Foundations of Network and Computer Security

John Black

Lecture #25
Nov 23rd 2004

CSCI 6268/TLEN 5831, Fall 2004

Announcements

- Proj #2 – Hand in today if you didn't already
- Quiz #4: last 30 mins today
- No class Thurs (Thanksgiving) or Tues (week from today)

More Contemporary Problems in Network Security

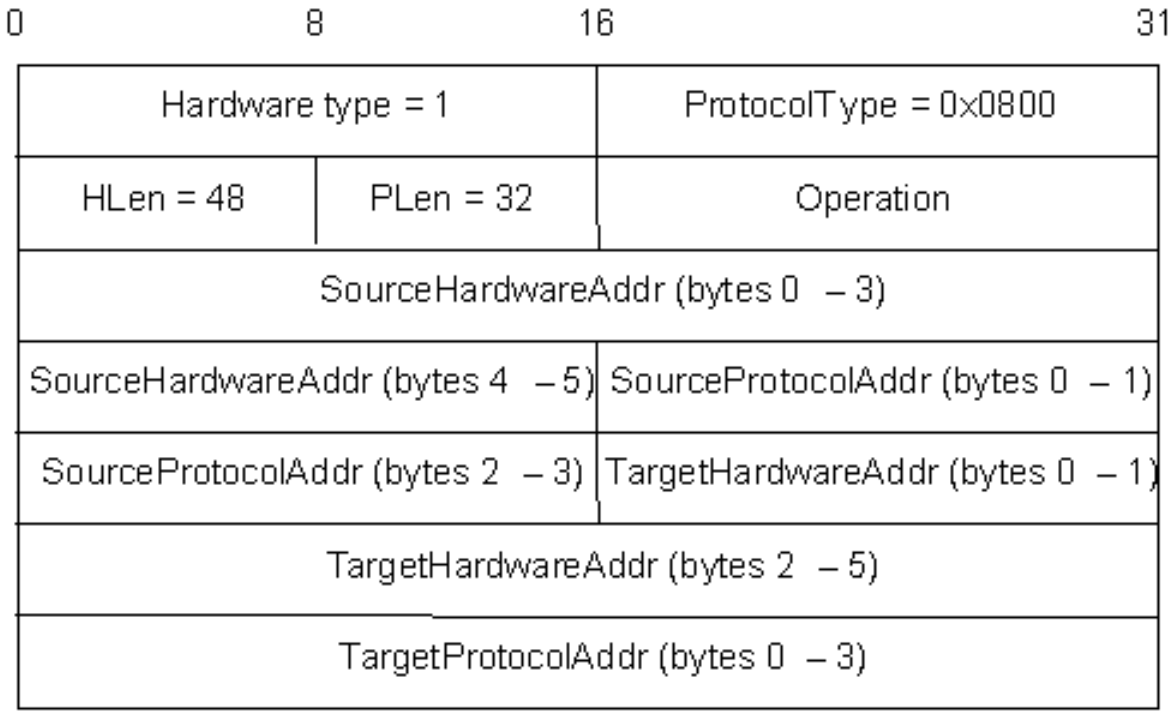
- So WEP is the only wide-spread and officially-recognized security protocol in the 802.11 standard, and it is awful

- But wait there's more:
  - Several other long-standing protocols are also badly flawed; today we'll look at two more
    - ARP
    - DNS

ARP: Address Resolution Protocol

- We already went through this protocol at a high level:
  - ARP_REQUEST
  - ARP_REPLY
  - Passive caching
  - Easily Spoofed
  - Note: this is for LANs only

ARP Packet

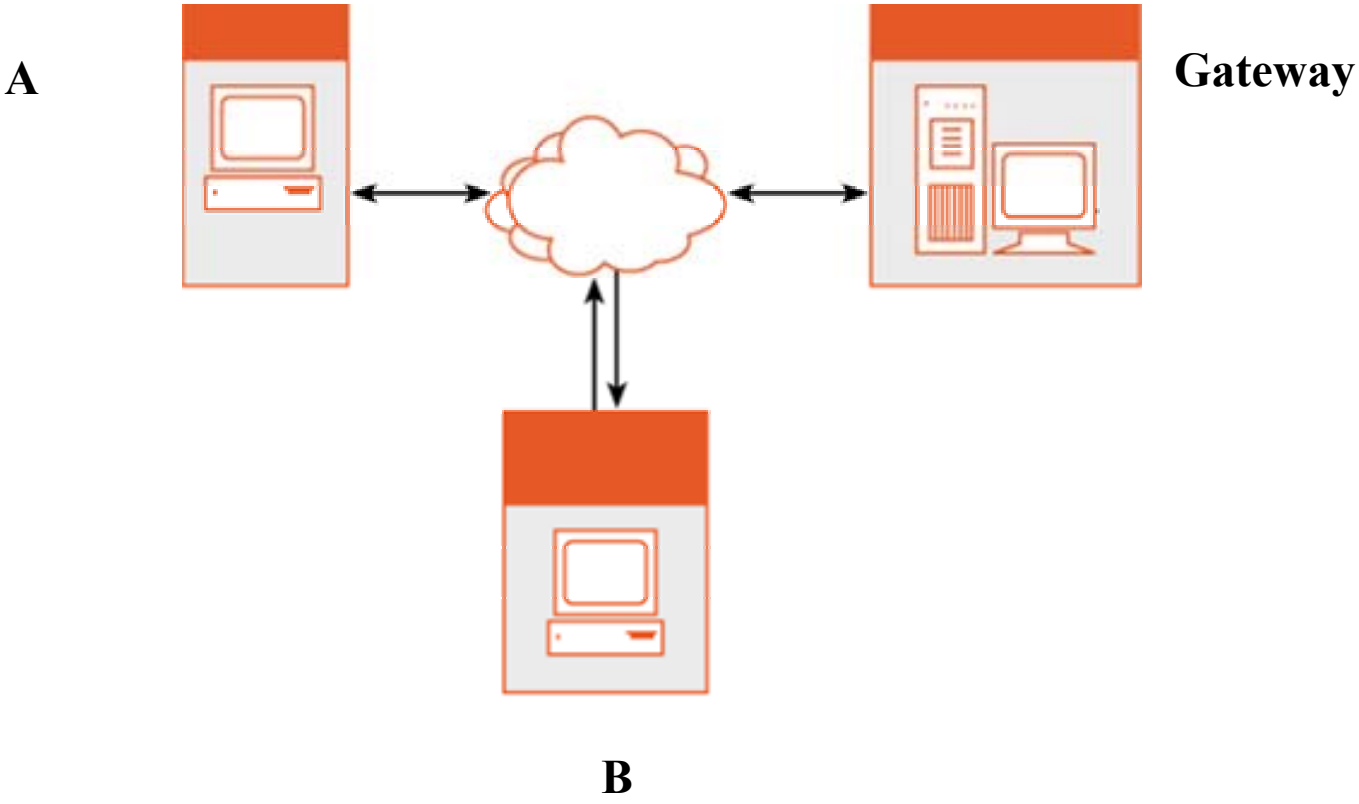


Hardware Type 1 = Ethernet; ProtocolType 0x0800 = IP; Operation 1 = Request, 2 = Reply; Source MAC and IP, then Target MAC and IP follow

ARP Cache Poisoning

- Client A requests MAC for IP 1.1.1.1
  - Client B replies “I am 1.1.1.1 with MAC 01:01:01:01:01:01” (broadcast)
  - Client C hears reply and caches
    - 1.1.1.1 → 01:01:01:01:01:01
- Unsolicited replies are also cached
  - Suppose gateway IP is 10.10.10.10 and A’s IP is 2.2.2.2
  - B tells A: 10.10.10.10 → 01:01:01:01:01:01
  - B tells gateway: 2.2.2.2 → 01:01:01:01:01:01
  - Note: these are unicast ARP_REPLYs

Man-in-the-Middle



***B** now proxies all traffic between **A** and the outside world*

Tools: Ettercap

- Ettercap is a freely-available tool that does ARP cache poisoning for you
  - I had a grad student do his thesis on this topic
  - It was easy to set up and use
  - Handles SSH as well
    - Uses OpenSSL library

Defenses

- Static ARP tables
  - Administrative headache
  - Doesn’t scale
- ARPWatch
  - Watches all traffic and detects anomolies
  - But only alerts admin after an attack has already occurred
  - Sometimes generates false positives

Using Cryptography

- AuthARP (Hector Urtubia)
  - Each client must sign replies with a public key
  - Unapproved users cannot issue ARP_REPLYs
  - Downside: PKI

DNS: Domain Name System

- Already covered this service (roughly)
- Distributed database mapping names to IP addresses
  - 13 root servers
  - locally cached like ARP
  - Recursive algorithm:
    - If colorado.edu doesn't know, ask edu, if they don't know, ask a root server

DNS: Security

- BIND
  - Berkeley DNS implementation
  - Ubiquitous
  - History of bugs
- Even without vulnerabilities, DNS is a flawed protocol
  - No authentication
  - Spoofing not too hard

Unsolicited Replies Not Accepted

- Can’t just send a DNS record to a client who did not request it

- But we CAN send a reply to a client who DID request it
  - Problems: we have to know the request was made
    - Not too hard if we control origin of the request (eg, a web page)
    - Not too hard if we can sniff local network
  - Problems: we have to throttle legitimate replier

DNS Spoofing

- A requests www.x.com
  - Local DNS server may have it cached, or may not; if cached, replies to A
  - Evil host (on local network) throttles DNS server
    - Ping of death, DoS, overflows, etc
    - Evil host answers for DNS server, redirecting A to bad IP address

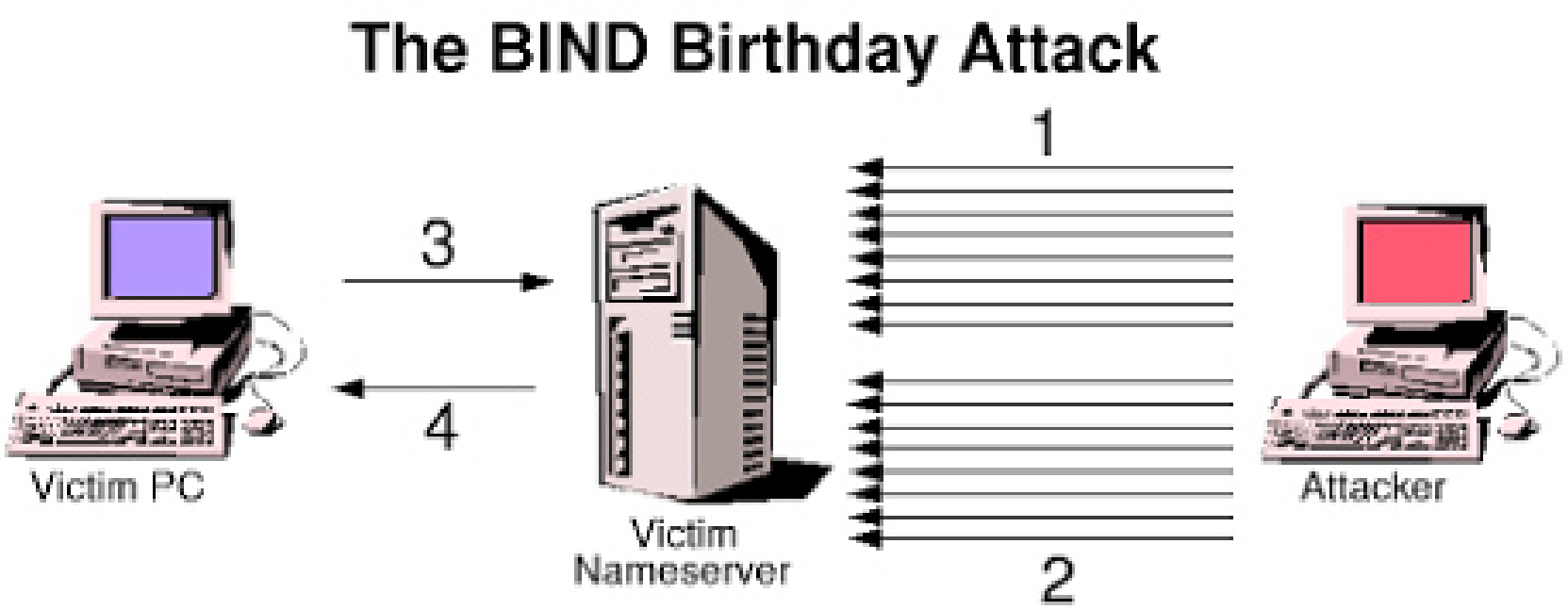
Remote Attacks

- You visit www.evil.com, which has a legitimate link to www.amazon.com
  - evil.com then throttles you DNS server and spoofs
  - evil.com knows you're waiting for a resolution for amazon.com
- Doesn't always work:
  - Sequence numbers are used, and they are sniffable on a LAN, but not remotely
    - They used to be sequential (thus easy to guess) but now they are randomized
    - Makes remote attacks much harder

Remote DNS Poisoning

- Attack a local nameserver
  - Send hundreds of requests to a victim nameserver for the same (bogus) name, bogus.com
    - nameserver must ask someone else, since he won't have this cached
  - Send hundreds of replies for bogus.com
    - Problem: sequence numbers of nameserver's help requests much be matched
    - Answer: birthday phenomenon
      - Random numbers aren't that random, which helps
      - Chance of a collision very high
  - Now users of this local nameserver will get the IP of your choice when asking for bogus.com

Remote DNS Poisoning



Step 1 - Attacker sends a large number of queries to the victim nameserver, all for the same domain name
Step 2 - Attacker sends spoofed replies giving fake answers for the queries it made
Step 3 - At a later time, victim PC sends a request for the spoofed domain name
Step 4 - Victim nameserver returns fake information to victim PC

DNSSEC

- DNSSEC is a project to have a central company, Network Solutions, sign all the .com DNS records. Here's the idea, proposed in 1993:

- Network Solutions creates and publishes a verification key. (They are the CA)
- Each *.com creates a key and signs its own DNS records. Yahoo, for example, creates a key and signs the yahoo.com DNS records under that key.
- Network Solutions signs each *.com key. Yahoo, for example, gives its cert to Network Solutions, and Network Solutions signs a document identifying that key as the yahoo.com key.
- Computers around the Internet are given the Network Solutions key, and begin rejecting DNS records that aren't accompanied by the appropriate signatures.
- As of November 2002, Network Solutions simply isn't doing this. There is no Network Solutions key. There are no Network Solutions *.com signatures.

DNSSEC

- On the table for over 10 years now; as of 2002:

  We are still doing basic research on what kind of data model will work for dns security. After three or four times of saying "NOW we've got it, THIS TIME for sure" there's finally some humility in the picture... "wonder if THIS'll work?" ... It's impossible to know how many more flag days we'll have before it's safe to burn ROMs that marshall and unmarshall the DNSSEC related RR's, or follow chains trying to validate signatures. It sure isn't plain old SIG+KEY, and it sure isn't DS as currently specified. When will it be? We don't know. What has to happen before we will know? We don't know that either. ...

  2535 is already dead and buried. There is no installed base. We're starting from scratch.

- BIND 9 was released earlier this year with DNSSEC disabled…