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:
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 Kx used in that one.

  A -> B: {Kx, A}Kb attacker replayed old message

  B -> A: {Nb}Kx
  A -> B: {Nb-1}Kx forged by attacker

- B now believes he shares a fresh secret key Kx 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

"Richard Stallman" Thwart big brother--trade charlie cards. 13:45 Tuesday at rm 381","I have a charlie card with zero value currently stored on it which I used for a couple of &hellip;","["112677a23fed4887",0,0,"12:58 pm","\u003cspan id\u003d"_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 it which I used for a couple of &hellip;","["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
QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.

QuickTime™ and a
TIFF (Uncompressed) decompressor
are needed to see this picture.
Authentication logic (p 11-83)

• 1. Delegation of authority:
  – If A says (B speaks for A) ⇒ B speaks for A

• 2. Use of delegated authority:
  – If B speaks for A and B says (A says X) ⇒ A says X

• 3. Chaining of delegation
  – If B speaks for A and A speaks for C ⇒ 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_{Apub} \text{ speaks for } A\}_{K_{MIT\text{priv}}}
   \quad \text{if verifies with } K_{MIT\text{pub}}

2. \(K_{MIT\text{priv}}\) says \(K_{Apub}\) speaks for \(A\)
   \quad \text{if } K_{MIT\text{priv}} \text{ speaks for } K_{MIT\text{pub}}

3. \(K_{MIT\text{pub}}\) says \(K_{Apub}\) speaks for \(A\)
   \quad \text{if } K_{MIT\text{pub}} \text{ speaks for } \text{MIT}

4. \text{MIT says } K_{Apub} \text{ speaks for } A
   \quad \text{if MIT speaks for } A

5. \(K_{Apub}\) speaks for \(A\)