

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 >
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

The screenshot shows a Mozilla Firefox browser window titled "UPS: Tracking Information - Mozilla Firefox". The address bar contains the URL: `http://wwwapps.ups.com/tracking/tracking.cgi?tracknum=1Z:1836810375022812`. The page content includes the UPS logo, navigation tabs (Shipping, Tracking, Freight, Locations, Support, Business Solutions), a search bar, and a tracking summary for a delivered package.

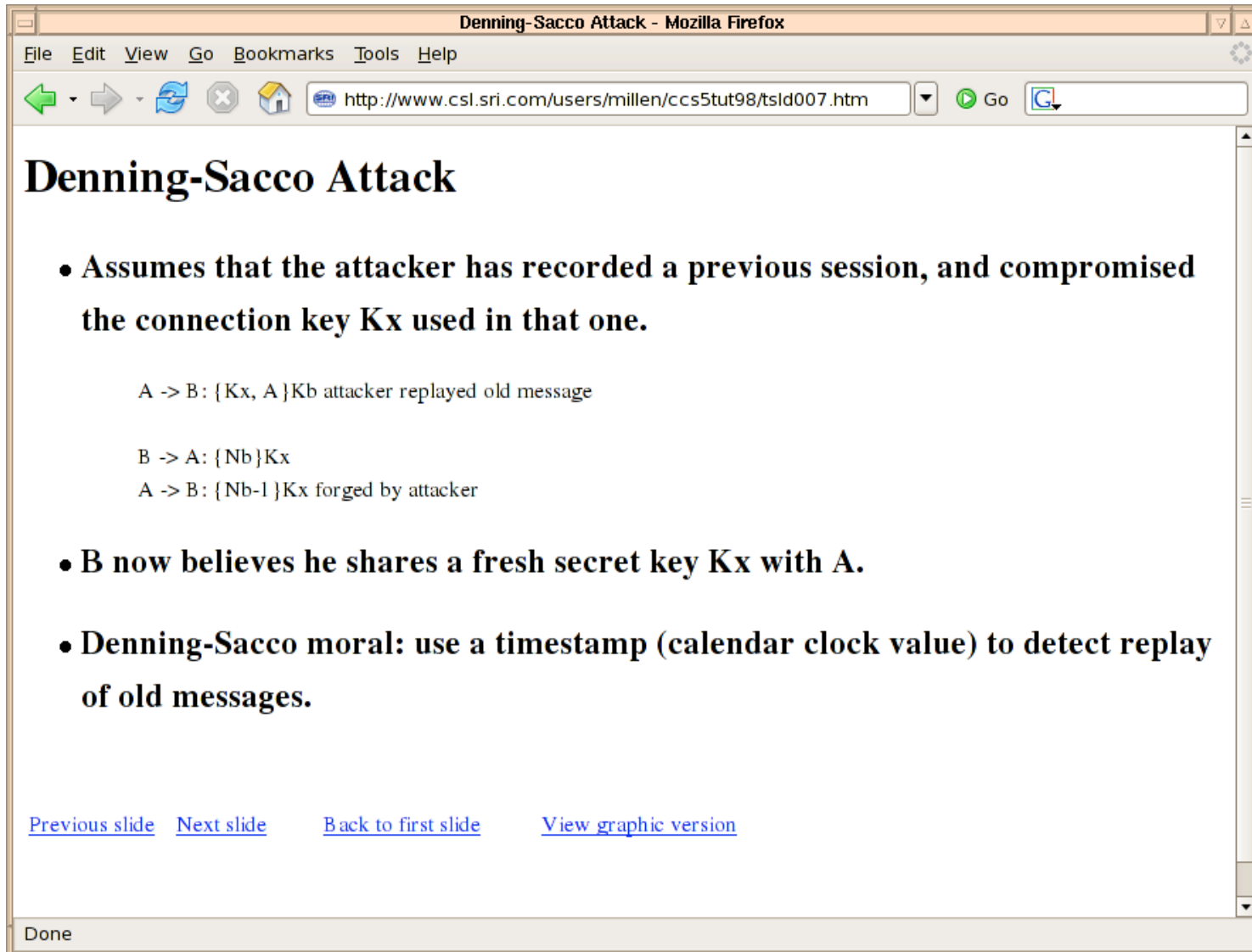
Tracking Summary

Tracking Number:	1Z 183 681 03 7502 281 2
Type:	Package
Status:	Delivered
Delivered on:	05/07/2007 5:31 P.M.
Delivered to:	CAMBRIDGE, MA, US
Signed by:	ZYNRO
Service Type:	GROUND

Tracking results provided by UPS: 05/08/2007 12:52 P.M. EST (USA)

NOTICE: UPS authorizes you to use UPS tracking systems solely to track shipments tendered by or for you to UPS for delivery and for no other purpose. Any other use of UPS tracking systems and information is strictly prohibited.

Auxiliary Material for Lecture



The image shows a screenshot of a Mozilla Firefox browser window. The title bar reads "Denning-Sacco Attack - Mozilla Firefox". The address bar contains the URL "http://www.csl.sri.com/users/millen/ccs5tut98/tsld007.htm". The main content area displays a slide titled "Denning-Sacco Attack" with the following text:

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

Below the bullet point, the following messages are listed:

A \rightarrow B: $\{K_x, A\}_{K_b}$ attacker replayed old message

B \rightarrow A: $\{N_b\}_{K_x}$

A \rightarrow B: $\{N_{b-1}\}_{K_x}$ 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.

At the bottom of the slide, there are four blue hyperlinks: "Previous slide", "Next slide", "Back to first slide", and "View graphic version". The status bar at the bottom of the browser window shows "Done".


Research into Video Streaming for DP2?

YouTube - MIT AXO New Member Lip Sync Act 2007 - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

http://www.youtube.com/watch?v=SidQNTLNEuQ

MIT AXO New Member Lip Sync Act 2007



Added May 01, 2007 From [jharpole](#) to jharpole

Alpha Chi Omega New Members perform a... [\(more\)](#)

Category [Entertainment](#)

Tags [MIT](#) [AXO](#) [Lip](#) [Sync](#)

URL <http://www.youtube.com/watch?v=SidQNTLNEuQ>

Embed `<object width="425" height="350"><param`

Director Video

[Clifton Suspension Bridge](#)
00:36
From: [timelapseman](#)

[NYIP Project Redeye - Halloween Ph Challenge](#)
07:00
From: [NewYorkInstitu](#)

[Young Tubers Seasons Greetings 200](#)
06:45

Related [More from this user](#) [Playlists](#)

Showing 1-20 of 25 [See All Videos](#)

- [MIT Cheerleading routine at AXO Lip Sync](#)
03:47
From: [morganc09](#)
Views: 956
- [SK 10s MIT AXO Lipsync 2007](#)
04:14
From: [EinsteinGuy](#)
Views: 134
- [MIT Fencing's AXO Lip Sync](#)
03:31
From: [FlippyCJ57](#)
Views: 186
- [MIT Ridonkulus @ AXO Lip Sync '07](#)

[Login](#) to rate

★ ★ ★ ★ ★
1 rating

[Save to Favorites](#) [Share Video](#) [Flag as Inappropriate](#)

[Add to Groups](#) [Post Video](#)

Views: 352 | Comments: 1 | Favorited: 2 times

Honors: 0 Links: 5

Transferring data from lax-v78.lax.youtube.com...

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 \>","&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 &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

Last Updated: Wednesday, 10 May 2006, 12:06 GMT 13:06 UK

[E-mail this to a friend](#)

[Printable version](#)

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.



Mr McKinnon could face a lengthy jail sentence in the US

[▶ VIDEO](#) [McKinnon's reaction](#)

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 $\text{verify}(\dots, K_{Apub})$ 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. $\{K_{A_{pub}} \text{ speaks for } A\}_{K_{MIT_{priv}}}$
if verifies with $K_{MIT_{pub}}$
2. $K_{MIT_{priv}}$ says $K_{A_{pub}}$ speaks for A
if $K_{MIT_{priv}}$ speaks for $K_{MIT_{pub}}$
3. $K_{MIT_{pub}}$ says $K_{A_{pub}}$ speaks for A
if $K_{MIT_{pub}}$ speaks for MIT
4. MIT says $K_{A_{pub}}$ speaks for A
if MIT speaks for A
5. $K_{A_{pub}}$ speaks for A