Computer security: certification

6.033 Spring 2007

How confidential is traffic in this lecture room?

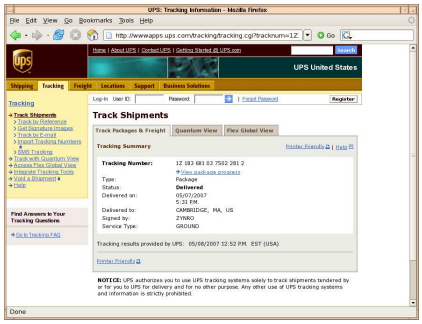
- sudo tcpdump -s 0 -Ai en1
  - Complete trace of all packets on wirelessc3d4
    - c3d4 a1b2 0002 0004 0000 0000
  - You shouldn't do this
- Example:

13:57:53.794429 IP 18.188.69.36.mdns > 224.0.0.251.mdns: 0 [4a] [4q] SRV? Ben's music._daap._tcp.local. TXT? Ben's music._daap._tcp.local. A? ben-powerbook-g4-15.local. AAAA? ben-powerbook-g4-15.local. (367)

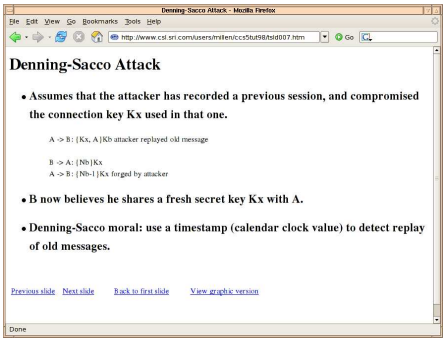
Example Data inside packet

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

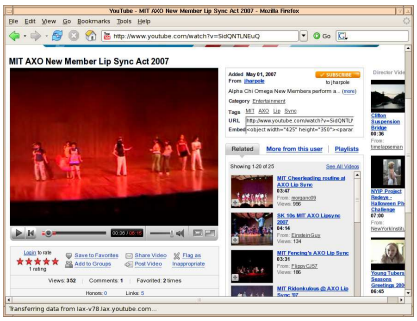
URLs are visible in Referer and in the GET command



Auxiliary Material for Lecture



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

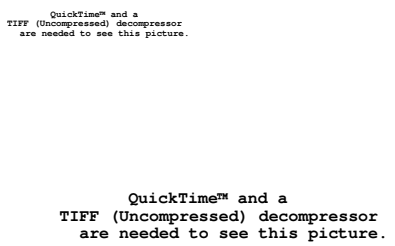

```
["112677a23fed4887",0,0,"12:58 pm","\u003cspan
id\u003d\"_upro_rms@ gnu.org\"\>Richard
Stallman\u003c/span\>"," ","[csail-
related] Thwart big brother--trade charlie
cards. 13:45 Tuesday at rm 381","I have a
charlie card with zero value currently stored
on on it which I used for a couple of
&hellip;",[],"","112677a23fed4887",0,"Mon 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.

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. $\{K_{Apub}$ speaks for A$\}_{KMITpriv}$
if verifies with K_{MITpub}

2. $K_{MITpriv}$ says K_{Apub} speaks for A
if $K_{MITpriv}$ speaks for K_{MITpub}

3. K_{MITpub} says K_{Apub} speaks for A
if K_{MITpub} speaks for MIT

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

5. K_{Apub} speaks for A