store DNS information until session ends
  - Online/offline switch
  - Ending the application
  - Server becomes unavailable
- HTTP/FTP proxies may also use pinning

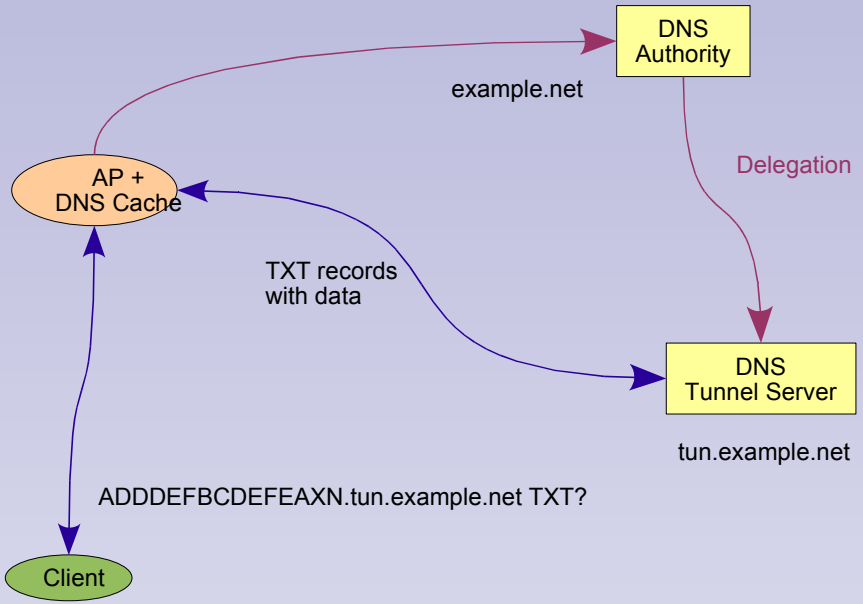
DNS Rebinding

- Offer records with a very short TTL
  - *attacker.example.net*
- Browser fetches HTML with JavaScript
- JavaScript sends another HTTP request
  - But *attacker.example.net* changed to internal address
  - Browser acts as probe to internal network
- Protecting Browsers from DNS Rebinding Attacks

DNS Tunnel

- DNS TXT records can hold BASE64 data
- Set up subdomain with dedicated NS
  - Encode data request into names
  - Encode response into TXT records
  - Use custom DNS software on both ends
  - Voilà – a “covert” channel!
- Useful for costly WLANs where you get free DHCP/DNS
- Disadvantage - slow

DNS Tunnel Illustrated



DeepSec Vienna 2007
7 Layers of Insecurity

DNS + TTL = NAS

- DNS replies have TTL
- Caches store information until expiration
- Use the DNS as NAS
  - Create a numbering scheme
  - Link DNS records sequentially
  - Put data into suitable records on NS
  - Retrieve data with suitable queries
- Risk and mitigation similar to DNS tunnel

DNSSEC

- DNS uses no integrity & encryption
- DNSSEC addresses integrity of data
  - Signed zones and records
  - Public key encryption
- RFC 2535 proposal can't handle
  - large networks
  - out-of-sync master/slave servers
- DNSSEC was modified → DNSSEC-bis

DNSSEC Deployment

- Current users
  - PIR, RIPE NCC, Sweden, VeriSign
- Major problems stopping deployment
  - DNSSEC requires full zone disclosure
  - Trust anchor keys for TLDs
  - Signature roll-out
  - Question about benefits and reliability
- Currently DNSSEC is ~~useless~~ without significant benefits

Chapter 61
Domain Name System

- Summary
  - DNS is crucial for you and attackers.
  - Use Split Horizon DNS when possible.
  - Limit access to DNS if possible.
  - Review DNS server configuration.
  - Use different caches and authorities.

Thank You!

- Questions?

DeepSec Vienna 2007
7 Layers of Insecurity

Chapter 61
Domain Name System (DNS)

- True Names have Power.

"I will give you three days' time," said he; "if by that time you find out my name, then shall you keep your child."

-- Rumpelstiltskin

DeepSec Vienna 2007
7 Layers of Insecurity

© November 2007 61 - DNS 1

Copyright Information

- Some rights reserved / Einige Rechte vorbehalten
- Michael Kafka, René Pfeiffer, Sebastian Mayer
  C.a.T. Consulting and Trainings, Vienna, Austria
- You may freely use, distribute and modify this work under following agreement:
- Diese Arbeit darf frei genutzt, verbreitet und bearbeitet werden unter folgenden Bedingungen:

Authors must be referenced (also for modification)
Autoren müssen genannt werden (auch bei Bearbeitung)

Only for non commercial use
Nur für nichtkommerzielle Nutzung

Derivative work under same licence
Derivative Arbeit unter selber Lizenz

creative commons http://www.creativecommons.com

DeepSec Vienna 2007
7 Layers of Insecurity

© November 2007 61 - DNS 2

This presentation is published under the CreativeCommons License which can be viewed in detail on their hompage: http://creativecommons.org/licenses/by-nc-sa/2.0/at/

Read more on http://www.creativecommons.com

You are free:

to Share — to copy, distribute and transmit the work

to Remix — to adapt the work

Under the following conditions:

Attribution. You must attribute the work in the manner specified by the author or licensor (but not in any way that suggests that they endorse you or your use of the work).

Noncommercial. You may not use this work for commercial purposes.

Share Alike. If you alter, transform, or build upon this work, you may distribute the resulting work only under the same or similar license to this one.

- **For any reuse or distribution, you must make clear to others the license terms of this work. The best way to do this is with a link to this web page.**
- **Any of the above conditions can be waived if you get permission from the copyright holder.**
- **Nothing in this license impairs or restricts the author's moral rights.**

Chapter 61
Domain Name System

- Agenda
  - Role of DNS
    - Deployment
    - Protocol
  - DNS Software
  - DNS Reconnaissance
  - DNS Poisoning
  - DNSSEC

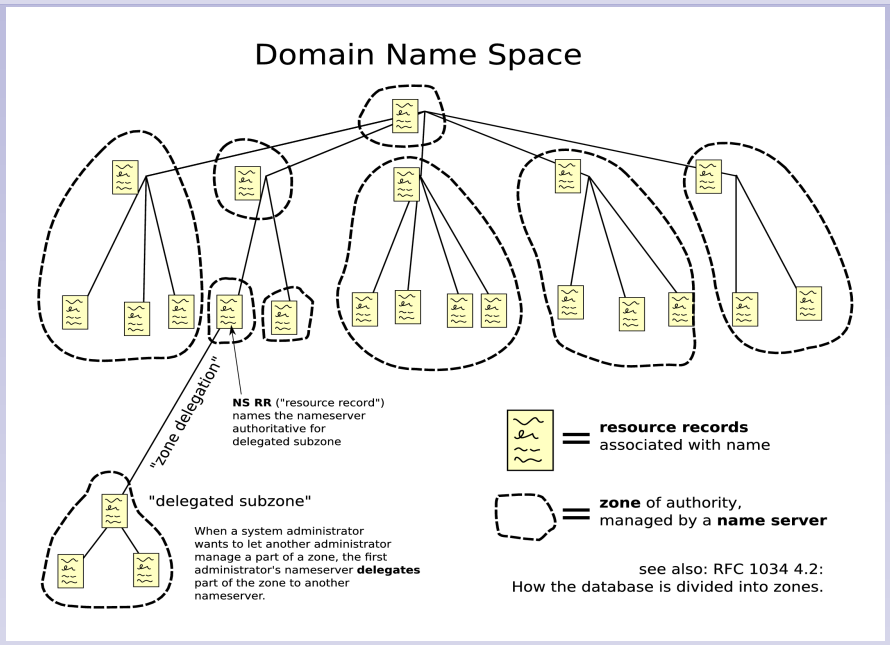
DeepSec Vienna 2007
7 Layers of Insecurity

Role of DNS

- Your Names are your Premium Resource.

DeepSec Vienna 2007
7 Layers of Insecurity

DNS Hierarchy



DeepSec Vienna 2007
7 Layers of Insecurity

The DNS has a hierarchical structure. There are also alternative root servers providing TLDs not registered with the “known” registrars.

DNS Protocol

- DNS uses TCP and UDP on port 53
  - UDP for most queries and answers
  - TCP for information > 512 byte
- DNS uses records to order information
  - MX, A, NS, PTR, SRV, LOC, …
  - Answers have TTL
- 16 bit ID used to distinguish query/response
- DNS servers usually act as
  - *authority* exclusive or
  - *cache*

DeepSec Vienna 2007
7 Layers of Insecurity

There are numerous sources available for DNS training and getting to know the protocol.

• DNS for Rocket Scientists

• DNS and BIND, Paul Albitz & Cricket Liu, O'Reilly & Associates, Inc., 4th edition 2001.

DNS Software

- **Well and Lesser Known Software.**

DeepSec Vienna 2007
7 Layers of Insecurity

DNS Software

- BIND V4, V8 and V9
  - Please use V9 if you use BIND
- djbdns
- dnsmasq
- Posadis
- PowerDNS
- MaraDNS
- Microsoft® DNS Server
- NSD

DeepSec Vienna 2007
7 Layers of Insecurity

The list shows the most common DNS server software in use. The licensing of the code ranges from proprietary to Free Software. BIND is the oldest product and can be called the “DNS pioneer”. Make sure that you evaluate all products properly, understand its limitations and configuration. Allow for generous testing prior to deployment.

DNS Reconnaissance

- Interesting names attract attackers
  - *auth.example.net, radius.example.net*
  - *secure.example.net*
- "Split Horizon" DNS
  - Maintain external and internal zone
  - Separate views of your namespace
- Risk: medium
- Impact: low

DeepSec Vienna 2007
7 Layers of Insecurity

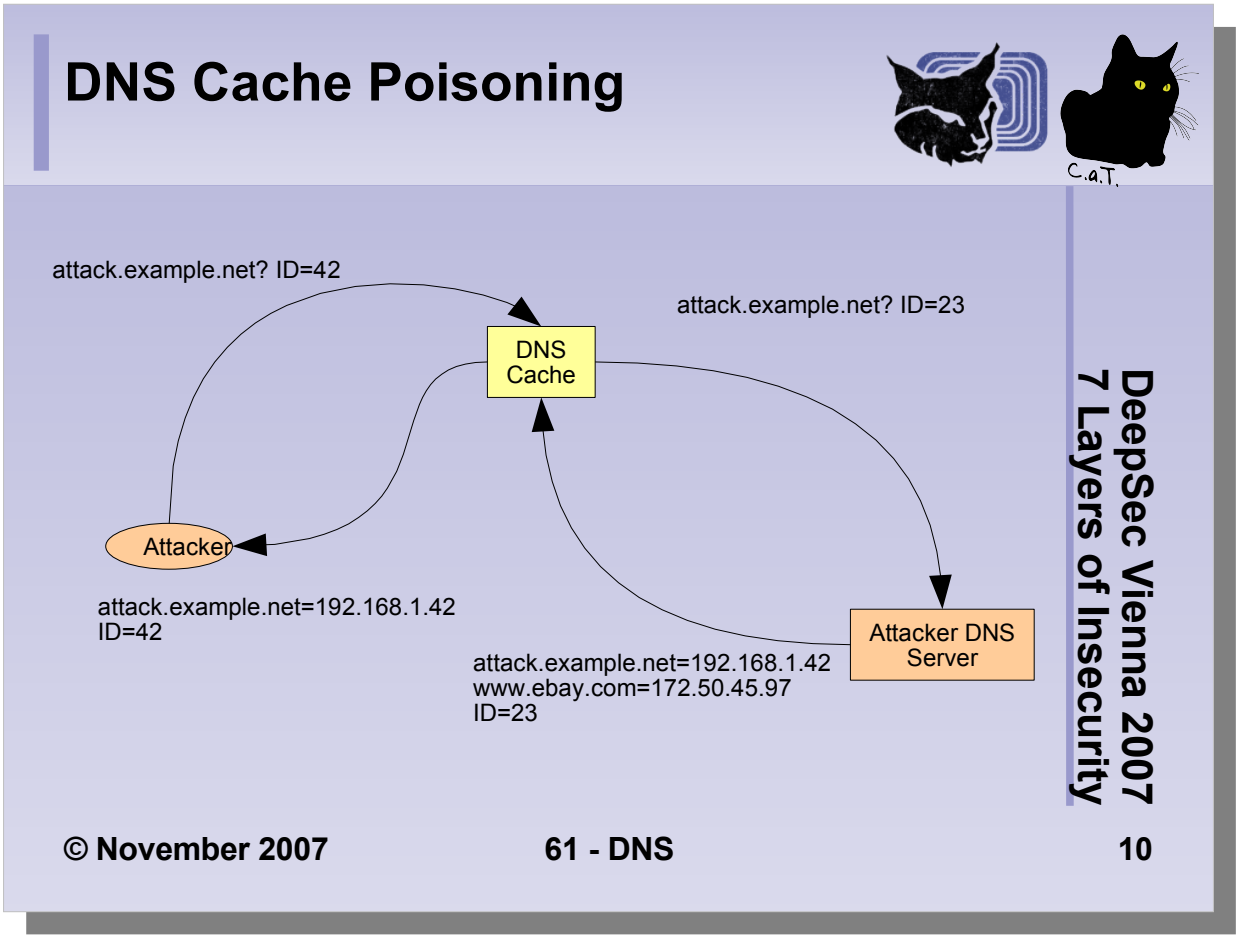
You can't hide a name in DNS. There are no access controls once the data is in the public zone. Anything present in your public zone will be announced publicly. Don't hide in plain sight.

Mitigation:

• The public DNS zone must only hold public information.

• Critical infrastructure announced in the public DNS must be secured by means of filters.

• Use a Split Horizon DNS configuration if you need an internal zone with a different set of information.



DNS Cache Poisoning works by sending additional “out-of-zone” information to a DNS server that issued DNS queries. An attacker usually provokes DNS lookups to a prepared zone and lets the DNS authority slip additional information to DNS servers. Depending on the DNS server software this additional information stays in the cache until it expires.

Risk: medium

Impact: medium/high

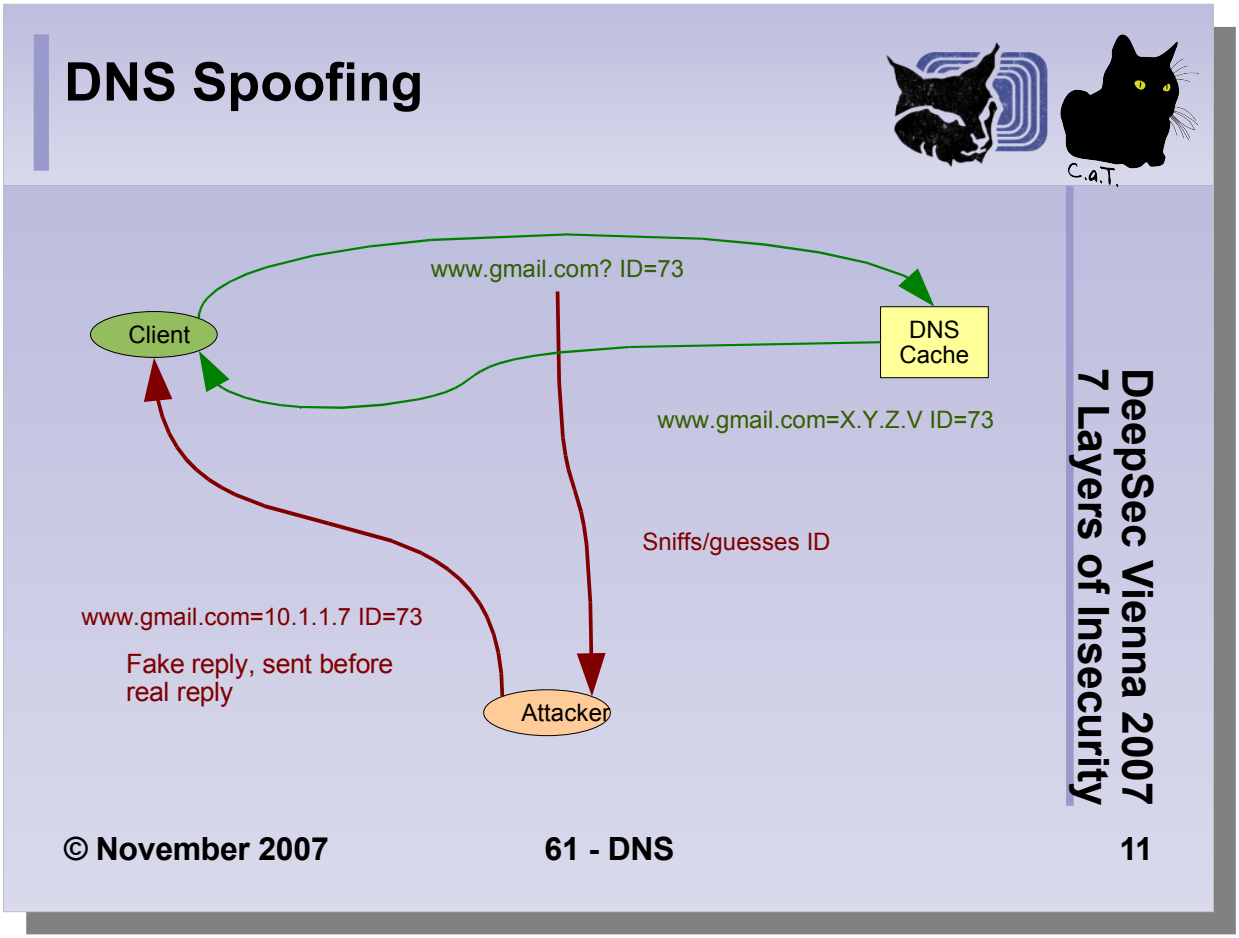
Mitigation:

• Be careful when using DNS forwarders (upstream DNS servers). Only use trustworthy servers.

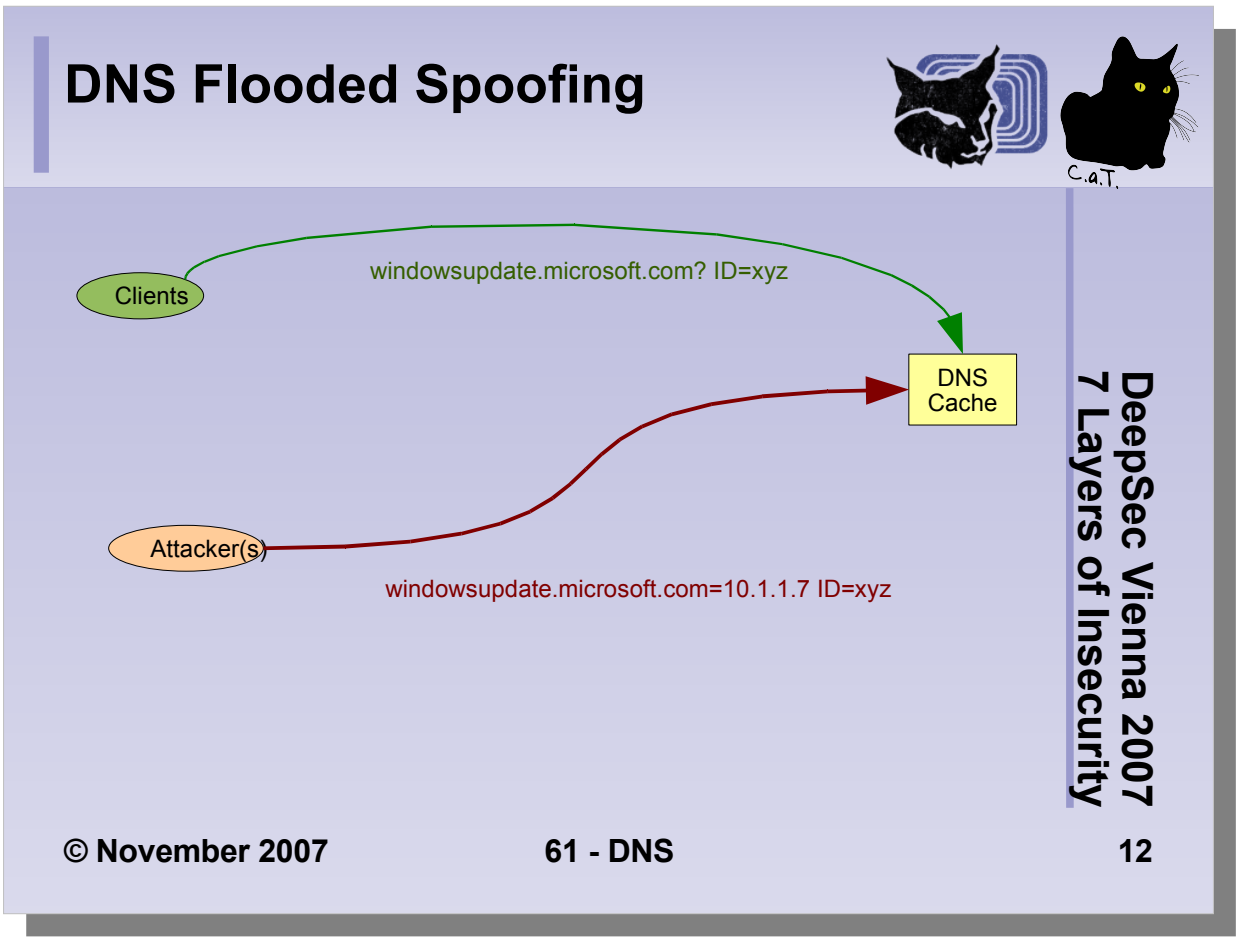
• Configure your DNS server to discard any additional information received as answers to queries.

• Use DNS software that uses sufficiently random source ports and 16-bit IDs when creating DNS queries.

• Deploy layer 3 / 4 transport security between DNS servers under your control.



DNS spoofing can occur if the attacker is able to sniff or guess the DNS ID of the query and is able to answer more quickly than the DNS cache. The transport over UDP makes the spoofing very easy.



Provided the attacker has sufficient bandwidth, it is also possible to send thousands or millions of answers to a DNS cache, thus trying to hit the right ID.

DNS Spoofing Defence

- DNS software checks source/target ports
- Split DNS service according to roles
  - Authority servers don't resolve recursively
  - Cache servers are never a authority
  - Use distinct internal/external namespace
- Don't cache additional records
- Don't rely on DNS on critical systems
- Use TLS & certificates to check origin and destination

DeepSec Vienna 2007
7 Layers of Insecurity

DNS Pinning

- Pinning is a defence used by browsers
- Store DNS information until session ends
  - Online/offline switch
  - Ending the application
  - Server becomes unavailable
- HTTP/FTP proxies may also use pinning

DeepSec Vienna 2007
7 Layers of Insecurity

DNS Rebinding

- Offer records with a very short TTL
  - *attacker.example.net*
- Browser fetches HTML with JavaScript
- JavaScript sends another HTTP request
  - But *attacker.example.net* changed to internal address
  - Browser acts as probe to internal network
- Protecting Browsers from DNS Rebinding Attacks

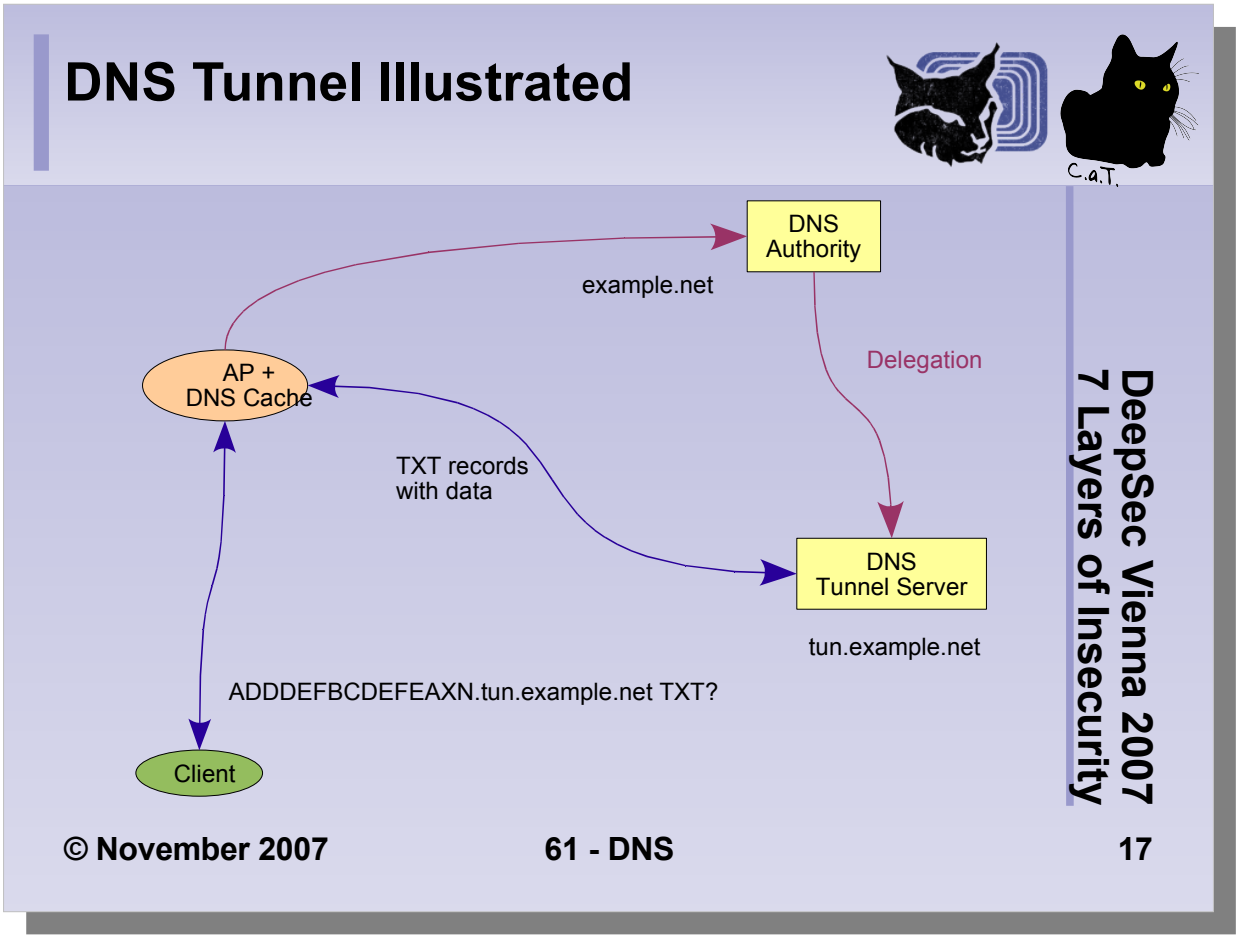
DeepSec Vienna 2007
7 Layers of Insecurity

The dnsmasq server has an option *–stop-dns-rebind* that tells the software to filter the private IP ranges from the DNS request (127.0.0.0/8, 192.168.0.0/16, 10.0.0.0/8, 172.16.0.0/12 and 169.254.0.0/16). Other DNS software or proxies may be configured to set a minimum TTL for cached information. Some ISPs set the initial TTL of cached information in their DNS to a minimum value.

DNS Tunnel

- DNS TXT records can hold BASE64 data
- Set up subdomain with dedicated NS
  - Encode data request into names
  - Encode response into TXT records
  - Use custom DNS software on both ends
  - Voilà – a “covert” channel!
- Useful for costly WLANs where you get free DHCP/DNS
- Disadvantage - slow

DeepSec Vienna 2007
7 Layers of Insecurity



A DNS tunnel reroutes other network traffic through DNS queries and answers. The setup shown in the graphic requires a special DNS tunnel client and server. nstx and OzymanDNS are examples.

Mitigation:

- Traffic spikes in terms of bandwidth or packets/second can be monitored.
- The format of the DNS names and the corresponding TXT records can be easily identified as non-standard.
- Allow only local DNS queries on access points prior to authentication.
- Use DNS proxies and allow local clients only the access to local zones.
- Rate or size limit DNS TXT queries.

DNS + TTL = NAS

- DNS replies have TTL
- Caches store information until expiration
- Use the DNS as NAS
  - Create a numbering scheme
  - Link DNS records sequentially
  - Put data into suitable records on NS
  - Retrieve data with suitable queries
- Risk and mitigation similar to DNS tunnel

DeepSec Vienna 2007
7 Layers of Insecurity

DNSSEC

- DNS uses no integrity & encryption
- DNSSEC addresses integrity of data
  - Signed zones and records
  - Public key encryption
- RFC 2535 proposal can't handle
  - large networks
  - out-of-sync master/slave servers
- DNSSEC was modified → DNSSEC-bis

DeepSec Vienna 2007
7 Layers of Insecurity

DNSSEC Deployment

- Current users
  - PIR, RIPE NCC, Sweden, VeriSign
- Major problems stopping deployment
  - DNSSEC requires full zone disclosure
  - Trust anchor keys for TLDs
  - Signature roll-out
  - Question about benefits and reliability
- Currently DNSSEC is ~~useless~~ without significant benefits

DeepSec Vienna 2007
7 Layers of Insecurity

Chapter 61
Domain Name System

- Summary
  - DNS is crucial for you and attackers.
  - Use Split Horizon DNS when possible.
  - Limit access to DNS if possible.
  - Review DNS server configuration.
  - Use different caches and authorities.

DeepSec Vienna 2007
7 Layers of Insecurity

Thank You!

- Questions?

DeepSec Vienna 2007
7 Layers of Insecurity