Risks and Security for the Domain Name System

BOF for Joint Techs
20 July 2005

mankin@psg.com

Introduction

- Attacks via and against the DNS infrastructure are increasing
  - Attacks are becoming costly and difficult to remedy
  - User confidence in Internet accuracy is decreasing
- The U.S. National Strategy to Secure Cyberspace (2003) recognized the DNS as a critical weakness
  - It called for coordinated public-private partnerships to encourage the adoption of improved security protocols
  - The DNSSEC Deployment Initiative is one of these partnerships (not U.S. only)
    - Open to all ready to implement (details later)

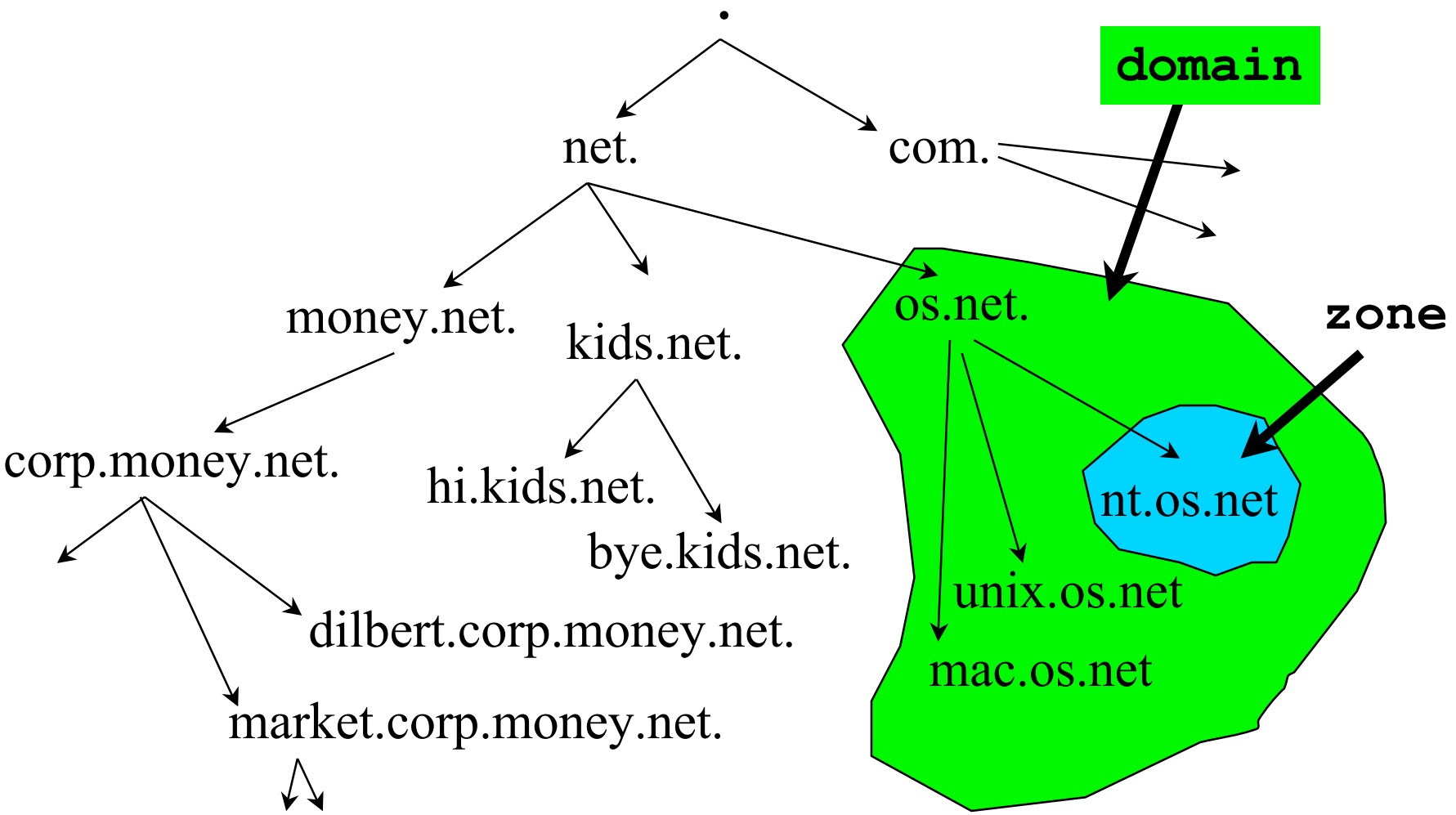
Breaking Network Trust

- Forged DNS data breaks applications
  - Genuine web sites can be replaced with a false site without ever touching the original site, but more insidiously the original site can be reached after stopping at a site that performs a malicious act.
  - E-mail and every other application (trusted backend and system security, included) can be re-routed or mis-delivered
  - Logins including ssh can be compromised through man in the middle attacks leading to identity theft
- DNS attack tools are readily available on the Internet (for example, dsniff, dnshijack, and many more) and they are all FREE!
- We'll look at recent real attack in a moment…

DNS Software is Part of the Problem

- There are many bugs in software and other issues underlying each specific attack
- A protocol/infrastructure approach to DNS security is best:
  - Because it is infrastructural, it detects and addresses attacks independent of software holes
  - New bugs and holes will always arise, but with the right upfront work, the system is catching the attacks (and the bugs) before the damage mounts

Sample DNS Tree



SOURCE: RUSS MUNDY

DNSSEC

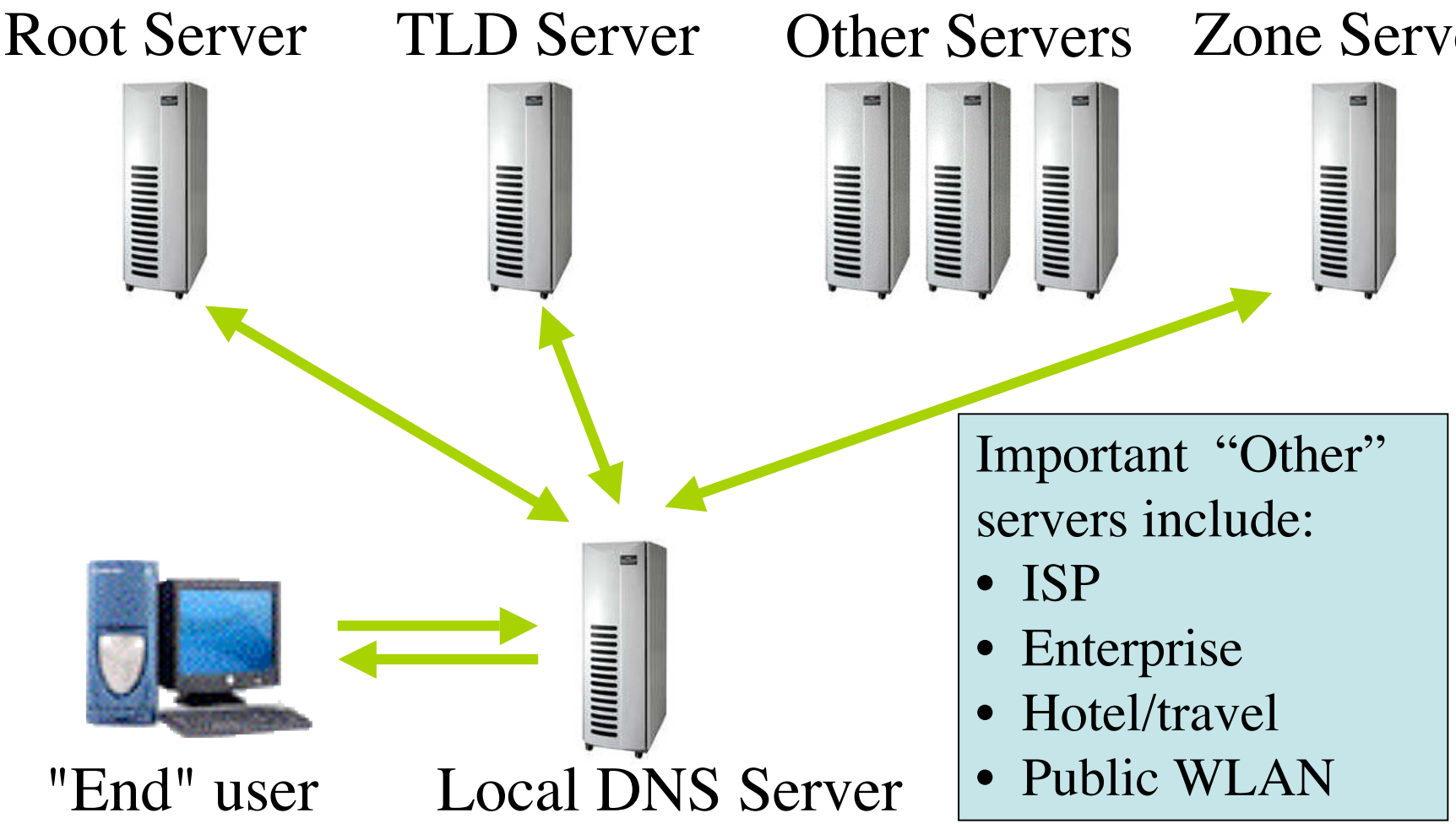
What Does DNSSEC Do?

- Provides an approach so DNS users can:
  - Validate that data they receive came from the correct originator → *Source Authenticity*
  - Validate that data they receive is the data the originator put into the DNS → *Data Integrity*
  - Ensure that the absence of a record is validated
- This approach integrates with existing server infrastructure and user clients.
- Maximized benefit when application software integrates (e.g. DNSSEC-aware DKIM), but dumb API also important.

What Doesn't DNSSEC Do?

- It does not prevent attacks, it only detects, and it does not do anything to affect most phishing, where the user chooses a valid site, just not one that makes sense for their application.
- Applications needing end user response need a breakthrough on human factors - DNSSEC-aware applications have this need as well as certificate-based applications security

DNS Name Resolution

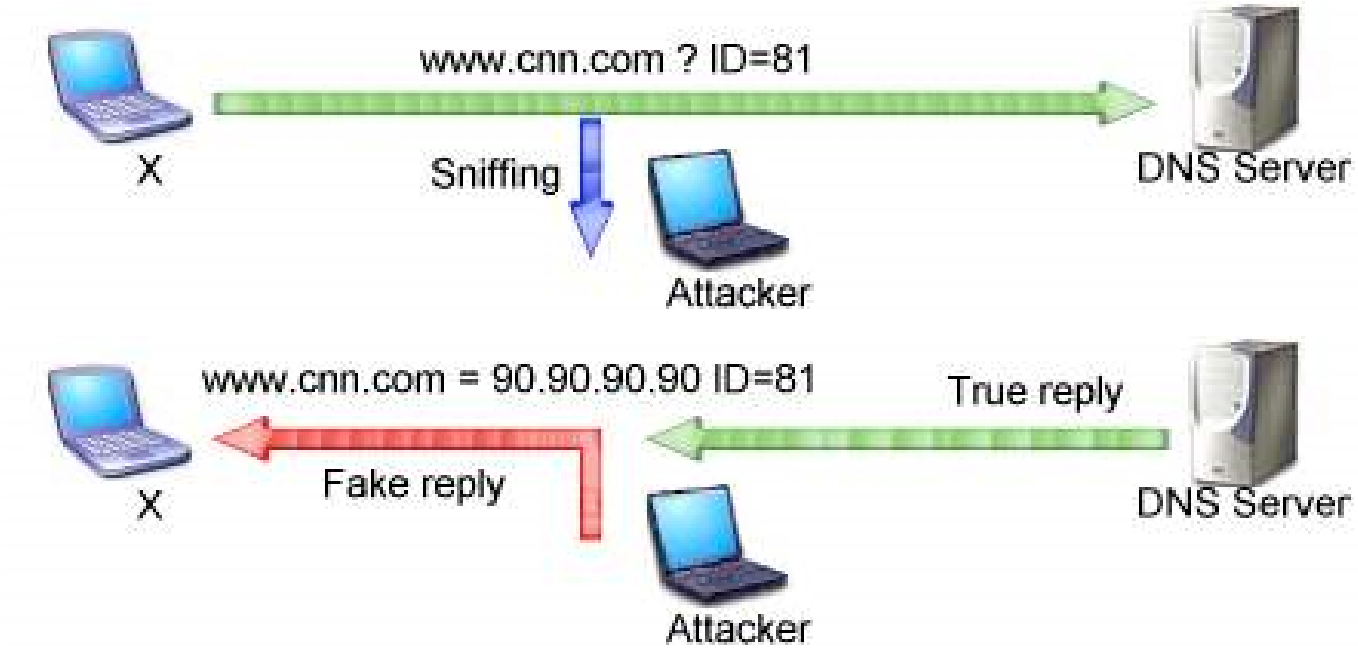


Important "Other" servers include:

- ISP
- Enterprise
- Hotel/travel
- Public WLAN

Process-in-the-middle (aka Evil Twin)

DNS query sent while working in Airport Lounge's Wireless LAN



First response wins. Second response is silently dropped on the floor. Site may relay to true destination after malicious act.

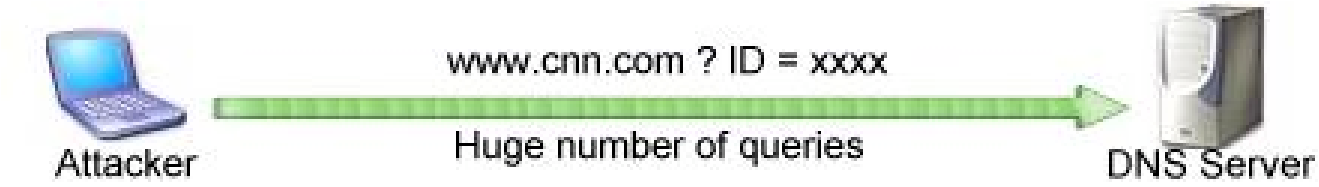
DNSSEC

Recent Live Attack: ISP Forwarder Cache Poisoning

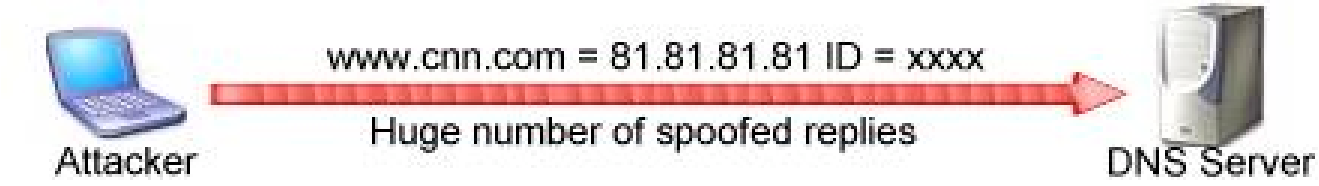
- DNS cache poisoning is an old problem but seems to continue unabated
  - Symantec products found to be vulnerable in March 2005
  - Microsoft and Linux BIND cache poisoning attacks in April 2005
  - DNS bots in May 2005
- Details on a recent widespread attack affecting many consumer ISP DNS servers at http://isc.sans.org/presentations/dnspoisoning.php

Cache Poisoning – Old Problem

- Attacker floods local DNS server with hundreds of queries for www.cnn.com



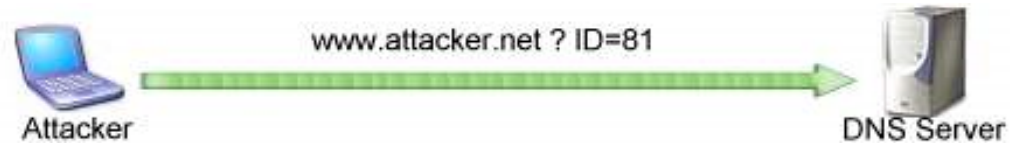
- Attacker then floods DNS server with hundreds of spoofed replies that appear to come from ns.cnn.com (CNN's authoritative name server)



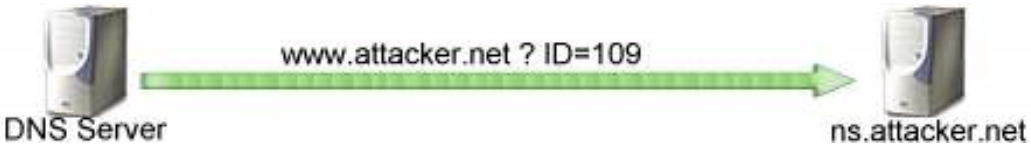
- Local DNS server is now "poisoned" with false data

Cache Poisoning – Another Method

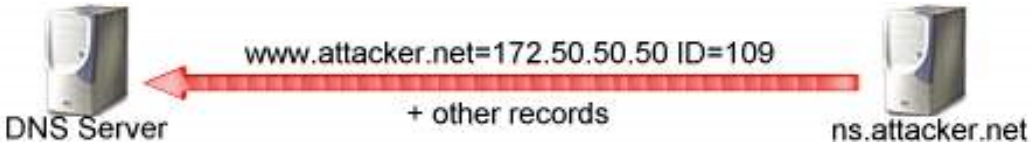
- Attacker sends a request to your local DNS asking it to resolve **`www.attacker.net`**



- Your local DNS server queries **`ns.attacker.net`** for the data



- **`ns.attacker.net`** replies, but also includes false information on **`www.cnn.com`**



- Your DNS server caches the false data on **`www.cnn.com`**

DNSSEC

Cache Poisoning – New Hybrid

- Attacker devised spam with a “bait” address.
- The record at the zone for this contained as additional material a false domain name for the .com server.
- Large numbers of small ISPs with susceptible consumers and not highly active DNS operations had .com lookups spoofed through man-in-the-middle (MITM).
- MITM was used in at least three ways: click-to-pay fraud, spyware installation, and spam sending installation.
- DNSSEC would have detected the attack in use for all of this (and what else)?
  - The DNS attack was meant to go undetected.

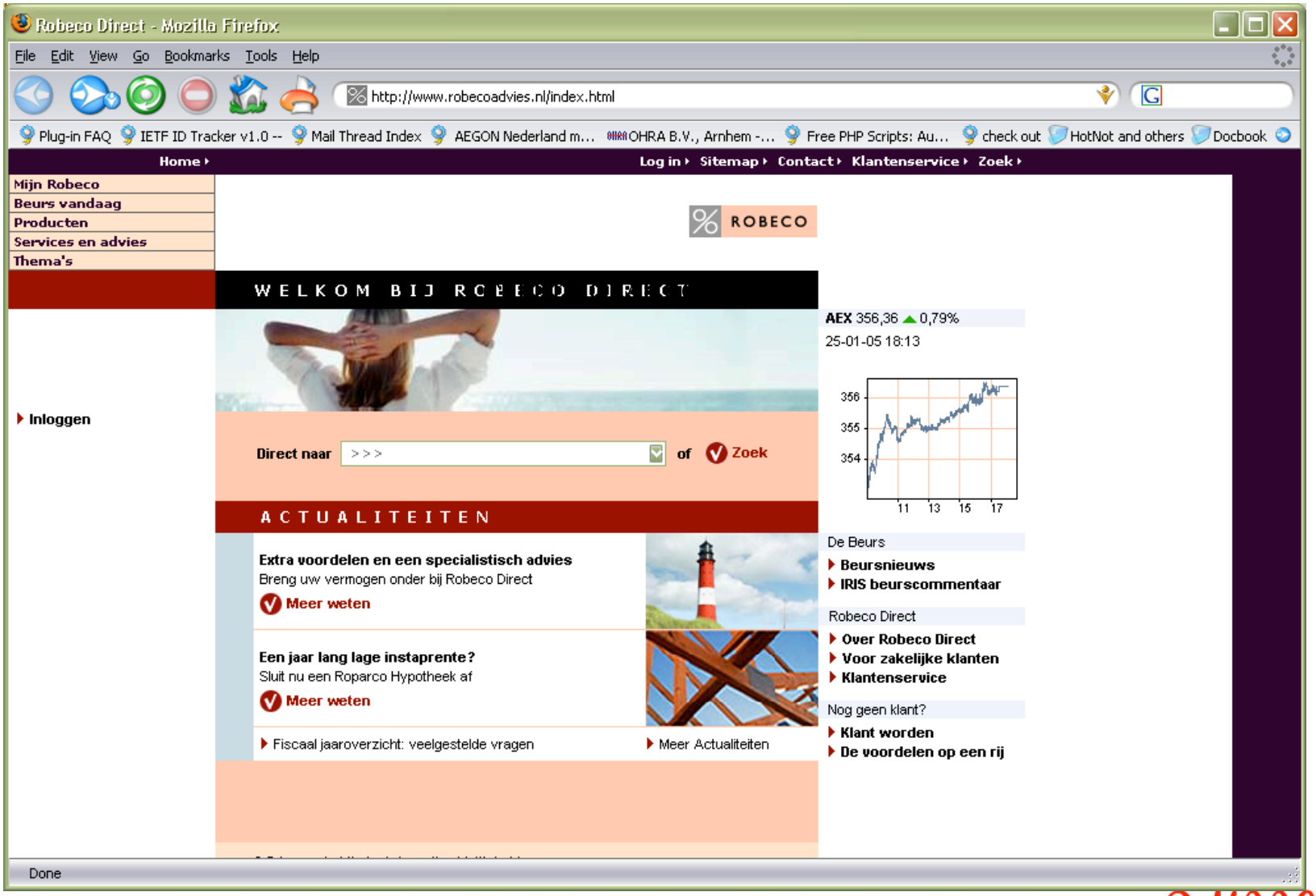
March-April ISP Attack - Impacts

- Many of the ISP users had specific spyware, or spam and pay-per-click trojans, from redirection sites (the apparent motivations for the attacks).
- Hundreds of DNS names were found spoofed in the ISP caches where data was recovered, including
  - americanexpress.com, citicards.com, dhl-usa.com, fedex.com, walmart.com, sabre.com, and many more
  - Any of these could have had man-in-the-middle attacks such as stolen passwords or intercepted traffic (no data)

DNS Software Bugs

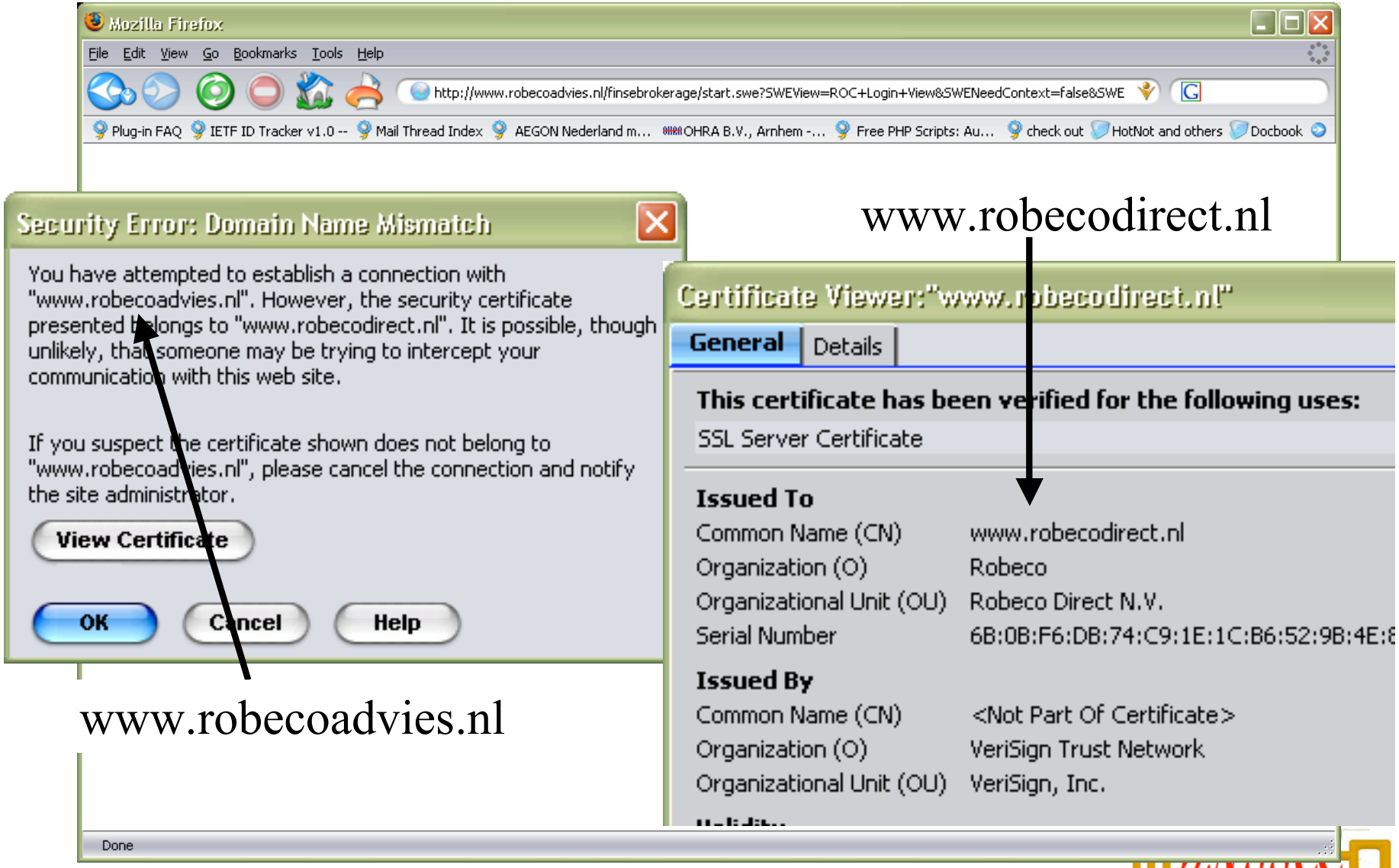
- DNS implementations have fixed many bugs that can lead to cache poisoning, including (supposedly) exploiting the additional information field. But…
- Possible solutions:
  - "Fix" all software releases against these and future attacks or :
  - Make the infrastructure generally robust against redirection
    - Because old software will be out there
    - And new vulnerabilities will be discovered
- The second option is best
- The same point applies to browsers and user behavior

Example SSL Attack: Dutch Website



CREDIT: OLAF KOLKMAN

User Easily Misses DNS Name Mismatch on the SSL Certificate, Clicks "OK"



CREDIT: OLAF KOLKMAN

DNSSEC Status

- The DNS Security Extensions (DNSSEC) protocol is now mature.
  - IETF RFCs 4033, 4034 and 4035 represent thorough testing of a simplified deployable protocol
- Implementations are up-to-date with those RFCs in BIND 9.3 (9.4 soon) and NSD 2
- Discussions with Microsoft will probably lead to a client-side (dumb API) in near-term.
- IETF DNSSEC operations guideline has been finished by its working group.
- A protocol addition may come: a new record to avoid zone-walking. Does not prevent deployment now.

DNSSEC Overview

- Each DNS zone signs its data with its private zone signing key
  - Signing should be done with zone data preparation
- User queries are answered with:
  - the requested information
  - DNSSEC data for the requested information
- Users authenticate responses with trusted key(s)
  - At least one trusted public key is pre-configured
  - Validation done with pre-configured key or keys learned via a sequence of queries to the DNS hierarchy
- Enables and supports other security technologies

DNSSEC and Costs

- DNSSEC costs associated with performance and systems overhead are in current extensive evaluation but results are encouraging (see http://www.dnssec-deployment.org/performance)
- Attackers use DNS vectors to make money
  - Both the loss from the attack and the cost to the infrastructure can be significant
  - Cost to attacker is low or nothing, gain is high
- Security always has costs besides crypto
  - What is the risk-benefit?
  - Additional costs to plan include software, training and operational activities and relationships

Getting There

- Have DNSSEC capable servers for the zone (and coordinate with the secondaries).
- Have policies in place.
- If there is a registrar-like function, make this interaction DNSSEC-capable.
- Establish key handling and key rollover.
- Sign and operate the signed zone.

Another Look at Next Steps

- Additional risk-benefit analysis
- Roles in the DNSSEC deployment initiative
  - Bringing awareness of community, of experience, of threats/attacks
  - Joining dnssec-deployment working group (see dnssec-deployment.org for more information and mailing list archive)
- Test and Engineering
  - Holding detailed community technical discussions
  - Participating in hands-on session(s) with tools, zone set-up
- Leading edge production
  - Establishing communication with zone providers, registrars, software vendors, and governing agencies
  - Bringing on line signed zones

Workshop?

- Would a hands-on workshop at the next Joint Techs be attended?
  - Two-three days

Organizational and more info

Department of Homeland Security Role in DNSSEC Deployment Initiative*

- DHS Science and Technology (S&T) Directorate sponsors several Internet security initiatives including
  - DNS Security Extensions
  - Secure Protocols for the Routing Infrastructure
  - Protected Repository for the Defense of Infrastructure against Cyber Threats
- DHS cannot secure the Internet
  - But is taking a leadership role in facilitating public-private partnerships that will result in a more secure Internet

*sponsor note :)

Some Other Sponsors of DNSSEC Initiative Activity

- The Swedish TLD registry
- The Japanese TLD registry (JPRS) and the WIDE Project
- RIPE NCC
  - Production DNSSEC deployment announced for August 2005

Not even trying to be complete list.

US DNSSEC Initiative Activities

- Roadmap published in February 2005
  - http://www.dnssec-deployment.org/roadmap.php
- Multiple workshops held world-wide
- DNSSEC testbed developed by
  - http://www-x.antd.nist.gov/dnssec/
- Formal publicity and awareness plan in development
- US Government's ".gov" zone could be DNSSEC compliant by end of 2005
- The ".us" and ".mil" zones are on track for DNSSEC compliance

For More Information

- For lots of detailed information:
  - http://www.dnssec-deployment.org
    - roadmap, operational guidelines, performance, calendar/proceedings, the dnssec-deployment working group
  - http://www.dnssec.net
    - specifications, articles, background
- This presentation -
  - Allison Mankin (Shinkuro), mankin@psg.com
  - Marcus Sachs (SRI), marcus.sachs@sri.com

  - Thanks to Peter Koch, Russ Mundy and Olaf Kolkman whose earlier presentations provided source material and help.