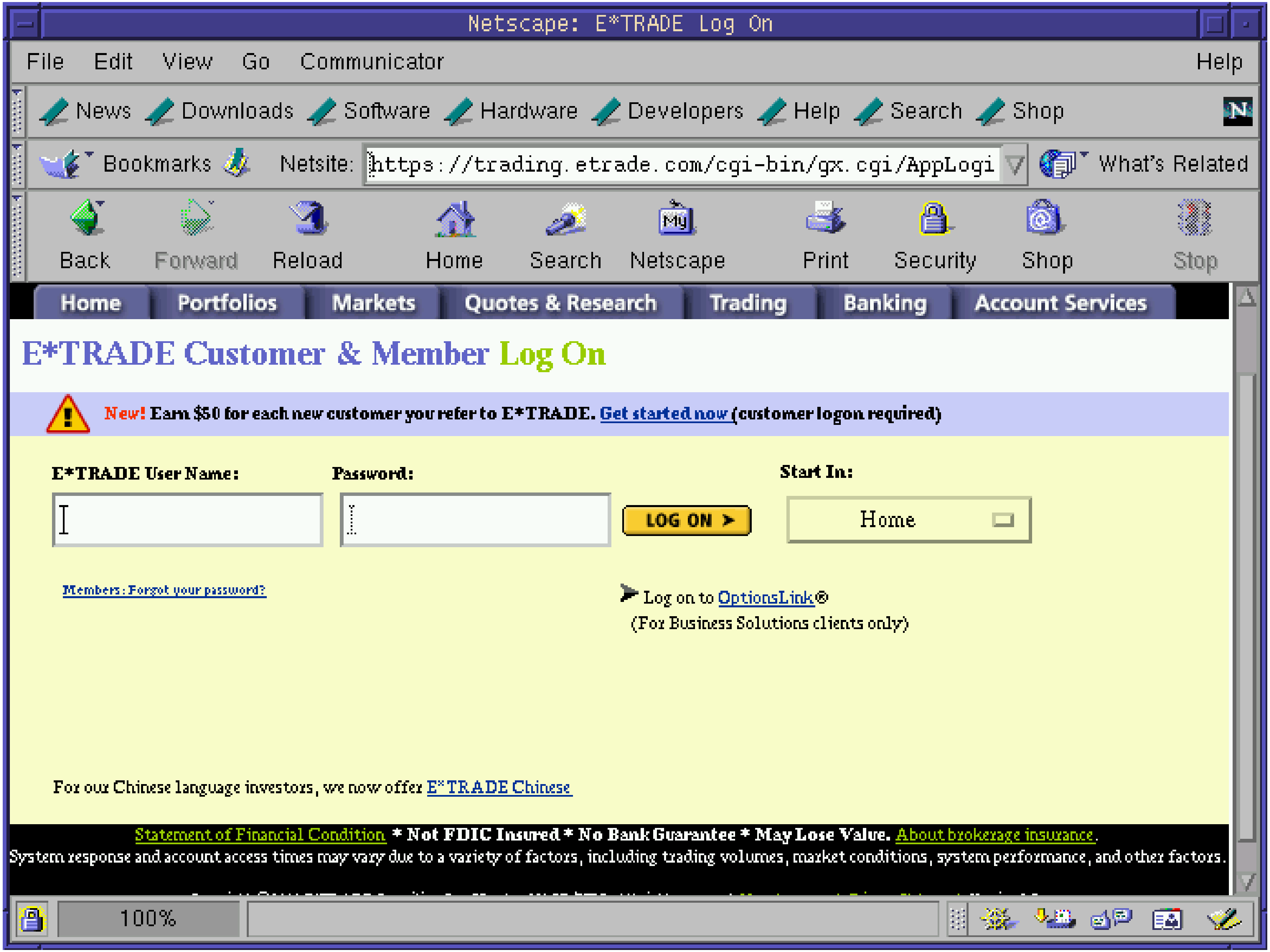
Dos and Don’ts of Client Authentication on the Web

Kevin Fu, Emil Sit, Kendra Smith, Nick Feamster

MIT Lab for Computer Science

`http://cookies.lcs.mit.edu/`

`cookie-eaters@mit.edu`



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:

LOG ON >

Start In: Home

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.

Client authentication is solved, right?

MANY WEB SITES GET IT WRONG

Site	Security problem
WSJ.com	crypto misuse, secret key exposed
SprintPCS.com	leaks authenticator in plaintext
FatBrain.com	predictable session ID, sequence number
PerformanceBike.com	predictable session ID, sequence number
highschoolalumni.com	circumvent password authentication
ign.com	circumvent password authentication
chickclick.com	circumvent password authentication
NEBride.com	circumvent password authentication
ihateshopping.net	circumvent password authentication
cstc.org	circumvent password authentication

SOFTWARE GETS IT WRONG TOO

Software product	Security problem
Allaire ColdFusion	session IDs, linear congruential number generator
ArsDigita ACS	signs ambiguous messages
Jakarta TomCat	session IDs, predictable random seed

HOW WE BROKE THESE SCHEMES

- **Gathered public information**
  - Usernames
  - Web server HTTP responses
  - Obtain sample authenticators
- **Observe authenticators while varying parameters**
- **No eavesdropping**

INTERROGATIVE ADVERSARY

- **Treat a server as an oracle for an adaptive chosen message attack**
- **Adaptively query a Web server a reasonable number of times**

THE INTERROGATIVE ADVERSARY DEFEATS...

- SSL client authentication? No.
- HTTP Basic or Digest authentication? No.
- Homebrew cookie authentication schemes? Maybe...

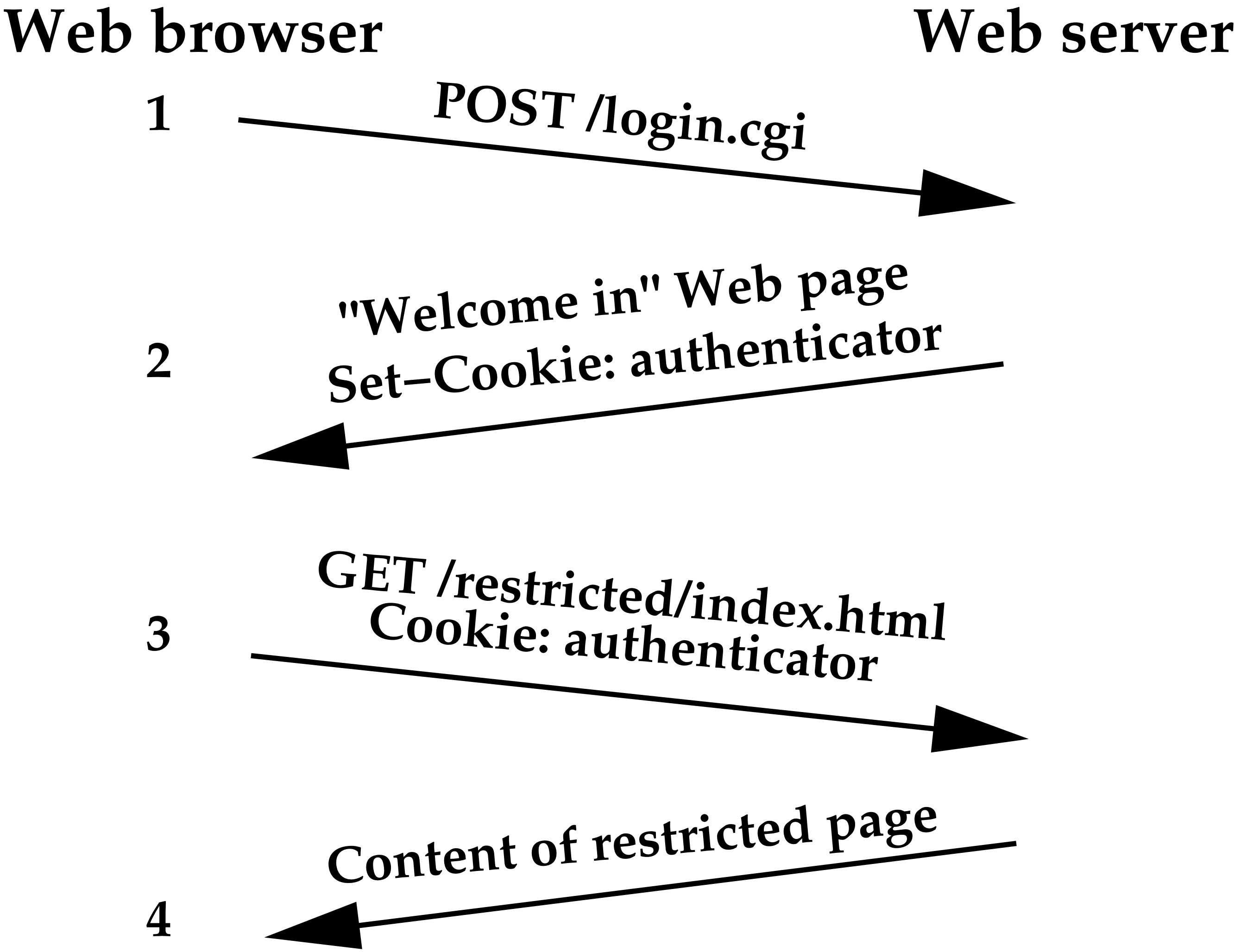
COOKIES

- **A Web server can store key/value pairs on a client**
- **Returned in subsequent requests to the server**
- **Can implement login sessions**

NETSCAPE COOKIE EXAMPLE

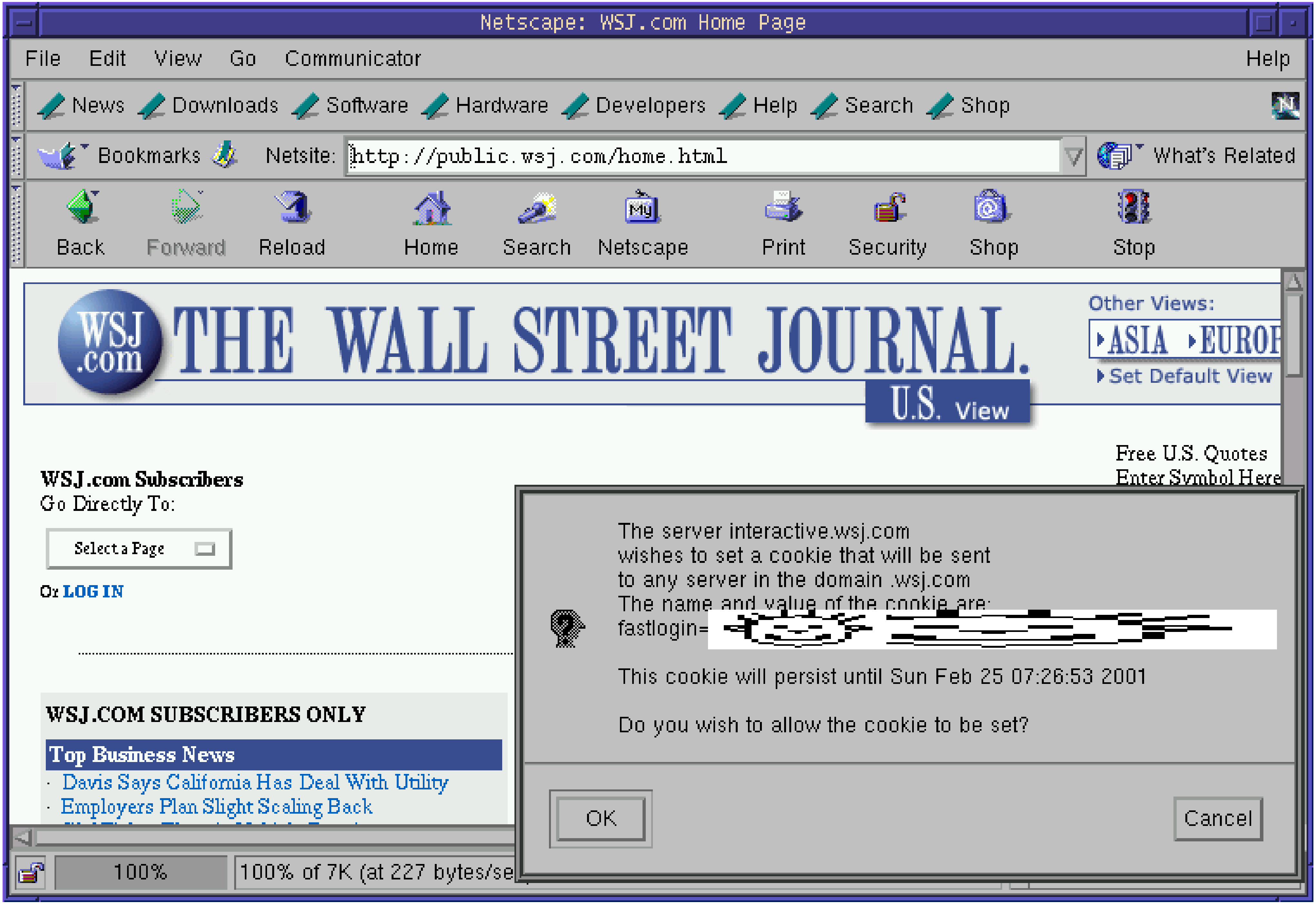
Domain	.wsj.com
Path	/cgi
Variable name	fastlogin
Value	bitdiddleMaRdw2J1h6Lfc
SSL?	FALSE
Expiration	941452067

COOKIES FOR LOGIN SESSIONS



- Enter password once per session

CASE STUDIES


Netscape: WSJ.com Home Page
File Edit View Go Communicator Help
News Downloads Software Hardware Developers Help Search Shop
Bookmarks Netsite: http://public.wsj.com/home.html What's Related
Back Forward Reload Home Search Netscape Print Security Shop Stop
WSJ.com
THE WALL STREET JOURNAL.
U.S. View
Other Views:
ASIA EUROP
Set Default View
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%
100% of 7K (at 227 bytes/se
OK
Cancel

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=[redacted]

This cookie will persist until Sun Feb 25 07:26:53 2001

Do you wish to allow the cookie to be set?

MISUSE OF CRYPTOGRAPHY: WSJ.COM

- **Weaker than plaintext passwords**
- **Extracted secret signing key**
- **Can create authenticators for anyone**

WSJ.COM ANALYSIS

- **Design: auth = $\{$user, $\mathtt{MAC}_{\mathtt{k}}$ (user)$\}$**
- **Reality: auth =**

  user $+$ UNIX-crypt (user $+$ server secret)
- **Easily produce authenticator cookies**

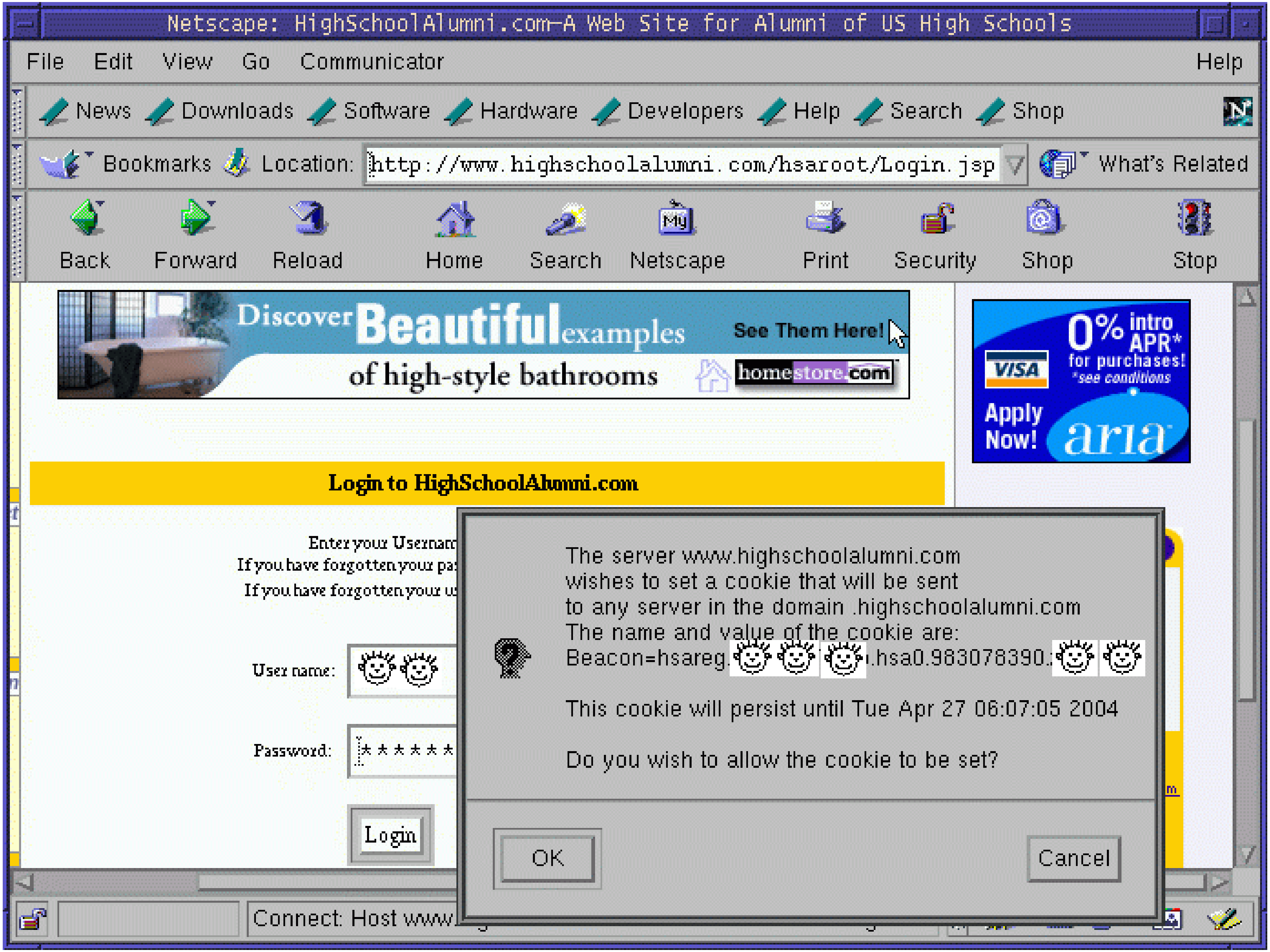
username	crypt() output	authenticator cookie
bitdiddl	MaRdw2J1h6Lfc	bitdiddlMaRdw2J1h6Lfc
bitdiddle	MaRdw2J1h6Lfc	bitdiddleMaRdw2J1h6Lfc

OBTAINING THE SERVER SECRET

- **Adaptive chosen message attack**
- **Perl script queried WSJ with invalid cookies**
- **Runs in max of 128×8 queries rather than intended 128^8 (1024 vs. 72057594037927936)**
- **17 minutes vs. 10^9 years**
- **The key is “March20”**

HOW OUR ATTACK WORKS

Secret guess	username	crypt input	worked?
	bitdiddl	bitdiddl	Yes
A	bitdidd	bitdiddA	No
⋮	⋮	⋮	⋮
M	bitdidd	bitdiddM	Yes
MA	bitdid	bitdidMA	No
⋮	⋮	⋮	⋮
Ma	bitdid	bitdidMa	Yes
⋮	⋮	⋮	⋮
March20	b	bMarch20	Yes



http://www.highschoolalumni.com/hsaroot/Login.jsp

Login to HighSchoolAlumni.com

Enter your Usernam

If you have forgotten your pa

If you have forgotten your u

User name: [redacted]

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.[redacted].hsa0.983078390.[redacted]

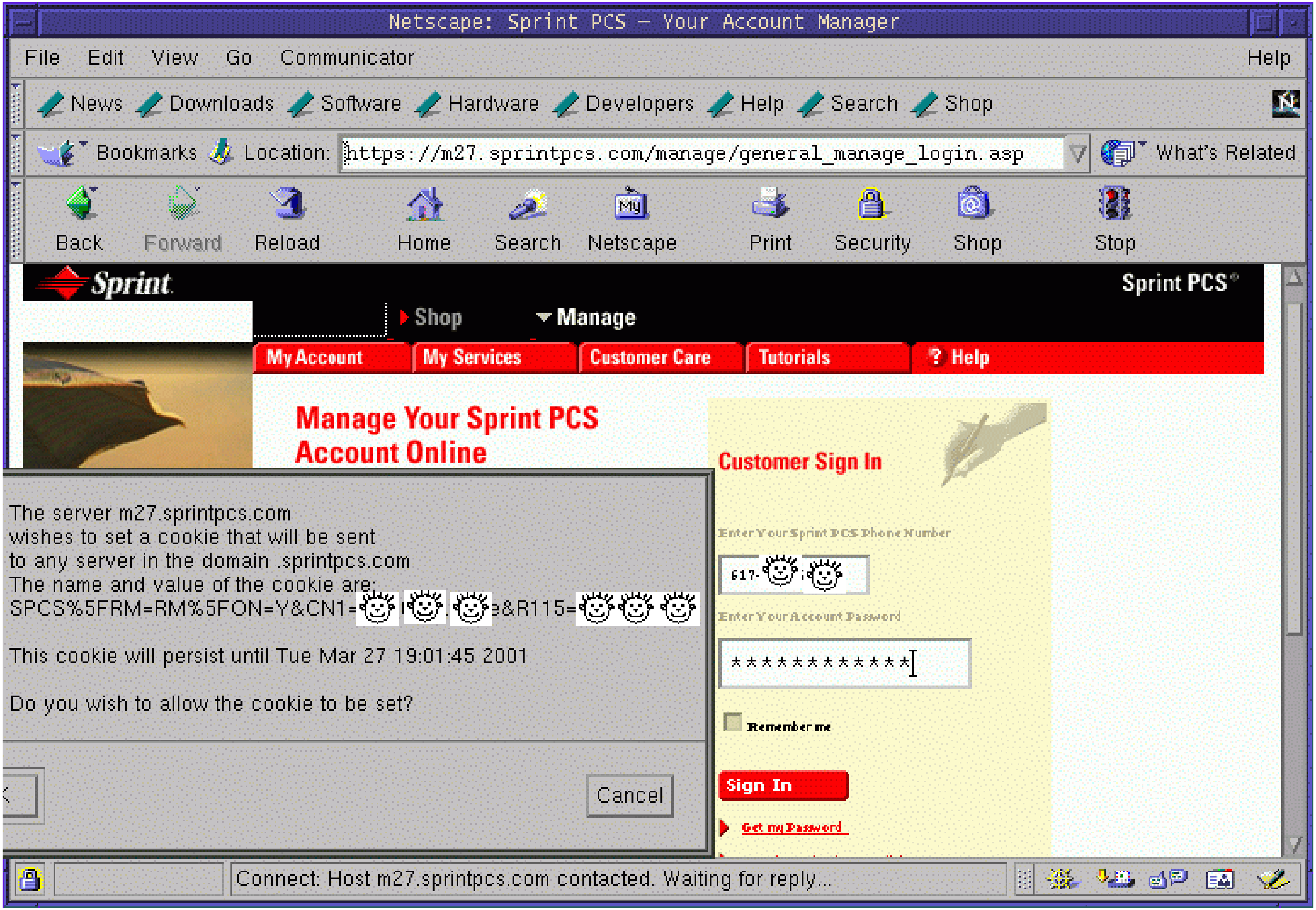
This cookie will persist until Tue Apr 27 06:07:05 2004

Do you wish to allow the cookie to be set?

Connect: Host www

LACK OF CRYPTOGRAPHY: HIGHSCHOOLALUMNI.COM

- **Circumvent password authentication**
- **Cookie authenticator is the public username and public user ID**



Location: https://m27.sprintpcs.com/manage/general_manage_login.asp

617-[redacted]

****

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=[redacted]e&R115=[redacted]

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

Do you wish to allow the cookie to be set?

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

LEAKING SECRETS: SPRINTPCS.COM

- **Secure content can leak through plaintext channels**
- **A cookie has flag to require SSL**
- **User logs in with HTTPS, then clicks back to main HTTP page**
- **Vulnerable to passive eavesdropper**

HINTS FOR CLIENT AUTHENTICATION

- **Limit the lifetime of authenticators**
- **Make authenticators unforgeable**
- **Sign what you mean**

LIMIT THE LIFETIME OF AUTHENTICATORS

- **Browsers cannot be trusted to expire cookies**
- **No revocation of WSJ cookies**

MAKE AUTHENTICATORS UNFORGEABLE

- Prevent modification of the cookie
- Do not allow bypass of password authentication
- Highschoolalumni.com

SIGN WHAT YOU MEAN!

- **badauth = sign (username + expiration, key)**
  - (Alice, 21-Apr-2001) → sign (Alice21-Apr-2001, key)
  - (Alice2, 1-Apr-2001) → sign (Alice21-Apr-2001, key)
- **Same authenticator!**
- **Use unambiguous representation or delimiters**

A SCHEME THAT WORKS

$$\textbf{auth} = \texttt{expire} + \texttt{data} + \texttt{MAC}_k(\texttt{expire} + \texttt{data})$$

where `MAC` could be HMAC-SHA1,

`data` could be a username or capability, and

$'+'$ denotes concatenation with a delimiter

Secure against interrogative adversary

SUMMARY

- **Many schemes easily broken**
- **Following hints can prevent vulnerabilities**
- **Juicy details in our technical report**
- **Cookies are limited; live with it or move on**

JOIN US

DONATE YOUR COOKIES FOR ANALYSIS*

`http://cookies.lcs.mit.edu/`

`cookie-eaters@mit.edu`

***may be tax deductible**

All your cookie are belong to us