6.033 Lecture 24
Protocols and Authorization

Nickolai Zeldovich

Spring 2009
Denning-Sacco Protocol

{A:Ka}, SIGN( {A:Ka}, Kc), ENC( {Kab, SIGN(Kab, Ka)}, Kb)

{B:Kb}, SIGN( {B:Kb}, Kc)

A, B

Kab

Alice

Charlie

Bob
Denning-Sacco Protocol

{A:Ka}, SIGN({A:Ka}, Kc), ENC({Kab, SIGN(Kab, Ka)}, Kb)

{A:Ka}, SIGN({A:Ka}, Kc), ENC({Kab, SIGN(Kab, Ka)}, Kv)

Alice, Bob, Charlie, Victim
Denning-Sacco Protocol

Alice

{A:Ka}, SIGN( {A:Ka}, Kc)

ENC( {Kab, SIGN( {A,B,Kab}, Ka) }, Kb)

Bob

Charlie

{A:Ka}, SING( {A:Ka}, Kc)

{B:Kb}, SING( {B:Kb}, Kc)

Victim

{A:Ka}, SING( {A:Ka}, Kc),

ENC( {Kab, SING( {A,B,Kab}, Ka) }, Kb)

{A:Ka}, SING( {A:Ka}, Kc),

ENC( {Kab, SING( {A,B,Kab}, Ka) }, Kv)
**Phase 1**
- Client: generate random number
- Server: generate random number
- Client: send server_hello (crypto information, ...) to Server
- Server: receive client_hello (crypto information, ...)

**Phase 2**
- Client: demand client certificate
- Server: check client certificate
- Server: send client certificate (encrypted with Private Key Client)
- Client: receive client certificate
- Client: check encrypted client certificate
- Client: generate random number pre-master-secret
- Client: encrypt pre-master-secret with public key server

**Phase 3**
- Client: send encrypted pre-master-secret to Server
- Server: receive encrypted pre-master-secret
- Server: decrypt pre-master-secret with private key server
- Server: calculate Master-Secret with encrypted pre-master-secret

**Phase 4**
- Client: change to encrypted connection with Master-Secret as key
- Server: change to encrypted connection with Master-Secret as key
- End SSL handshake
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

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) Version/3.2.1 Safari/525.27.1
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=0.5
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) Version/3.2.1 Safari/525.27.1
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/*;q=0.5
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
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>
...</html>
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\">","&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 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=XXXXXXXXXXXXXXX;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