

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 /mword, */*

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=1Z1836810375022812`. The page content includes a navigation menu with options like "Shipping", "Tracking", "Freight", "Locations", "Support", and "Business Solutions". A "Tracking" sidebar is visible on the left. The main content area is titled "Track Shipments" and displays a "Tracking Summary" for a package with tracking number 1Z 183 681 03 7502 281 2. The status is "Delivered" on 05/07/2007 at 5:31 P.M. in Cambridge, MA, US. A notice at the bottom states: "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."

UPS: Tracking Information - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

[Home](#) | [About UPS](#) | [Contact UPS](#) | [Getting Started @ UPS.com](#)

UPS United States

Shipping Tracking Freight Locations Support Business Solutions

Tracking

Log-In User ID: Password: [Forgot Password](#)

Track Shipments

Track Packages & Freight

Tracking Summary

[Printer Friendly](#) | [Help](#)

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

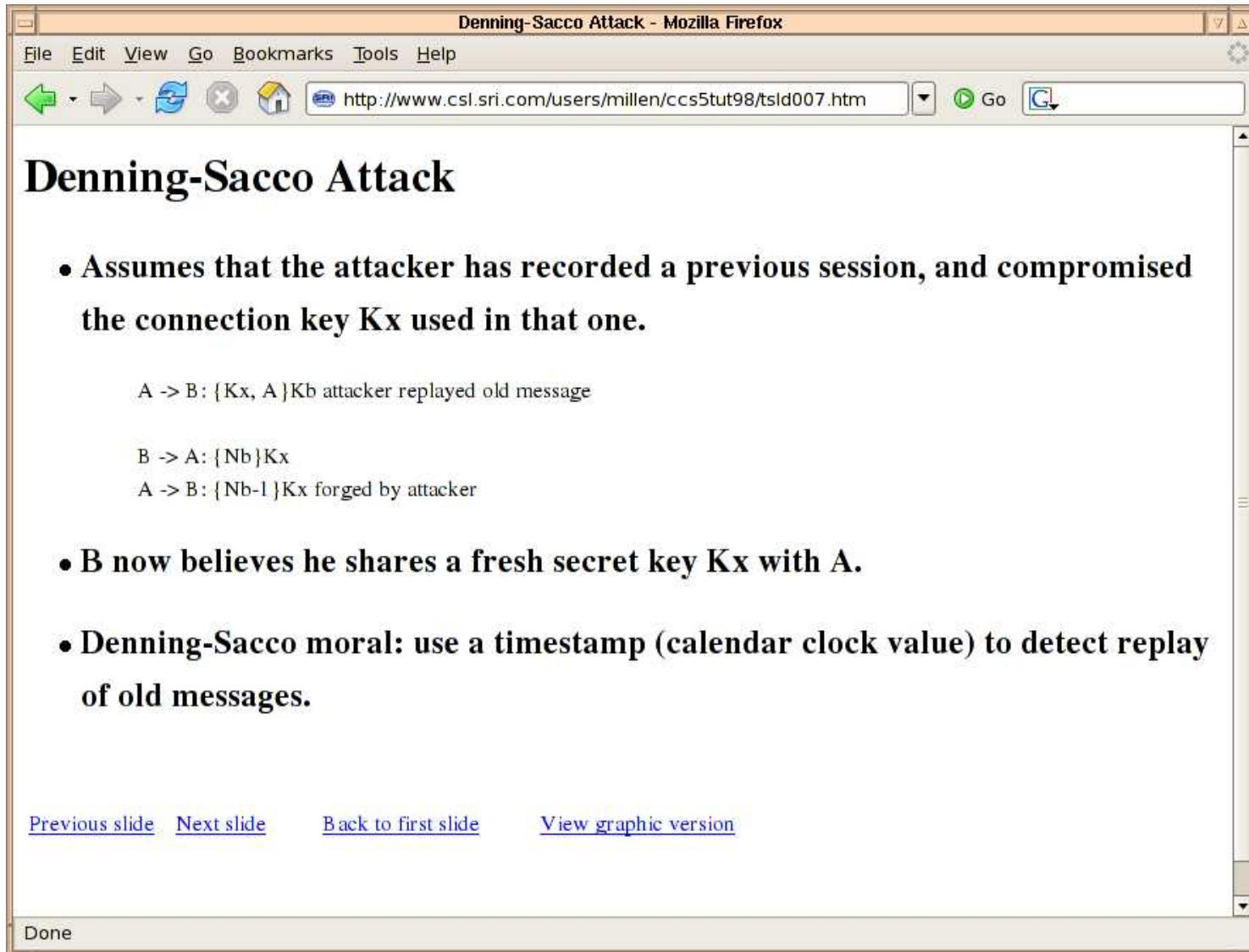
Tracking results provided by UPS: 05/08/2007 12:52 P.M. EST (USA)

[Printer Friendly](#)

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.

Done

Auxiliary Material for Lecture



The screenshot shows a Mozilla Firefox browser window with the title "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 the following text:

Denning-Sacco Attack

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

A -> B: $\{K_x, A\}K_b$ attacker replayed old message

B -> A: $\{N_b\}K_x$

A -> 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.**

Navigation links: [Previous slide](#) [Next slide](#) [Back to first slide](#) [View graphic version](#)

Done

Research into Video Streaming for DP2?

The screenshot shows a Mozilla Firefox browser window displaying a YouTube video. The video title is "MIT AXO New Member Lip Sync Act 2007". The video player shows a group of performers on a stage with red lighting. The video progress bar indicates 00:36 / 06:16. Below the video player, there are options to login to rate, save to favorites, share video, and flag as inappropriate. The video has 1 rating, 352 views, 1 comment, and 2 favorites. To the right of the video player, there is a metadata section with the following information:

- 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"><par`

Below the metadata section, there are tabs for "Related", "More from this user", and "Playlists". The "Related" tab is selected, showing a list of 25 related videos. The first few videos are:

- [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 Ridonkulous @ AXO Lip Sync '07](#)

On the right side of the page, there is a "Director Vide" section with a video thumbnail and a "Clifton Suspension Bridge" video with a duration of 00:36. Below that, there is a "NYIP Project Redeye - Halloween Ph Challenge" video with a duration of 07:00. At the bottom of the page, there is a "Young Tubers Seasons Greetings 200" video with a duration of 06:45.

At the bottom of the browser window, there is a status bar that says "Transferring data from lax-v78.lax.youtube.com..."

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) \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. $\{K_{Apub} \text{ speaks for } A\}_{K_{MITpriv}}$
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