

Client Authentication on the Web

Kevin Fu (fubob@mit.edu)

MIT Lab for Computer Science

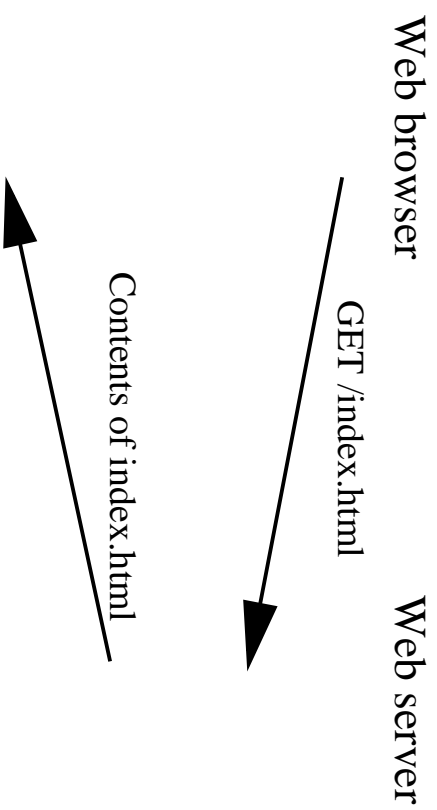
Northeastern University ACM

February 26, 2001

Caveat haxor

- **There are fine lines.**
- **Don't do this.**

The Web Protocol: HTTP



What is authentication?

Helps answer question “who are you?” and verifies the identity of an entity.

- **Knowing something (e.g., password)**
- **Having something (e.g., token)**
- **Being something (e.g., biometrics)**

File Edit View Go Communicator

Help


News Downloads Software Hardware Developers Help Search Shop

Bookmarks NetSite: What's Related

Back Forward Reload Home Search NetScap.e Print Security Shop Stop

Home Portfolios Markets Quotes & Research Trading Banking Account Services

E*TRADE Customer & Member Log On

 **New!** Earn \$50 for each new customer you refer to E*TRADE. [Get started now!](#) (customer logon required)

E*TRADE User Name:

Password:

Start In:

[Members: Forgot your password?](#)

Log on to [OptionsLink](#)®
(For Business Solutions clients only)

For our Chinese language investors, we now offer [E*TRADE Chinese](#)

Statement of Financial Condition * Not FDIC Insured * No Bank Guarantee * May Lose Value. [About brokerage insurance.](#)
System response and account access times may vary due to a variety of factors, including trading volumes, market conditions, system performance, and other factors.

File Edit View Go Communicator

Help

News Downloads Software Hardware Developers Help Search Shop

Bookmarks Netsite: What's Related

Back Forward Reload Home Search Netscape Print Security Shop Stop

Student Information System

MIT WebSIS

for Students

Adding and Dropping

Academic Record

current registration, grade

Financial Record

student account, financial

Biographic Record

addresses, required emerge

Physical Education

lottery and information

- [search](#)
- [email](#)

Subject Offerings and Schedule



Select A Certificate

The site 'student.mit.edu' has requested client authentication.

Here is the site's certificate:

Certificate for: Massachusetts Institute of Technology
Signed by: Massachusetts Institute of Technology
Encryption: Highest Grade (RC4 with 128 - bit secret key)

Select Your Certificate:



Why is client authentication on the Web difficult?

- **Limited interface.**
- **Hard-to-manage client-side storage.**
- **Solutions that exist are not deployable (e.g., personal certificates).**

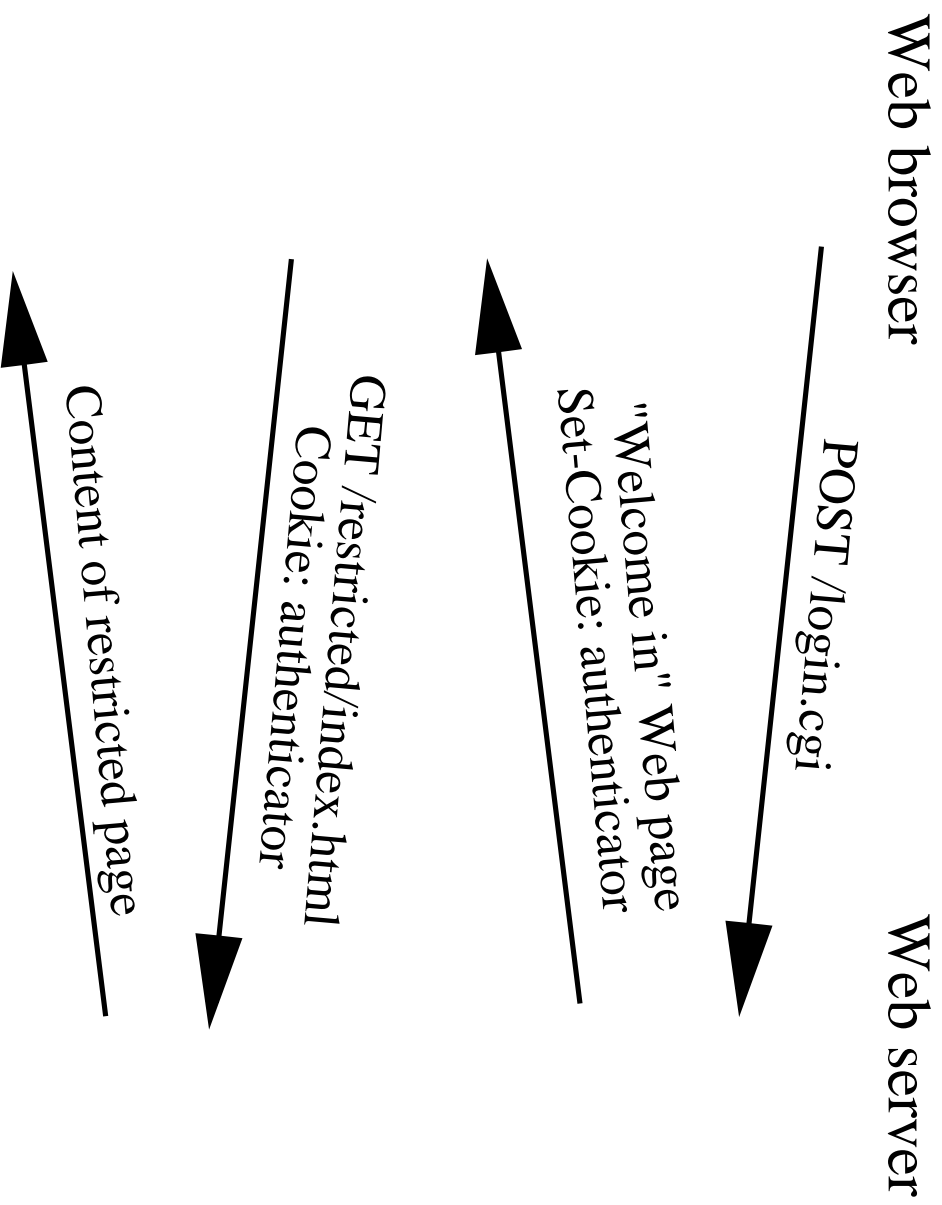
Case studies of Web authentication

- **SSL and plain HTTP do not work together: SprintPCS**
- **Letting clients name the price: InstantShop**
- **Security through obscurity: HighSchoolAlumni.com**
- **Predictable sequence numbers: Fatbrain.com**
- **Misuse of cryptography: WSJ.com**

Cookies: What are they?

- **A server can store key/value pairs on a client.**
- **The client sends previously set cookies to the server.**

The Web protocol with cookies



Netscape cookie example

domain	Javascript?	Path	SSL?	Expiration	Variable name	Value
.wsj.com	FALSE	/cgi	FALSE	941452067	fastlogin	bitdiddleMaRdw2J1h6Lfc

SSL and plain HTTP do not work together:

SprintPCS.com

- **Problem: Secure content can leak through plaintext channels.**
- **Cookie file has flag to require SSL.**
- **User logs in with HTTPS, then clicks back to main HTTP page.**
- **Vulnerable to eavesdroppers.**

File Edit View Go Communicator

Help

- News
- Downloads
- Software
- Hardware
- Developers
- Help
- Search
- Shop

Bookmarks Location: https://m27.sprintpcs.com/manage/general_manage_login.asp What's Related

- Back
- Forward
- Reload
- Home
- Search
- Netscape
- Print
- Security
- Shop
- Stop



Sprint PCS

- My Account
- My Services
- Customer Care
- Tutorials
- Help

- Shop
- Manage

Manage Your Sprint PCS Account Online

Customer Sign In

Enter Your Sprint PCS Phone Number

617-

Enter Your Account Password

Remember me

Sign In

[Get my Password](#)

The server m27.sprintpcs.com wishes to set a cookie that will be sent to any server in the domain .sprintpcs.com. The name and value of the cookie are: SPCS%5FRM=RM%5FON=Y&CN1= &R115=

This cookie will persist until Tue Mar 27 19:01:45 2001

Do you wish to allow the cookie to be set?

Cancel

Connect: Host m27.sprintpcs.com contacted. Waiting for reply...



Letting clients name the price: Instant Shop

- **Problem: Trusting clients not to modify HTML variables.**
- **Price determined by hidden variable in Web page.**
- **Make a local copy of the Web page. Modify it.**

File Edit View Go Communicator

Help

News Downloads Software Hardware Developers Help Search Shop

Bookmarks Location: What's Related

Back Forward Reload Home Search Netscape Print Security Shop Stop

To confirm your purchase, submit below.

Batteries \$10
Biology textbook \$99
Britney Spears CD \$25



Instant Shop: Mock up of what's inside

```
<html><body>
<form action=commit_sale.cgi>
<input type=hidden name=item1 value=10>Batteries $10<br>
<input type=hidden name=item2 value=99>Biology textbook $99<br>
<input type=hidden name=item3 value=25>Britney Spears CD $25<br>
<input type=submit>Confirm purchase
</form>
</body></html>
```

Instant Shop: Malicious client

```
<html><body>  
<form action=commit_sale.cgi>  
<input type=hidden name=item1 value=0>Batteries $10<br>  
<input type=hidden name=item2 value=0>Biology textbook $99<br>  
<input type=hidden name=item3 value=0>Britney Spears CD $25<br>  
<input type=submit>Confirm purchase  
</form>  
</body></html>
```

Security through obscurity: HighSchoolAlumni.com

- **Problem: No cryptographic authentication at all.**
- **Cookie authenticator is the public username and public user ID.**

File Edit View Go Communicator Help

News Downloads Software Hardware Developers Help Search Shop

Bookmarks Location: What's Related

Back Forward Reload Home Search Netscape Print Security Shop Stop

Discover **Beautiful** examples of high-style bathrooms

See Them Here!



Apply Now! **VISA**

0% intro APR* for purchases! see conditions




Login to HighSchoolAlumni.com

Enter your Username
If you have forgotten your password
If you have forgotten your user name

User name:

Password:

 The server www.highschoolalumni.com wishes to set a cookie that will be sent to any server in the domain .highschoolalumni.com. The name and value of the cookie are: Beacon=hsareg[smiley][smiley][smiley][smiley].hsa0.983078390.

This cookie will persist until Tue Apr 27 06:07:05 2004

Do you wish to allow the cookie to be set?

Connect Host WWW

Predictable sequence numbers: fatbrain.com

- **Problem: Customer can determine the authenticator for any other user.**
- **Authenticators are sequence numbers in the URL.**
- **Guess a victim's sequence number by decrementing.**
- **Access to personal information, receive password by email.**

File Edit View Go Communicator

Help

News Downloads Software Hardware Developers Help Search Shop

Bookmarks Go To: What's Related

Back Forward Reload Home Search Netscape Print Security Shop Stop

Your Account

- **Account Help**

Welcome to Your Account.

- **[Change Sign-in E-mail](#)**

Manage your account information, check on orders you have placed and more.

- **[Change Password](#)**

Use the menu bar on the left to:

- **[Edit Profiles](#)**
 - **Change Sign-in E-mail** -- change your sign-in e-mail. [More...](#)
 - **Change Password** -- change your sign-in password. [More...](#)
- **[Order Status](#)**
 - **Edit Profiles** -- edit your shipping, billing and payment information or create a new profile. [More...](#)
 - **Order Status** -- view your order history or check the status of orders en route. [More...](#)
- **[Keep Me Posted](#)**
 - **Keep Me Posted** -- view your email notifications. [More...](#)
- **[Password Reminder](#)**
 - **Password Reminder** -- send yourself an email containing your password. [More...](#)

For detailed information on what you can do with Your Account, click the "More..." link next to your topic of interest or simply scroll down this page.

Thanks and we hope you enjoy the flexibility available with Your Account.



100%



Fatbrain URL authenticator

<https://www.fatbrain.com/HelpAccount.asp?t=0&p1=email1@neu.edu&p2=13535997>

<https://www.fatbrain.com/HelpAccount.asp?t=0&p1=email2@neu.edu&p2=13535998>

Fatbrain response

“Its [sic] frustrating that programmers ... continue to fall prey to the same old tricks. Simple problems like lazy sequence numbers and buffer overflows in most cases can be easily eliminated if we as programmers would be a little vigilant about **sound design and solid code reviews**. **I just *love* being at work on a Friday at midnight** managing unscheduled production releases. :)”

—Chris Grant

WSJ.com

- **Wanted to authenticate paid subscribers.**
- **Half million paid-subscriber accounts.**
- **Can purchase articles. Optional stock portfolio tracking.**

Misuse of cryptography: WSJ.com

- **Problem: Cryptography used incorrectly can be worse than no cryptography at all.**
- **Easily guessable authenticator.**
- **Given a username, our Perl script produces the authenticator.**

WSJ.com analysis: the `crypt()` hash function

- **Takes an 8-character input and salt.**
- **Ignores all input after the 8th character.**
- **Produces a hash.**

File Edit View Go Communicator

News Downloads Software Hardware Developers Help Search Shop

Bookmarks Netsite: http://public.wsj.com/home.html

Back Forward Reload Home Search Netscape Print Security Shop Stop



THE WALL STREET JOURNAL.

U.S. View

Other Views:
ASIA EUROPE

Free U.S. Quotes
Enter Symbol Here

WSJ.com Subscribers
Go Directly To:

Select a Page

Or LOG IN

WSJ.COM SUBSCRIBERS ONLY

Top Business News

- Davis Says California Has Deal With Utility
- Employers Plan Slight Scaling Back

100% of 7K (at 227 bytes/sec)



The server interactive.wsj.com wishes to set a cookie that will be sent to any server in the domain .wsj.com. The name and value of the cookie are: fastlogin=



This cookie will persist until Sun Feb 25 07:26:53 2001
Do you wish to allow the cookie to be set?

OK

Cancel

Wsj.com analysis continued

- `fastlogin = user + crypt (user + rotating server secret).`

- Using your fastlogin cookie to produce another:

username	Crypt() Output	Fastlogin Cookie
bitdiddle	MaRdw2J1h6Lfc	bitdiddleMaRdw2J1h6Lfc
bitdiddler	MaRdw2J1h6Lfc	bitdiddlerMaRdw2J1h6Lfc

- Lack of revocation.
- The fastlogin cookie lasts forever

How did we obtain the rotating server secret?

- Adaptive chosen plaintext attack (dynamic programming).
- Perl script queried WSJ with invalid cookies.
- Runs in max 128×8 queries rather than intended 128^8 (1024 vs. 72057594037927936).
- 1 sec/query yields 17 minutes vs. 10^9 years.
- The key is “March20”.

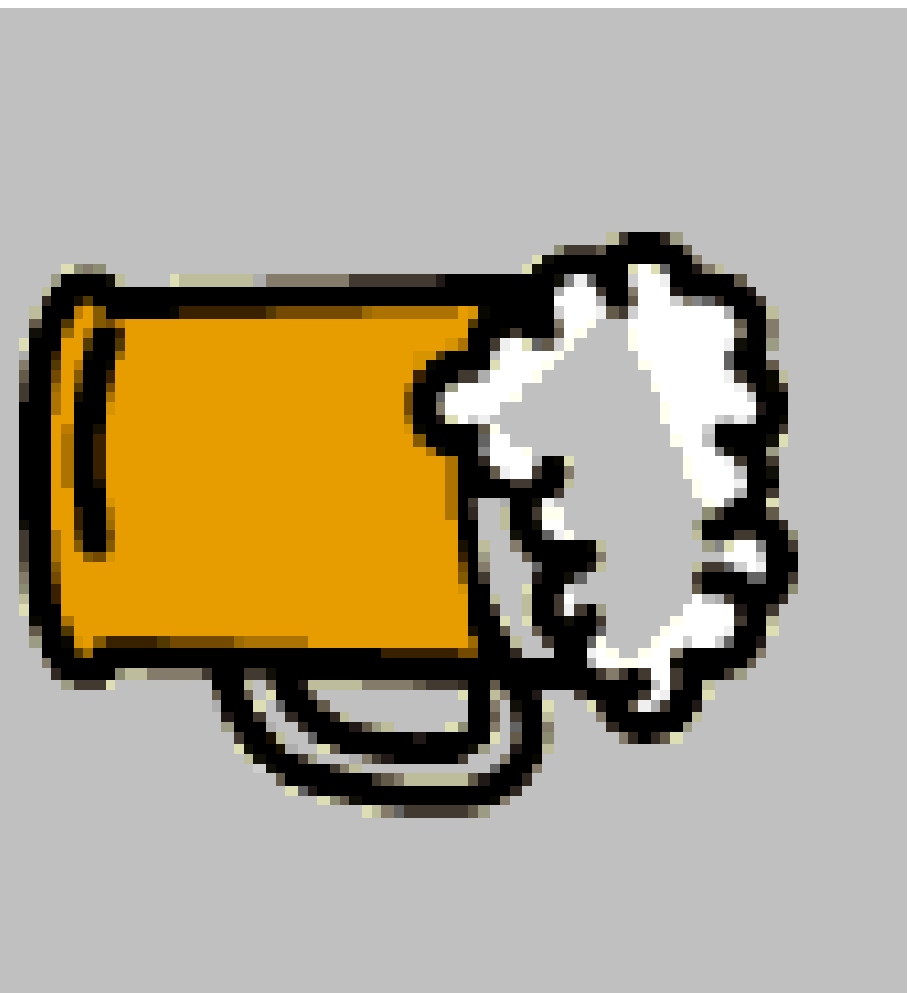
Dow Jones Response

“ ... about the factors affecting design decisions, it is certainly result of **time to market** considerations. ... we simply **didn't have clear security requirements** defined within the group and outside the group. So, we did what worked. We tried a better encryption algorithm, but hit a bug that we couldn't fix, so we implemented one that worked even though the architect in charge was fully aware of its short-comings. You must understand that I'm giving you my read on the situation since **I've joined WSJ.com just 5 weeks ago.** ”

—Javeh Saleh

Vice President, Technology

Interactive Business Technology Services, WSJ.com



Stop homebrew authentication!

Is there a solution?

- **Standardize. But on what?**
- **Use well-understood protocols.**
- **What prevents this? Clumsy interfaces, politics, lack of coordination.**
- **Collect and analyze cookie schemes on <http://cookies.fooworld.org/>.**

Server authentication is difficult too

- **Caching SSL sessions on IP address rather than hostname.**
- **Netscape demo.**

Are there any systems that work?

- **Some sites have secure Web authentication.**
- **Such sites are few and far between**

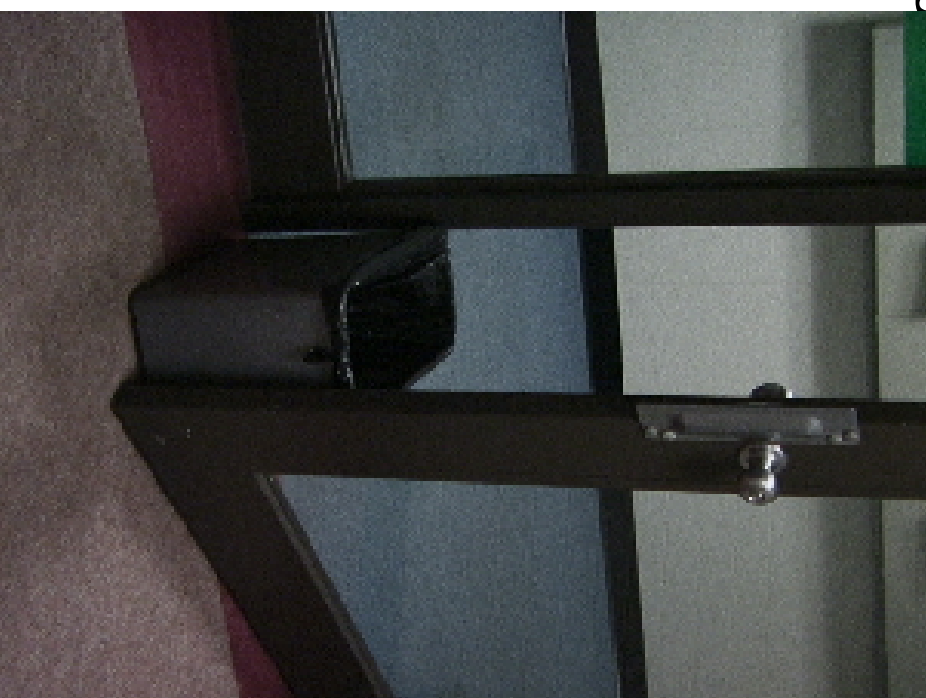
Conclusions

- **Good designs do not imply good implementations.**
- **Keep It Simple, Stupid (KISS).**
- **Subtle assumptions can lead to insecurity.**

Suggested reading

- **Schneier's "Secrets and Lies"**
- **Menezes et al's "Handbook of Applied Cryptography"**
- **Schneier's "Applied Cryptography"**

If you leave the door open...



What is SSL: channel security

- **Confidentiality**
- **Authentication**
- **Integrity protection**

Certificates

- **Contains a public key, meta data, and a signature by a trusted third party.**

Certificate Authorities (CAs)

- **Trusted third party with well-known public key.**
- **Certifies who belongs to a public key.**
- **Example: Verisign.**

What does a CA-issued certificate mean?

- **No one knows exactly.**
- **That a public key belongs to someone authorized to represent a hostname?**
- **That a public key belongs to someone who is associated in some way with a hostname?**
- **That a public key belongs to someone who has lots of paper trails associated to a company related to a hostname?**

How to get a Verisign certificate

- **Pay Verisign (\$300)**
- **City of Cambridge license (\$20)**
- **Letterhead from company (\$0)**
- **Notarized document (need driver's license) (\$0)**

SSL pitfalls: Default CAs in browsers

- **Neither Netscape or Microsoft have published their rule set for deciding which CA roots to include in browsers.**
- **Every CA is equally trusted.**
- **A single bad CA can disrupt authentication for the whole system.**

Certificate Signers' Certificates

[Security Info](#)

[Passwords](#)

[Navigator](#)

[Messenger](#)

[Java/JavaScript](#)

[Certificates](#)

[Yours](#)

[People](#)

[Web Sites](#)

[Signers](#)

[Cryptographic Modules](#)

These certificates identify the certificate signers that you accept:

ABAAccom (sub, Am Bankers Assn.) Root CA
American Express CA
American Express Global CA
BelSign Object Publishing CA
BelSign Secure Server CA
Deutsche Telekom AG Root CA
Digital Signature Trust Co. Global CA 1
Digital Signature Trust Co. Global CA 2
Digital Signature Trust Co. Global CA 3
Digital Signature Trust Co. Global CA 4
E-Certify Commerce ID
E-Certify Internet ID
Entrust.net Premium 2048 Secure Server CA
Entrust.net Secure Personal CA

Edit

Verify

Delete

SSL pitfalls: CA revocation

- **Certificates last for a long time, typically a year.**
- **No way to revoke a certificate.**
- **What if a CA itself is compromised? [Sun CA]**

SSL pitfalls: Random number generation

- **Netscape used predictable numbers to generate SSL session keys.**
- **Two Berkeley graduate students were able to predict sessions keys.**
- **Because of an insecure implementation, SSL was insecure.**

SSL pitfalls: End-to-end content authentication

- **SSL authenticates servers, not content. [Akamai]**

File View Go Communicator

- Downloads
- Software
- Hardware
- Developers
- Help
- Search
- Shop

Bookmarks Netsite: https://a248.e.akamai.net/n/248/1777/aks20010221.7.0/img.etrade.com/images/tab_none.gif

- Forward
- Reload
- Home
- Search
- Netscape
- Print
- Security
- Shop
- Stop

Portfolios Markets Quotes & Research Trading Banking Account Services



SSL pitfalls: Perfect forward secrecy

- **Compromised server private key → decrypt future and past traffic.**