DNS Process-in-the-middle Attack

Bill Manning presents:
Fujiwara, Kazunori
<fujiwara@jprs.co.jp>
Japan Registry Services Co., LTD.

Demonstration

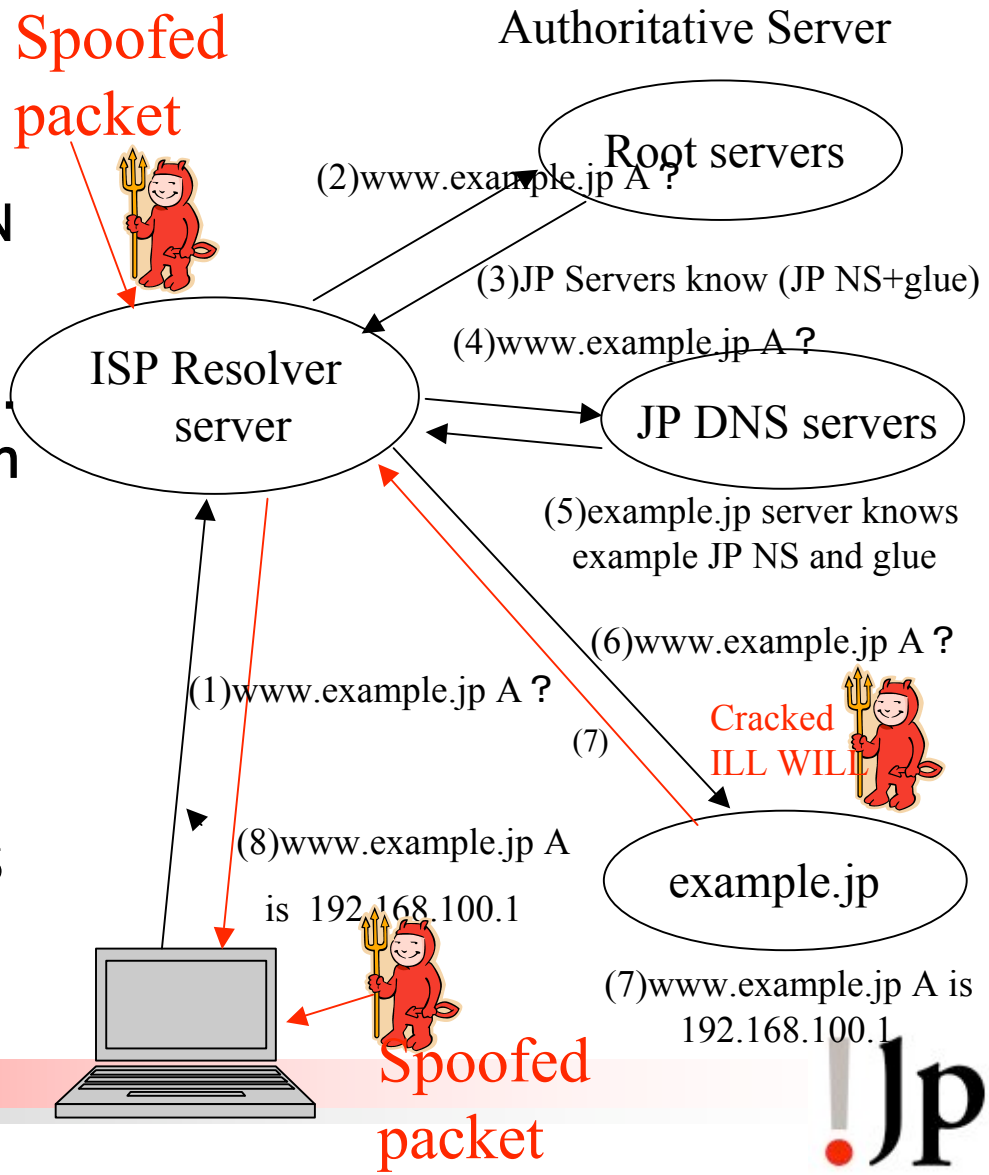
- Today, I will demonstrate DNS spoofing.
- This uses special network
  - SSID: BADBOY
- You don't like this demonstration, use ICANN SSID: ICANN

Attacks to DNS

- DoS to servers
  - Send many queries to DNS servers
  - It is mere disturbance.
  - It's easy, but attacker gets benefit?
- DNS data spoofing
  - Induce to another site
    - Phishing: economical benefit
    - Alternative root

RFC2833 Threat Analysis

- Packet Interception
  - Process-in-the-middle
  - Intercept DNS queries(1) on Shared ethernet or Wireless LAN and answers spoofed response before a correct response(8).
  - Easiest and efficient -> We tried.
- ID Guessing and Query Prediction
  - injection at (3), (5),(7)
- Name Chaining
  - cache poisoning
- Hijacked DNS server
- Measure:
  - Application side:　SSH, SSL/TLS
  - TSIG
  - DNSSEC



Process-in-the-middle attack

- packet intercept
  - tcpdump dst port domain
  - Shared ethernet
  - Wireless (using Shared WEP key)
    - Hot spot everywhere
  - tap at the Router or Switch
  - Cut cables and tap
- Parse query packet
- Generate Fake DNS answer
- Write to the Network Interface

Attack tools

- There are SEVERAL… here are three

- dnshijack
  - somewhere in the Internet
- uso800d
  - It's made by Yuji Sekiya, WIDE Project.
  - for Linux
- This attack tool (dnsattack.c)
  - To research and demonstrate for DNSSEC
  - Two days work, originally 400 lines C code
  - It uses BPF and pcap
  - It runs on *BSD and MacOS X

DNS attack experiment in WIDE

- at WIDE Project Research camp
  - about 200 testees
  - announce 15 minutes DNS attack experiments without start time
  - Any DNS 'A' query is induced to a specific address.
  - At the inducement destination, we prepared web server, SSH server, ...
- Environment
  - Wireless LAN, 11A, 11B　multiple channels, (WEP)
  - DNS attack tools on portable PC
  - Inducement destination PC
  - recording (tcpdump) PC
  - Sekiya's uso800d, fujiwara's attack tool

DNS attack result

- Found 100 IP addresses from tcpdump
- 90% IP addresses were induced to fake web site.
- evaluation by dig, 80% answers were induced.
- Some people ignored ssh warning of host key change.

- Some failure to forge
  - Wireless channel problem (Only a part of channel was attacked.)
  - Wireless reachability (Between user station and forging station)
  - Already cached DNS data is faster than forging.
  - This tool did not support IPv6 DNS resolving

Experiment validity

- No need to consider this attack in ethernet switch environment?
- We can attack using ARP Poisoning/ARP Spoofing
  - To Confuse Switch's ARP table
- On 802.11x environment,
  - No shared key, cannot intercept packets
- At the shared network, we can attack all protocols directly, some people says protecting only DNS is useless.
- But, DNS forging raises efficient phishing.

Demonstration

- Use special network
  - SSID: BADBOY
- If you don't like this demonstration, use ICANN SSID: ICANN
- Please refrain from important new communication.
- Now, I start the attack program.
- Let's see web.
- Most access will be induced to special site.
- How do you think ?

Restore from this demonstration

- Change SSID to 'ICANN'

- WindowsXP
  - ipconfig /flashdns
  - restart applications (Web browsers)
- MacOS X
  - lookupd –flashcache
- BSD
  - restart local caching server (If you use)
  - restart applications

Assertion

- DNSSEC may help identify and foil this kind of attack.