Client Authentication on the Web

February 26, 2001
Northeastern University ACM

MIT Lab for Computer Science
Kevin Fu (fubob@mit.edu)

Client Authentication on the Web
There are fine lines.

• Don't do this.

• There are fine lines.

Caveat haxor
The Web Protocol: HTTP

- Web browser
- Web server

GET /index.html

Contents of index.html
What is authentication?

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

Helps answer the question “who are you?” and verifies the identity of an entity.
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).
Misuse of cryptography: WSI.com

HighschoolAlumni.com

Security through obscurity:

Letting clients name the price: InstantShop

SprintPCS

SSL and plain HTTP do not work together:

Case studies of Web authentication
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

Web browser

Web server

GET /restricted/index.html

Set-Cookie: authenticator

Cookie: authenticator

"Welcome in Web page"

POST /login.cgi

Content of restricted page
Netscape cookie example
SSL and plain HTTP do not work together:

Problem: Secure content can leak through plaintext channels.

- User logs in with HTTPS, then clicks back to main page.
- Cookie file has flag to require SSL.
- Vulnerable to eavesdroppers.
- HTTP page.

SprintPCS.com
Do you wish to allow the cookie to be set?

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

The name and value of the cookie are:

SPCS%$FRN=RM%$FON=V8%$C1=%$3%$R115=

The server m27.sprintpcs.com wishes to set a cookie that will be sent.
Letting clients name the price: InstantShop

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.
Instant Shop: Mock up of what's inside
<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" value="Confirm purchase"/>
</form>
</body>
</html>

Instant Shop: Malicious Client
Problem: No cryptographic authentication at all.

Public user ID.

Cookie authenticator is the public username and public ID.

HighSchoolAlumni.com
A customer can determine the authenticator for any other user. Authenticators are sequence numbers in the URL.

Access to personal information, receive password by decrementing:

- Guess a victim's sequence number by decrementing.

By email:

- Predictable sequence numbers: fatbrain.com
Thanks and we hope you enjoy the flexibility available with your account.

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.

- Password Reminder -- send yourself an email containing your password.
  More...
- Keep Me Posted -- view your email notifications.
  More...
- Order Status -- view the status of your order.
  More...
- Edit Profile -- edit your shipping billing and payment information or create a new profile.
  More...
- Change Sign-in E-mail -- change your sign-in e-mail.
  More...

Use the menu bar on the left to:

- Change Your Account Information, check on orders you have placed and more.

Welcome to Your Account.
Fatbrain URL authenticator

https://www.fatbrain.com/HelpAccount.asp?t=0&p1=email1@neu.edu&p2=13535998

https://www.fatbrain.com/HelpAccount.asp?t=0&p1=email2@neu.edu&p2=13535997
Fatbrain response

"It's 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
Can purchase articles. Optional stock portfolio tracking.

Half million paid-subscriber accounts.

Wanted to authenticate paid subscribers.

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.

• Misuse of cryptography: WSJ.com
WSJ.com analysis: The `crypt()` hash function

- Takes an 8-character input and salt.
- Ignores all input after the 8th character.
- Produces a hash.
The fastlogin cookie lasts forever.

Lack of revocation.

Using your fastlogin cookie to produce another:

```plaintext
username Cryplt() Output Fastlogin Cookie

user + Cryplt (user + Rotating Server Secret) = fastlogin
```

Wsj.com analysis continued
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 x 8 quarters rather than intended (128 vs. 1024 vs. 72057594037927936).
- Perl script queried WSJ with invalid cookies.
- 1 sec/query yields 17 minutes vs. 10^9 years.
- The key is "March 20".
"...about the factors affecting design decisions, it is certainly the 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 found 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!
Isthereasolution?

Standardize. But on what?

Use well-understood protocols.

What prevents this? Clumsy interfaces, politics,

Collect and analyze cookie schemes on

https://cookies.footwork.orge

Lack of coordination.

Is there a solution?
Server authentication is difficult too.

- Netscape demo.
- Hostname.

Caching SSL sessions on IP address rather than

Server authentication is difficult too.
Are there any systems that work?  

Some sites have secure Web authentication.  

Such sites are few and far between.
Conclusions

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

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, metadata, 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 who has lots of paper trails associated to a company related to 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 is to represent a hostname?

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.

SSL pitfalls: Default CAs in browsers
These certificates identify the certificate issuers that you accept:
SSL Pitfalls: CA Revocation

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

SSL Pitfalls: CA Revocation
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 authentication servers, not content. [Akamai]
SSL pitfalls: Perfect forward secrecy

- Comromised server private key → decrypt future and past traffic.