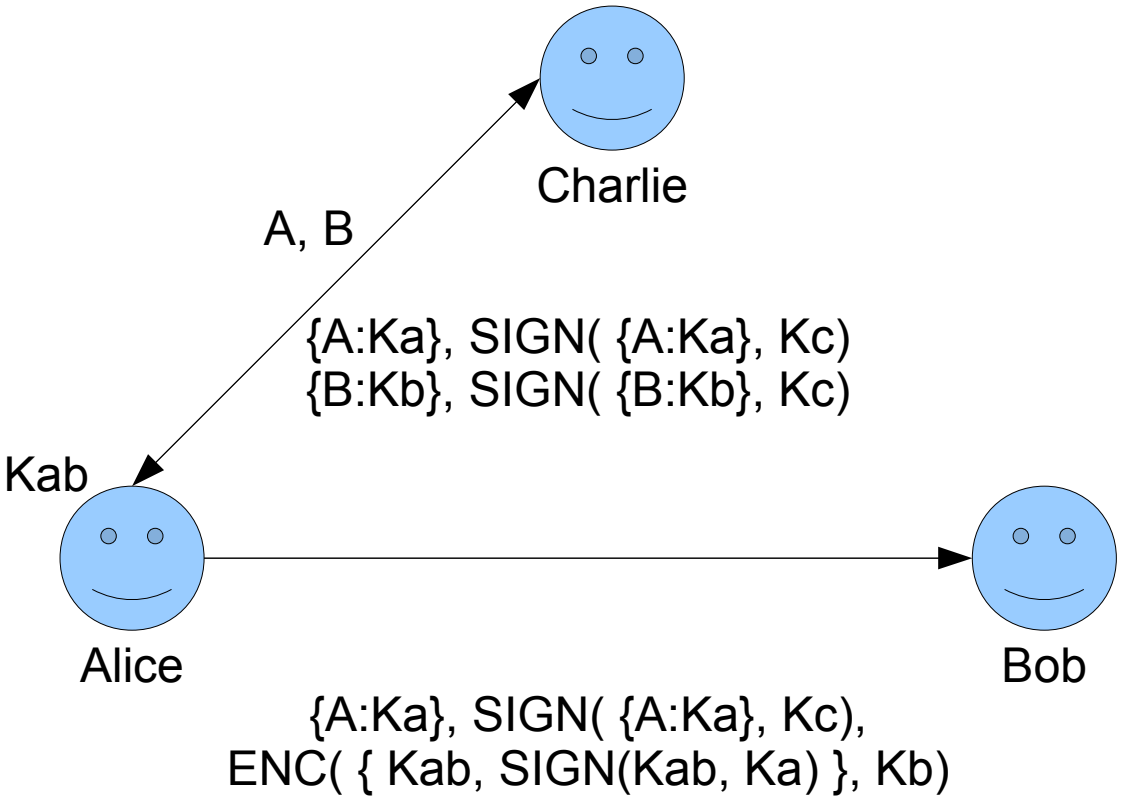
6.033 Lecture 24
Protocols and Authorization

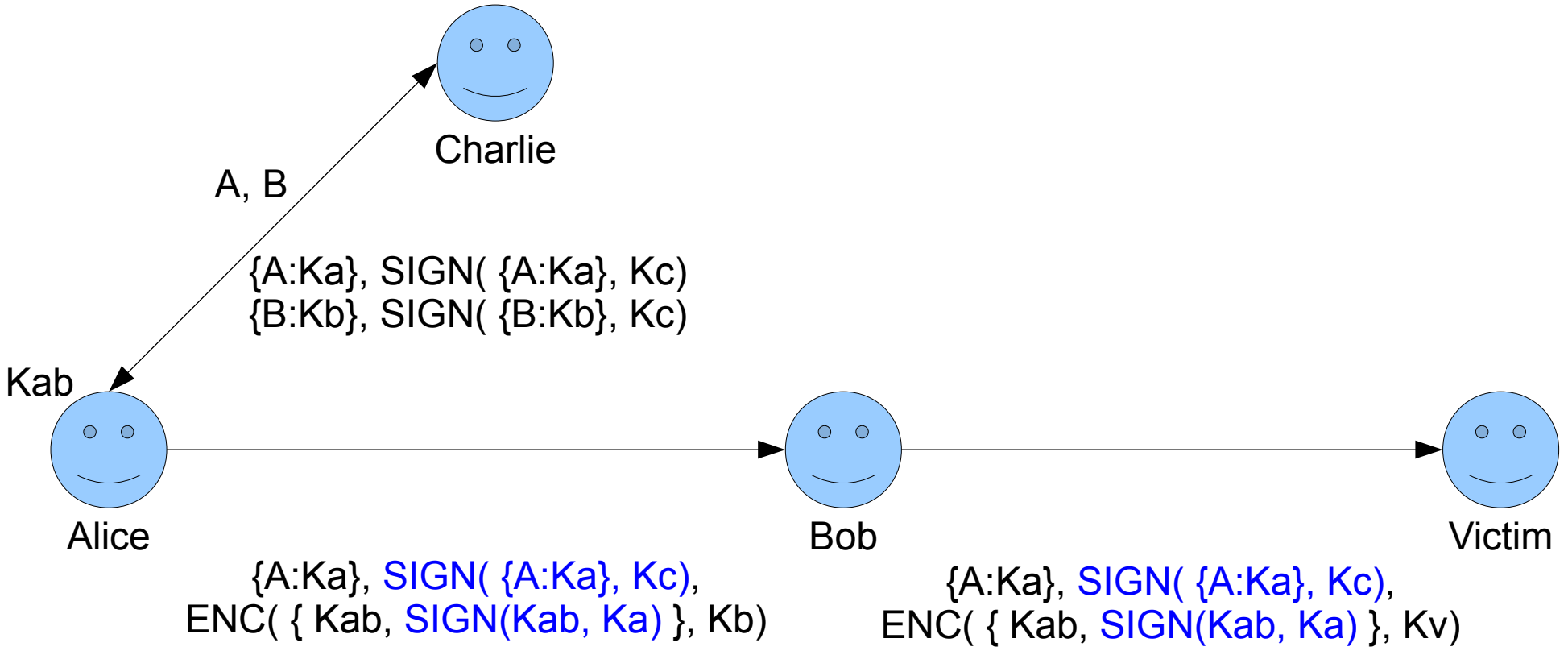
Nickolai Zeldovich

Spring 2009

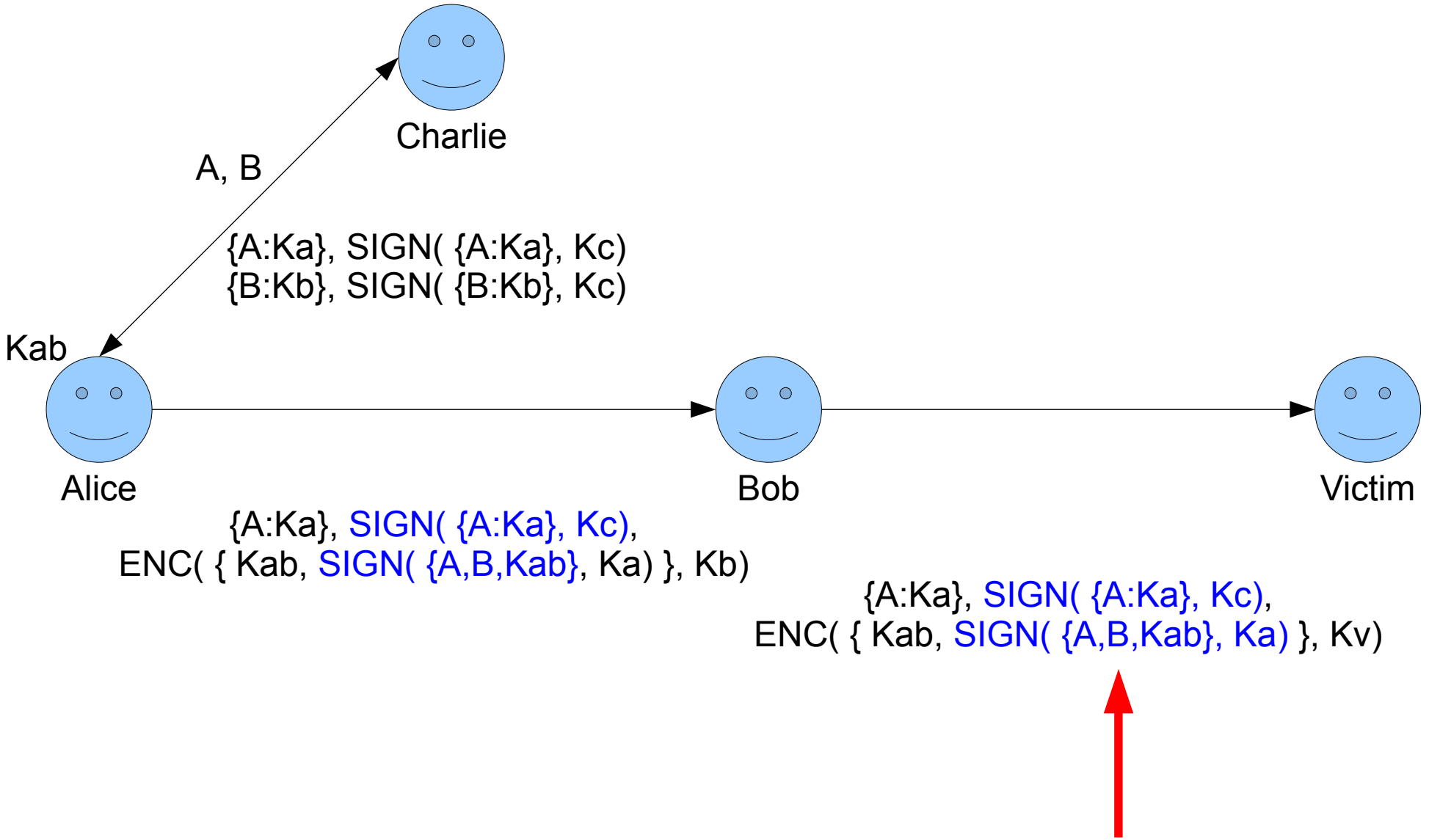
Denning-Sacco Protocol

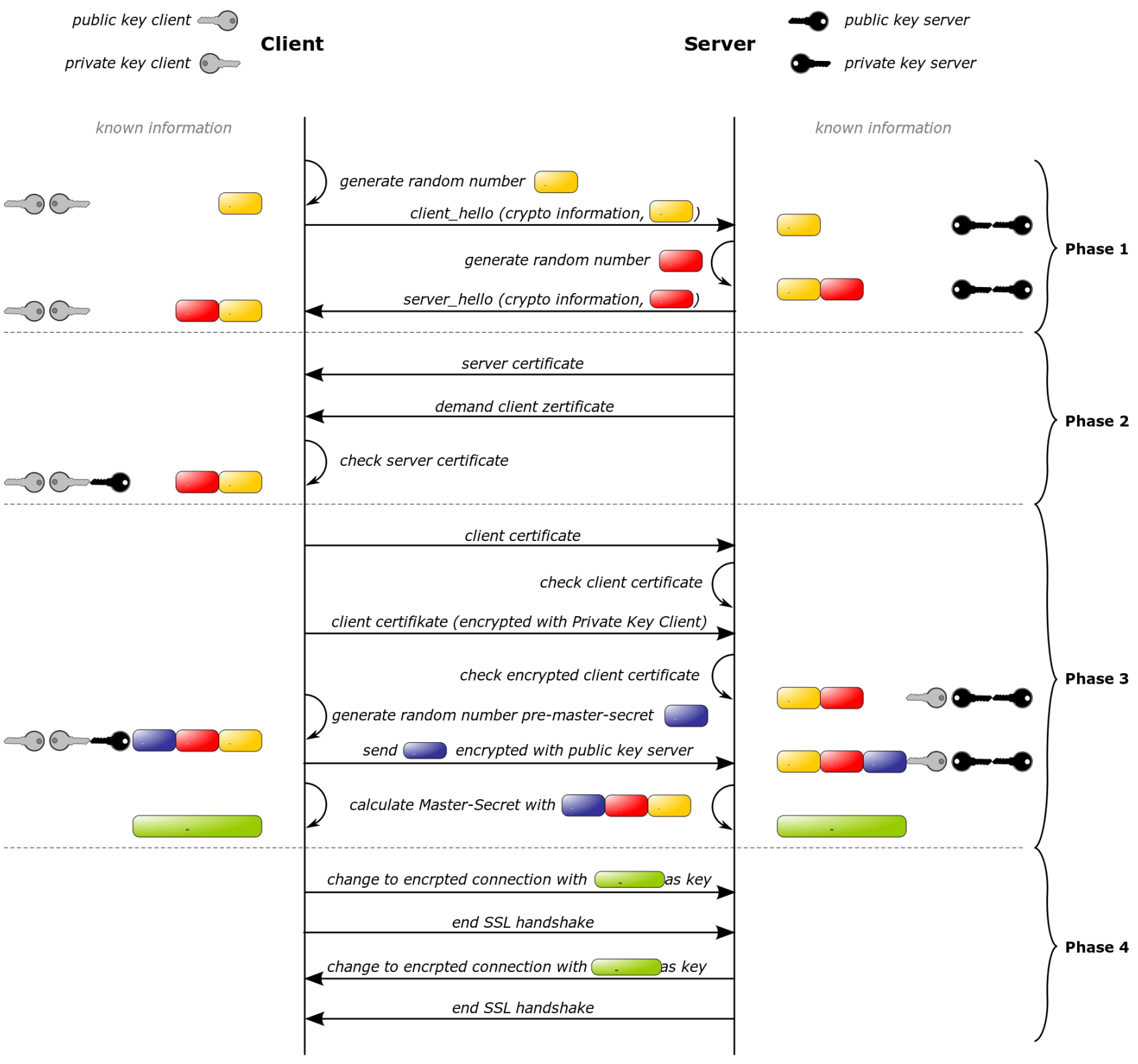


Denning-Sacco Protocol



Denning-Sacco Protocol




public key client
private key client
Client
Server
public key server
private key server
known information
known information
generate random number
client_hello (crypto information,)
generate random number
server_hello (crypto information,)
Phase 1
server certificate
demand client zertificate
check server certificate
Phase 2
client certificate
check client certificate
client certifikate (encrypted with Private Key Client)
check encrypted client certificate
generate random number pre-master-secret
send encrypted with public key server
calculate Master-Secret with
Phase 3
change to encrpted connection with as key
end SSL handshake
change to encrpted connection with as key
end SSL handshake
Phase 4

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

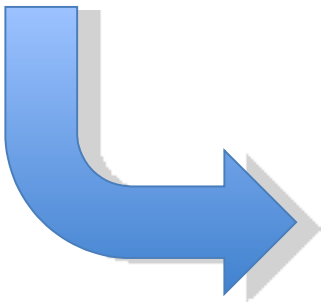
- 14:04:59.999646 IP HSI-KBW-091-089-230-121.hsi2.kabel-badenwuerttemberg.de.45843 > dhcp-18-111-20-195.dyn.mit.edu.39211: P 127234932:127234940(8) ack 4112680742 win 65429 <nop,nop,timestamp 6345692 18015400>

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 (KHT
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
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 (KH
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
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

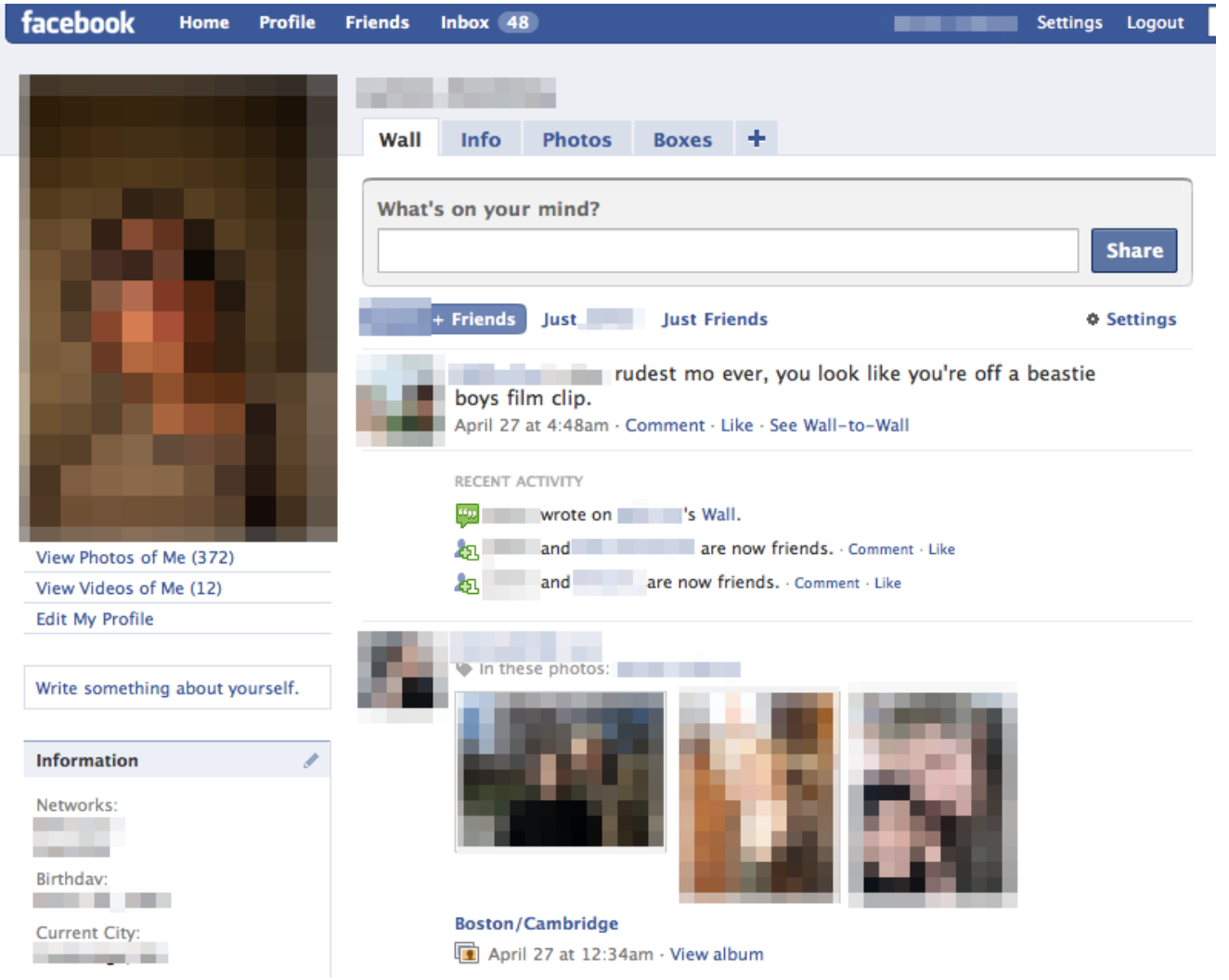
["112677a23fed4887",0,0,"12:58 pm","\u003cspan id\u003d\"_upro_rms@ gnu.org\"\>Richard Stallman\u003c/span\>"," ","[csail- related] Thwart big brother--trade charlie cards. 13:45 Tuesday at rm 381","I have a charlie card with zero value currently stored on on it which I used for a couple of …",[],"","112677a23fed4887",0,"Mon May 7 2007_12:58 PM",0,"",0,0,1]

Hint: Change http:// to https://

Facebook is Plaintext

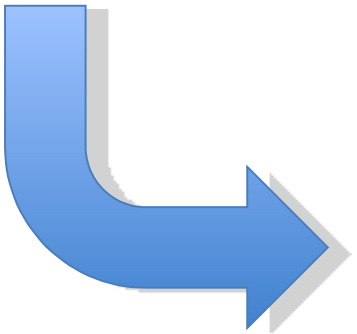
(as is AIM, Google Docs, iChat, etc…)

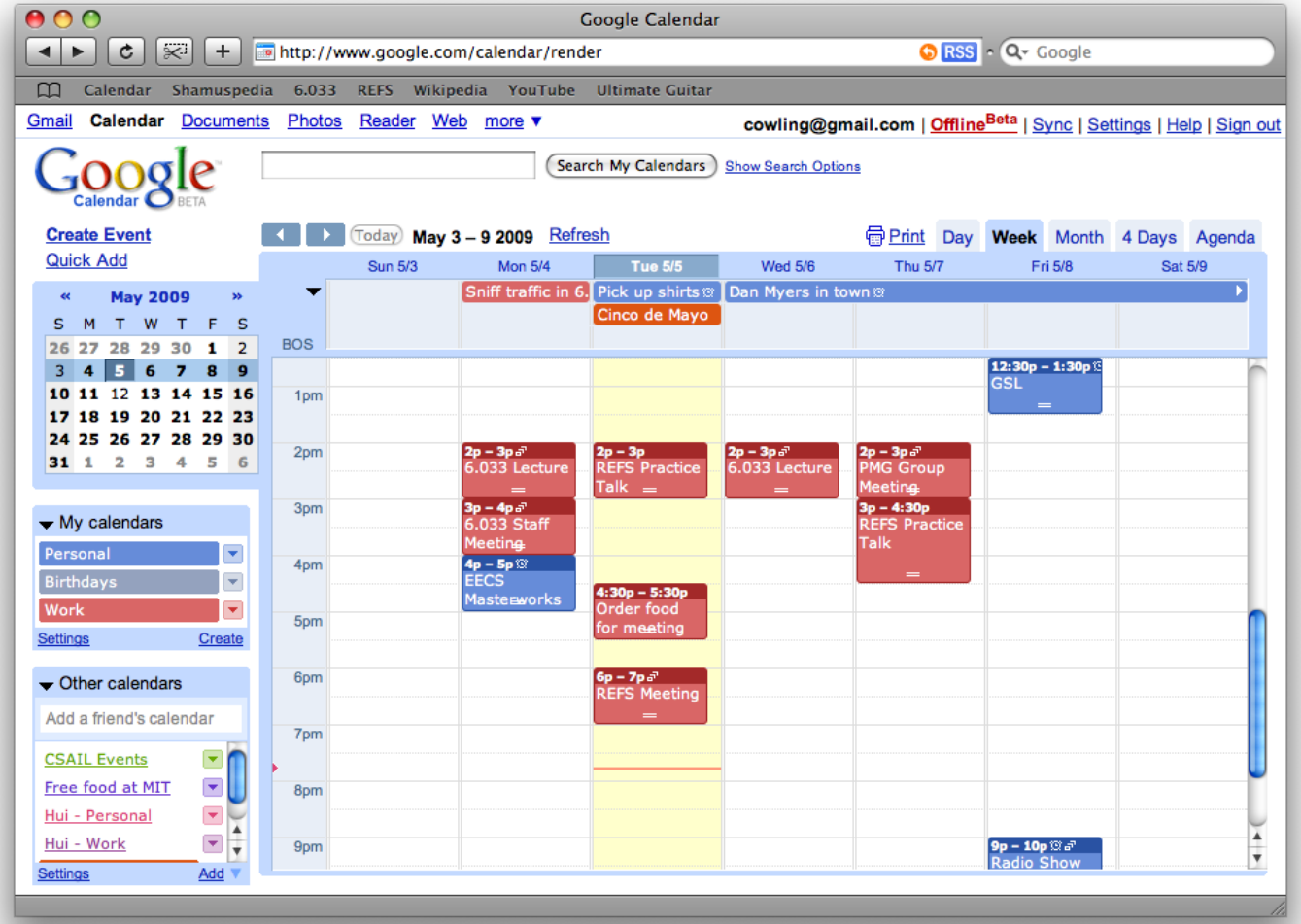
{"name": ”XX XXXX",
"firstName": ”XX",
"thumbSrc”: "XXX.jpg",
"status": "says a man should always dress for the job he wants. So why am I dressed up like a pirate in this restaurant? It's all because some hacker stole my identity, now I sit here every evening serving chowder and iced tea. Should've gone 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}



Authentication Cookies

HTTP/1.1 200 OK
Set-Cookie: **CAL=XXXXXXXXXXXX**;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





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