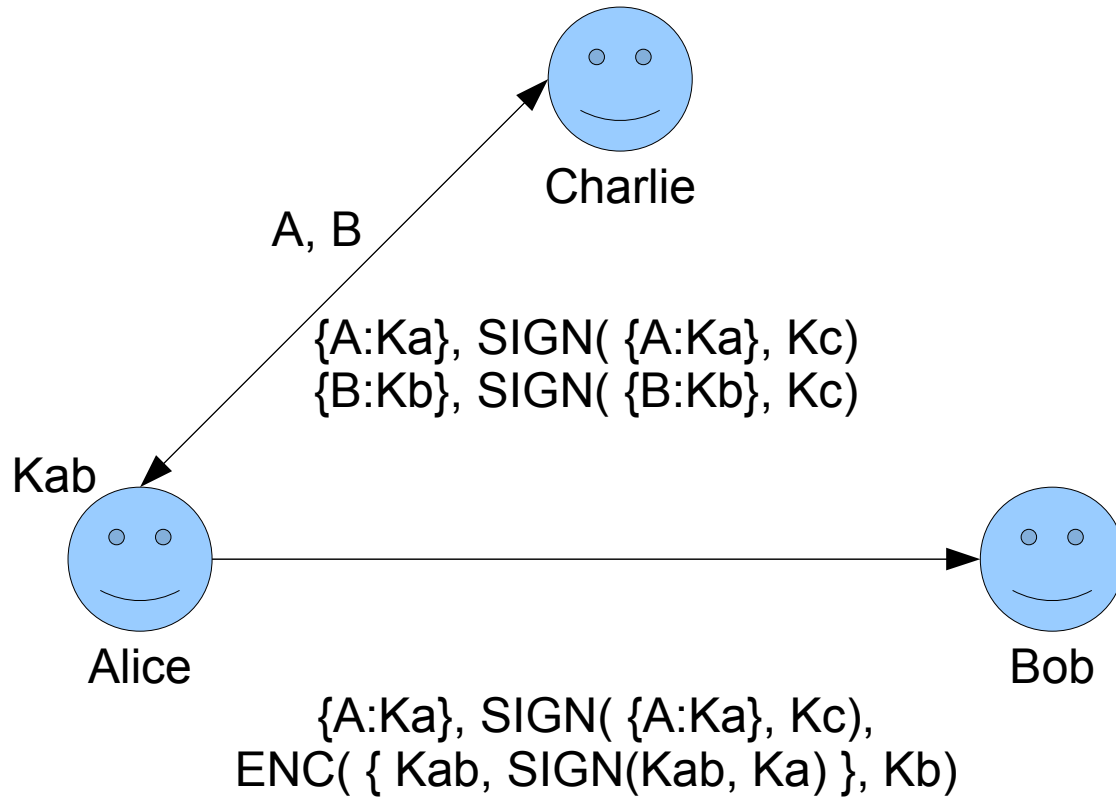


6.033 Lecture 24
Protocols and Authorization

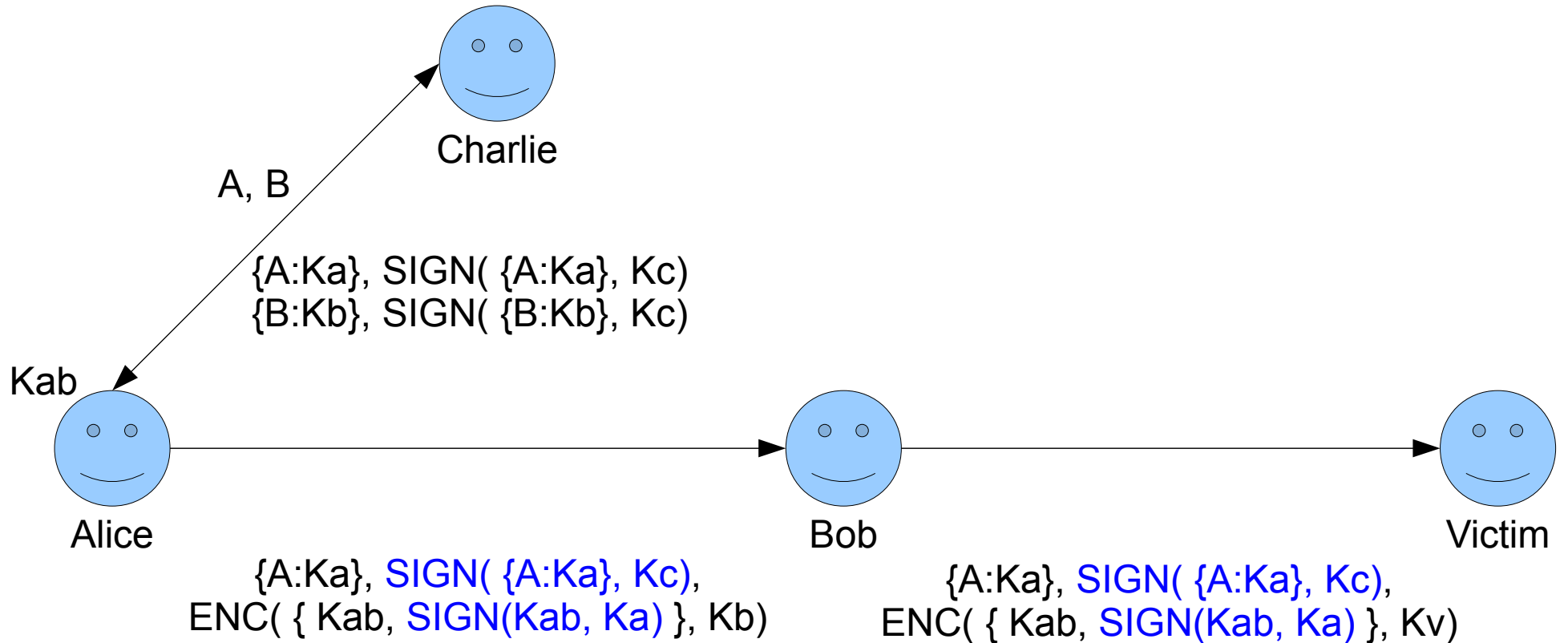
Nickolai Zeldovich

Spring 2009

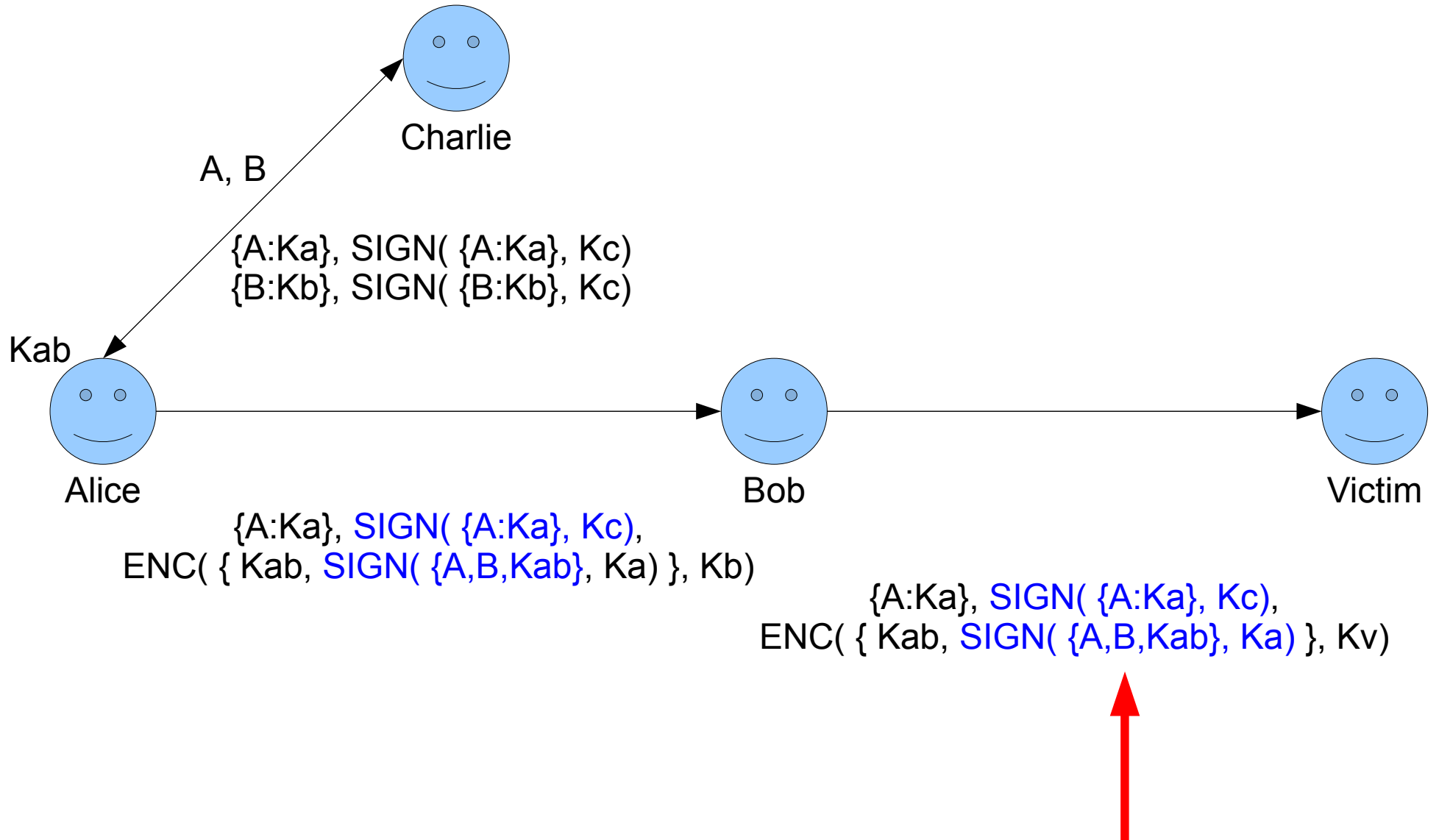
Denning-Sacco Protocol





Denning-Sacco Protocol



Denning-Sacco Protocol





public key client 

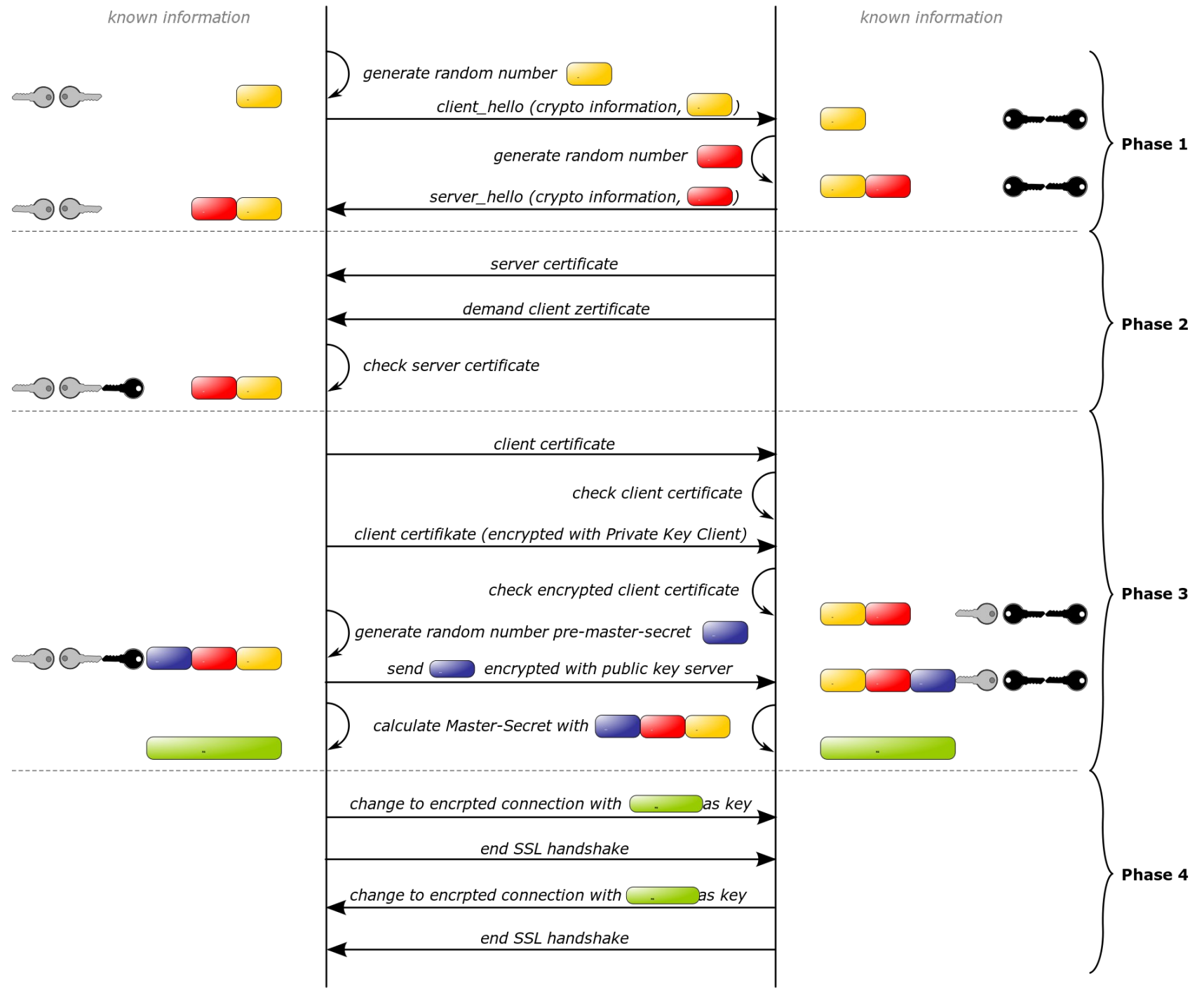
private key client 

Client

Server

 public key server

 private key server



How confidential is traffic in this lecture room?

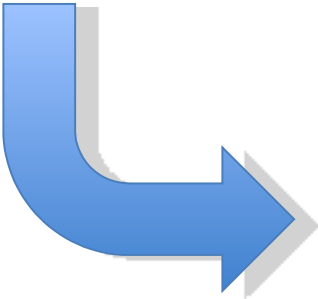
- `sudo tcpdump -s 0 -Ai en1`
 - Complete trace of all packets on wireless network
 - You shouldn't do this
- 14:04:59.999646 IP HSI-KBW-091-089-230-121.hsi2.kabel-badenwuerttemberg.de.45843 > dhcp-18-111-20-195.dyn.mit.edu.39211: P 127234932:127234940(8) ack 4112680742 win 65429 <nop,nop,timestamp 6345692 18015400>

Example Data Inside a Packet

```
GET /6.033/2007/wwwdocs/ HTTP/1.1
User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_5_6; en-us) AppleWebKit/525.27.1 (KHTML, like Gecko)
Referer: http://mit.edu/6.033/2008/wwwdocs/schedule.html
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png;q=0.8
Accept-Language: en-us
Accept-Encoding: gzip, deflate
Connection: keep-alive
Host: mit.edu
```

Example Data Inside a Packet

GET /6.033/2007/wwwdocs/ HTTP/1.1
User-Agent: Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_5_6; en-us) AppleWebKit/525.27.1 (KHTML, like Gecko) Chrome/1.0.154.53
Referer: http://mit.edu/6.033/2008/wwwdocs/schedule.html
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/png;q=0.8
Accept-Language: en-us
Accept-Encoding: gzip, deflate
Connection: keep-alive
Host: mit.edu



HTTP/1.1 200 OK
Date: Wed, 29 Apr 2009 18:56:00 GMT
Server: MIT Web Server Apache/1.3.26 Mark/1.5 (Unix) mod_ssl/2.8.9 OpenSSL/0.9.7c
Last-Modified: Fri, 25 May 2007 17:15:48 GMT
ETag: "b884046-46a4-465719c4"
Accept-Ranges: bytes
Content-Length: 18084
Connection: close
Content-Type: text/html

<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
<title>6.033 / Spring 2007 / Welcome</title>
...

GMail is not encrypted by default

Passed in the clear:

- Contacts lists
- Calendar events

Gzipped text:

- Inbox entries
- Mail messages

```
["112677a23fed4887",0,0,"12:58 pm","\u003cspan  
id\u003d\"_upro_rms@gnu.org\">Richard  
Stallman\u003c/span>","\u0026nbsp;","\u003cspan  
[csail-related] Thwart  
big brother--trade charlie cards. 13:45 Tuesday at rm  
381","\u003cspan  
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 <http://> to <https://>

Facebook is Plaintext

(as is AIM, Google Docs, iChat, etc...)

```
{"name": "XX XXXX",  
"firstName": "XX",  
"thumbSrc": "XXX.jpg",  
"status": "says a man should  
always dress for the job he  
wants. So why am I dressed up  
like a pirate in this restaurant?  
It's all because some hacker  
stole my identity, now I sit  
here every evening serving  
chowder and iced tea.  
Should've gone to  
FreeCreditReport.com, I  
could've seen this coming at  
me like an atom bomb. They  
monitor your credit and send  
you e-mail alerts, so you don't  
end up selling fish to tourists in  
t-shirts.",  
"statusTime":1240674216,  
"statusTimeRel":"on Saturday",  
"enableVC":false}
```

The image shows a screenshot of a Facebook profile page. At the top, there is a navigation bar with the Facebook logo and links for Home, Profile, Friends, and an Inbox with 48 notifications. Below this, the profile header includes tabs for Wall, Info, Photos, and Boxes. A text box for 'What's on your mind?' is visible with a 'Share' button. The main content area shows a post from a friend with the text 'rudest mo ever, you look like you're off a beastie boys film clip.' Below the post is a 'RECENT ACTIVITY' section showing friend additions. At the bottom, there is a photo album titled 'Boston/Cambridge' with a 'View album' link.

Authentication Cookies

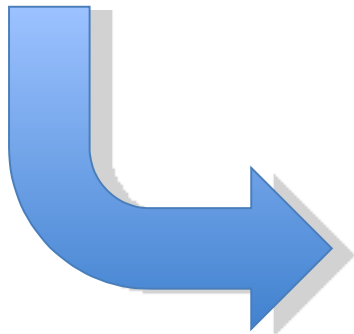
HTTP/1.1 200 OK

Set-Cookie: **CAL=XXXXXXXXXXXXX**;Domain=**www.google.com**;Path=/calendar;

Expires= Tue, 19-May-2009 18:23:37 GMT

Cache-Control: no-cache, no-store, max-age=0, must-revalidate

Pragma: no-cache



The screenshot shows the Google Calendar web interface. The browser address bar displays `http://www.google.com/calendar/render`. The page title is "Google Calendar BETA". The navigation bar includes links for "Gmail", "Calendar", "Documents", "Photos", "Reader", "Web", and "more". The user's email address is "cowling@gmail.com". The calendar is set to "Today" (May 3 - 9 2009). The view is "Week". The calendar grid shows events for the week of May 3-9, 2009. The events are:

Day	Event	Time
Sun 5/3		
Mon 5/4	Sniff traffic in 6.	6:00 - 6:30
Tue 5/5	Pick up shirts	6:00 - 6:30
Tue 5/5	Cinco de Mayo	6:00 - 6:30
Wed 5/6	Dan Myers in town	6:00 - 6:30
Thu 5/7		
Fri 5/8		
Sat 5/9		

The calendar grid also shows events for the week of May 10-16, 2009:

Day	Event	Time
Sun 5/10		
Mon 5/11		
Tue 5/12		
Wed 5/13		
Thu 5/14		
Fri 5/15		
Sat 5/16		

Authentication Cookies

HTTP/1.1 200 OK

Date: Mon, 04 May 2009 18:20:10 GMT

...

Set-Cookie: _twitter_sess=XXXXXXXXXXXX; domain=**.twitter.com**; path=/

HTTP/1.1 200 OK

Date: Mon, 04 May 2009 18:06:24 GMT

...

Set-Cookie: xs=XXXXXXXXXXXX; path=/; domain=**.facebook.com**;

HTTP/1.1 200 OK

Date: Mon, 04 May 2009 18:19:19 GMT

...

Set-Cookie: itsessionid=XXXXXXXXXXXX; path=/;
domain=**.analytics.yahoo.com**

etc etc etc