Computer security: certification

Frans Kaashoek
6.033 Spring 2007
How confidential is traffic in this lecture room?

- sudo tcpdump -s 0 -Ai en1
  - Complete trace of all packets on wirelessc3d4
    - c3d4 a1b2 0002 0004 0000 0000
  - You shouldn’t do this

- Example:
  13:57:53.794429 IP 18.188.69.36.mdns >
  (367)
Example Data inside packet

GET /tracking/tracking.cgi?tracknum=1Z1836810375022812
HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shock wave-flash, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, */*
Accept-Language: en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322; InfoPath.1)
Host: wwwapps.ups.com
Connection: Keep-Alive
URLs are visible in Referer and in the GET command.
Denning-Sacco Attack

- Assumes that the attacker has recorded a previous session, and compromised the connection key $K_x$ used in that one.

\[
A \rightarrow B: \{K_x, A\}K_b \text{ attacker replayed old message}
\]

\[
B \rightarrow A: \{N_b\}K_x
\]

\[
A \rightarrow B: \{N_{b-1}\}K_x \text{ forged by attacker}
\]

- $B$ now believes he shares a fresh secret key $K_x$ with $A$.

- **Denning-Sacco moral:** use a timestamp (calendar clock value) to detect replay of old messages.
Research into Video Streaming for DP2?
GMail is not encrypted by default

- Passed in the clear:
  - Contacts lists
  - GCalendar events

- GZipped text
  - Inbox entries
  - Mail messages

["112677a23fed4887",0,0,"12:58 pm","\u003cspan id="upro_rms@gnu.org\"\">Richard Stallman\u003c/span\">","&nbsp;","[csail-related] Thwart big brother--trade charlie cards. 13:45 Tuesday at rm 381","I have a charlie card with zero value currently stored on on it which I used for a couple of...",["",",","112677a23fed4887",0,"Mon May 7 2007_12:58 PM",0,"",0,0,1]

Hint: Change the GMail URL to https://!
IChat is Plaintext

• `strings log.dump | grep ichatballoon | cut -d\> -f 4-

A: it's just better not to reveal personal information
B: why?
A: I dunno, identity theft and stuff
B: oh, okay
A: maybe I just won't worry about it
UK hacker 'should be extradited'

UK hacker Gary McKinnon should be recommended for extradition to the US, a district judge has ruled.

The decision means Mr McKinnon will face trial in America for what the US has called "the biggest military hack of all time".

Although he has admitted hacking US military networks, Mr McKinnon said he was motivated by curiosity not malice.

just whack it out across the systems. Unfortunately for them, the local system administrator's password was blank. So you don't even need to become the domain administrator. That's 5,000 machines all with a blank system level administrator password. To be fair to them, as I got deeper into it, they closed me down pretty quickly.
Authentication logic (p 11-83)

1. Delegation of authority:
   - If A says (B speaks for A) \(\Rightarrow\) B speaks for A

2. Use of delegated authority:
   - If B speaks for A and B says (A says X) \(\Rightarrow\) A says X

3. Chaining of delegation
   - If B speaks for A and A speaks for C \(\Rightarrow\) B speaks for C
Example

0. \( \{A: M\}_{K_{Apriv}} \)
   if verify( ..., \( K_{Apub} \)) accepts then:

1. \( K_{Apriv} \) says A says M
   if \( K_{Apriv} \) speaks for \( K_{Apub} \), apply rule 3:

2. \( K_{Apub} \) says A says M
   if \( K_{Apub} \) speaks for A, apply rule 2:

3. A says M
   does \( K_{Apub} \) speak for A?
1. \{K_{A_{pub}} \text{ speaks for } A\}_{K_{MIT_{priv}}} 
   \text{ if verifies with } K_{MIT_{pub}}

2. K_{MIT_{priv}} \text{ says } K_{A_{pub}} \text{ speaks for } A 
   \text{ if } K_{MIT_{priv}} \text{ speaks for } K_{MIT_{pub}}

3. K_{MIT_{pub}} \text{ says } K_{A_{pub}} \text{ speaks for } A 
   \text{ if } K_{MIT_{pub}} \text{ speaks for MIT}

4. MIT \text{ says } K_{A_{pub}} \text{ speaks for } A 
   \text{ if } MIT \text{ speaks for } A

5. K_{A_{pub}} \text{ speaks for } A