How it works ...

**Internet Corporation for Assigned Names and Numbers (ICANN)**
Nonprofit organization assigned to coordinate IANA’s functions
Manages generic top-level domains (gTLDs) and country code top-level domains (ccTLDs)
Helps preserve the operational stability of the Internet
Achieves broad representation of global Internet community

**Internet Assigned Numbers Authority (IANA)**
Delegates local registrations of IP addresses to Regional Internet Registries
Administers the data in the root name servers, which is the top of the hierarchical DNS tree
Works with the Internet Engineering Task Force regarding parameters and protocols on the internet that registry related
How it works ...

ARIN – American Registry for Internet Numbers
RIPE NCC – Réseaux IP Européens Network Coordination Centre
APNIC – Asia Pacific Network Information Centre
LACNIC – Latin America and Caribbean Internet Addresses Registry
AfriNIC – African Network Information Centre
How it works ...
How it works ...

1. Translate www.google.com into IP address
2. IP address is 64.233.167.147
3. Connection Establish

IP:
- src IP = 68.94.156.1
- dst IP = 192.26.92.30

UDP:
- src port = 5798
- dst port = 53

QID = 43561
- Question count = 1
- Answer count = 0
- Authority count = 0
- Additional Record count = 0

Qu: What is A record for www.unicode.net?

RD=1 - recursion desired
OP=0 - standard query
QR=0 - this is a query

dnsr1.sbcglobal.net
c.gtld-servers.net
How it works ...
[Demo]
Use DNS for attacks

Giant Distributed System
Amplification attack
Fast-flux
Attacks ...

A. DNS: Server Attacks

B. DNS: Protocol Attacks
   - DNS cache poisoning
   - DNS Spoofing
   - DNS ID Hacking
DNS Server Attacks

- Attacks taking advantage of bugs in DNS Software implementation (buffer overflows in BIND for instance).

- Attack by Denial of Service (using flooding).
DNS cache poisoning:
attack consisting of making a DNS server
.cache false information: usually, a wrong
record that will map a name to a
“wrong” IP address.

Not always a hacker.
Cache Poisoning

Method 1:
1. hacker asks the victim DNS for a nonexistent name mapping.
2. DNS, will go and ask the DNS server responsible for the required domain. Remember this server is under the control of the hacker.
3. The hacker will answer, and add in the answer anything he wants to be cached in the victim DNS’ cache.
+ fixed in BIND, by forbidding anything that is not related to the original request to be cached.
DNS: Protocol Attacks

DNS Spoofing:

answering a DNS request that was intended for another server (a "real" DNS server).

But DNS uses ID number to identify queries and answer, so the hacker needs to find the ID the client is waiting for: DNS ID hacking.

![Diagram of DNS spoofing]

1. Normal dialog
   - Client requests ID, IP of xxx?
   - DNS server responds with ID, IP of xxx = yyy

2. DNS spoofing
   - Client requests ID, IP of xxx?
   - DNS server responds with ID, IP of xxx = zzz
   - Hacker intercepts the request and sends a response with ID, IP of xxx = zzz
Defense

Randomized query ID:
- Attacker can make a LOT of queries with names that are not likely to exist in the cache
- Most of the attempts will fail, but one will eventually succeed
  In practice, apparently, it can succeed in as little as 10 seconds.
**DNSSec**

- Uses Chain-of-Trust to establish authenticity
  - Each child signs their zone “resource record set” with the private key
  - Child’s public-key authenticity is established by the parent. Whose key is verified by its parent and so-on until we reach the root

- Can co-exist with existing DNS infrastructure
DNSSec (Domain Name System Security Extensions)

1. Q: www.papaki.eu
   A: 195.26.3.132

2. Q: www.papaki.eu
3. A: Ask www.papaki.eu
   (*ns.dns.papaki.eu)

4. www.papaki.eu

5. Q: www.papaki.eu
6. A: Ask www.papaki.eu
   (dns.papaki.eu)

7. www.papaki.eu

8. Q: www.papaki.eu
   A: 195.26.3.132

9. www.papaki.eu

10. User (stub resolver)

ISP (caching recursive resolver)

TLD - .eu (authoritative name server)

Root (authoritative name server)

Domain owner - papaki.eu (authoritative name server)
DNSSec

Chain Of Trust

KSK: Key
Signing Key

ZSK: Zone
Signing Key

DS: Delegated
Signer

Root KSK
Public Key

Root KSK
Private Key

Trust Anchor
Published by IANA

Root ZSK
Public Key

Root ZSK
Private Key

.edu KSK
Public Key

.edu KSK
Private Key

.edu zone
contains

.edu ZSK
Public Key

.edu ZSK
Private Key

.university edu
contains

.university KSK
Public Key

.university KSK
Private Key

.university zone
contains

.university edu
DS record

.university edu
ZSK Public Key

.university edu
ZSK Private Key

Signed 'bursar'
DNSSEC Deployment Growth
presented by Steve Crocker @ ICANN Cartagena Dec 2010

(The information above is representative of limited publicly available data only. The deployment of DNSSEC is rapidly changing in the market and this data should not be taken as authoritative.)