



National Institute of
Advanced Industrial Science
and Technology
AIST

RCIS
Research Center for
Information Security

PAKE-based mutual HTTP authentication for preventing phishing attacks

Research Center for Information
Security

National Institute of
Advanced Industrial Science and
Technology

Our Proposal

■ Our proposal

new mutual authentication protocol for Web
systems against phishing attacks

■ Some of design goals are

- ◆ Secure,
- ◆ Easy to use, and
- ◆ Generic.

... details follow.

Design Goals

■ Secure

- detecting phishing websites reliably
 - ◆ Both users and servers are authenticated
- no password information leaks for false websites
 - offline dictionary attack impossible

(\leftrightarrow DIGEST auth, PwdHash:
>20 chars required for password secrecy)

Design Goals

■ Easy to use

- using human-memorable passwords only
- no need for personal secret storage
(↔TLS client auth., password reminders)

■ Generic

- no whitelist (↔EV SSL)
- no blacklist (↔IE/Firefox phishing warnings)
- not site-specific

Design Goals

■ *Aiming for long-term solution:*

- ◆ *future replacement for form-based auth.*
- Requires server modifications
 - ◆ Installation of the new authentication module.
- Requires client modifications
 - ◆ Browsers must be modified to support this algorithm.

Technology

- Adopting PAKE for Web authentication
 - Mutual auth. with weak secret (password)
 - Password information is not leaked at all
 - ◆ Offline dictionary attack impossible
- Naturally extending RFC2617
 - Drop-in replacement for BASIC/DIGEST
 - Replacement for form-based authentication in web applications
 - Relying on TLS for secrecy of payload
 - ◆ Assume transport/DNS security
- Host-name based detection of phishing
 - avoiding man-in-the-middle phishing

Protocol details

- Based on ISO-defined variant of PAKE protocol (ISO 11770-4 KAM3)
 - Password is combined with hostname as “weak secret” to prevent MIM attack.
 $\pi = H(\text{password}, \text{host})$
- Computational cost similar to TLS
 - Single public-key op. for 1st access
 - A few hash op. for 2nd access & more



Protocol details

■ Some features

■ Session management

- ◆ reuse negotiated key for several requests
 - reducing computational overhead

■ “Optional” authentication

- ◆ Support guest/authenticated accesses in same URI
 - Like Yahoo! top-page and many other websites

```
GET / HTTP/1.1  
Host: www.example.com
```

```
HTTP/1.1 401 Authentication required  
WWW-Authenticate: Mutual algorithm=iso11770-4-ec-p256,  
    validation=host, realm="Protected Contents",  
    stale=0  
Content-Type: text/html; charset="ISO-8859-1"  
Content-Length: 5163  
.....
```

```
GET / HTTP/1.1  
Host: www.example.com  
Authorization: Mutual algorithm=iso11770-4-ec-p256,  
    validation=host, user=foobar,  
    wa=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

```
HTTP/1.1 401 Authentication required  
WWW-Authenticate: Mutual sid=yyyyyyyy,  
    wb=zzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzzz,  
    nc-max=1024, nc-window=64, time=300, path="/"  
Content-Length: 0
```

```
GET / HTTP/1.1  
Host: www.example.com  
Authorization: Mutual sid=yyyyyyyy, nc=0,  
    oa=wwwwwwwwwwwwww
```

```
HTTP/1.1 200 OK  
Authentication-Info: Mutual sid=yyyyyyyy,  
    ob=vvvvvvvvvvvv  
Content-Type: text/html; charset="ISO-8859-1"  
Content-Length: 7043  
.....
```

First request
(w/o authentication)

Key exchange phase

Authentication
confirmation phase

First Request

GET / HTTP/1.1

Host: www.example.com

HTTP/1.1 401 Auth. required

WWW-Authenticate: Mutual
algorithm=iso11770-4-ec-p256,
validation=host,
realm="Protected Contents",
stale=0

Content-Type: text/html;
charset="ISO-8859-1"

Content-Length: 5163

■ First request without auth.

- 401 response
(as in usual HTTP auth.)
- Specify crypto. algorithm
from server

- Content body displayed
 - ◆ Requesting login
- ID/Pass requested

Variant to First Request

GET / HTTP/1.1

Host: www.example.com

HTTP/1.1 200 OK

Optional-WWW-Authenticate:
Mutual

algorithm=iso11770-4-ec-p256,
validation=host,
realm="Protected Contents",
stale=0

Content-Type: text/html;
charset="ISO-8859-1"

Content-Length: 5163

- Variant: 200 + optional auth.
 - New introduction in ours
- “Guest Contents” displayed with Optional-WWW-auth header
 - User can continue to be a guest
 - Or
 - User can enter ID/Pass to login to the site

Key exchange

GET / HTTP/1.1

Host: www.example.com

Authorization: Mutual
algorithm=iso11770-4-ec-p256,
validation=host, **user=foobar,**
wa=xxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxx

HTTP/1.1 401 Authentication
required

WWW-Authenticate: Mutual
sid=yyyyyyyy,
wb=zzzzzzzzzzzzzzzzzzzzzzzzzzzzzz,
nc-max=1024, nc-window=64,
time=300, path="/"

Content-Length: 0

- PAKE Key exchange ongoing
 - Client/server exchanges key materials wa & wb, twisted by password-based weak secrets
- Session ID (sid) established
- Temporary key shared between client & server, *only if the weak secrets are generated from the same password*

Final authentication

GET / HTTP/1.1

Host: www.example.com

Authorization: Mutual

sid=yyyyyyyy, nc=0,

oa=aaaaaaaaaaaaaaaaaaaa

HTTP/1.1 200 OK

Authentication-Info: Mutual

sid=yyyyyyyy,

ob=vvvvvvvvvvvvvvvv

Content-Type: text/html;
charset="ISO-8859-1"

Content-Length: 7043

- Checking proper key exchange using shared-key and hash functions
- Both clients and servers are authenticated (oa, ob)
 - Client MUST check the validity of ob

Next request

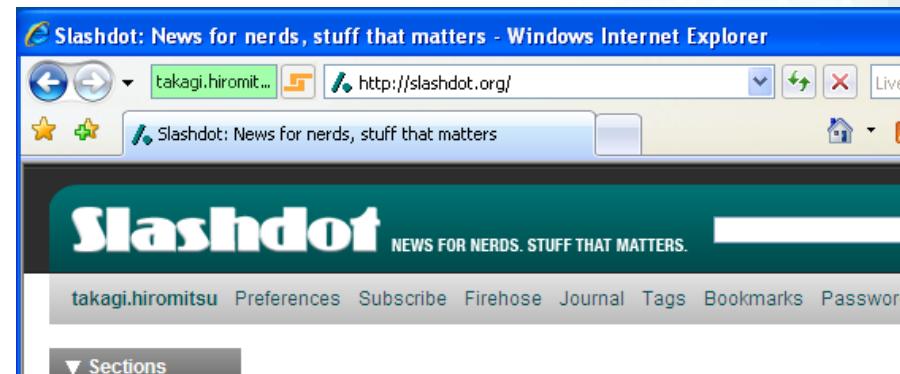
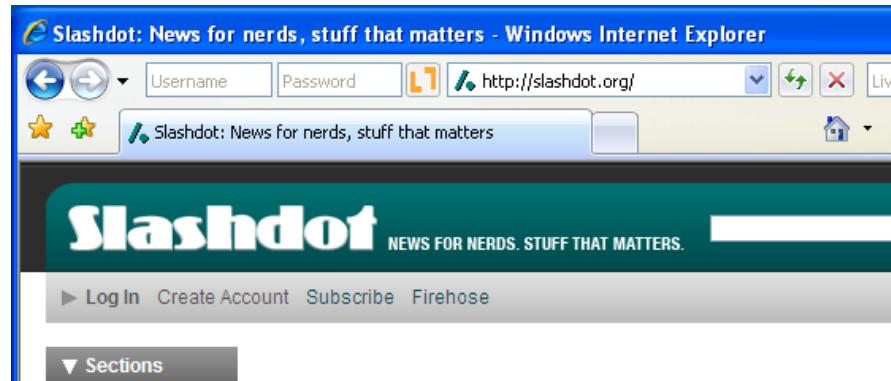
GET /logo.png HTTP/1.1
Host: www.example.com
Authorization: Mutual
 sid=yyyyyyyy, nc=1,
 oa=oooooooooooooooooooo

- Shared key can be reused for multiple requests
 - Nonce prevents replay
 - Number of reuse are limited by nonce counter limit

HTTP/1.1 200 OK
Authentication-Info: Mutual
 sid=yyyyyyyy,
 ob=oooooooooooooooooooo
Content-Type: image/png
Content-Length: 15082

UI consideration

- Entry field must be protected from image-based forgeries
 - no popup dialog (\leftrightarrow BASIC/DIGEST auth.)
 - e.g. use toolbar area (see above)
- Auth. status must be indicated
 - to prevent imitated auth. success



Current status

- Plugin for Apache server implemented
- Test Firefox extension implemented
 - Full implementation is about to start
- Internet-Draft in preparation

Future Plans

- Field test in a part of Yahoo! Japan
- Distribution of open-source modules
- Submitting Internet-Draft

Related Work

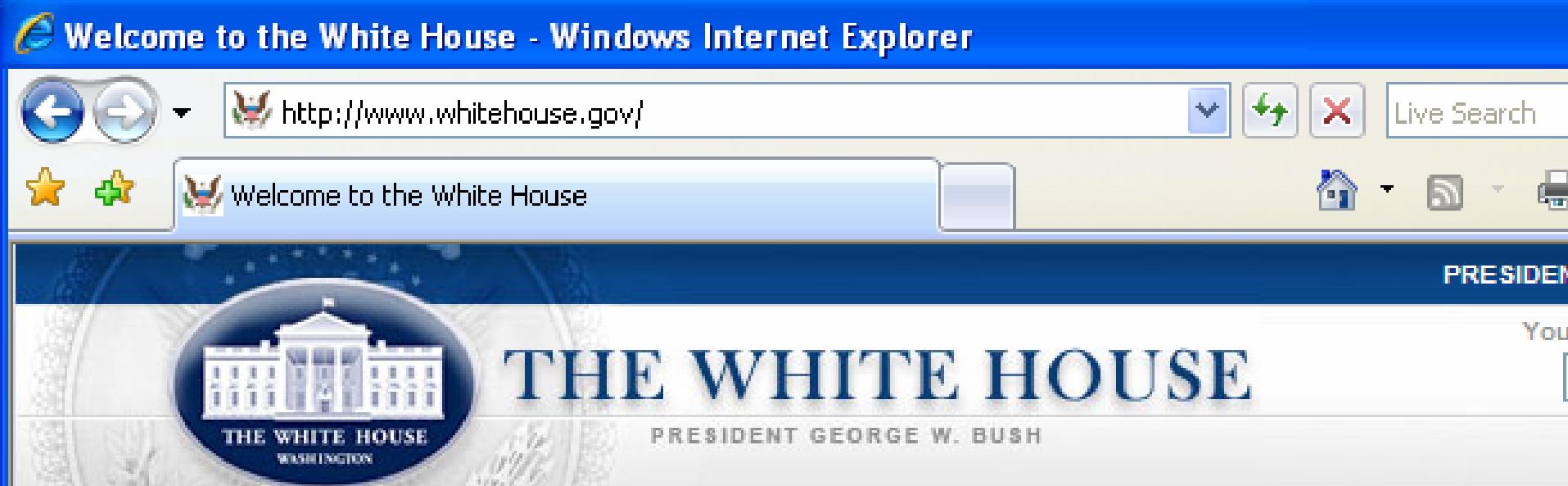
- EV-SSL ... relies on central authorities
- Passpet ... requires private key storage
- PwdHash
 - Similar hostname-based mangling
 - Weak against offline attacks



Page Transition Examples

Websites not supporting authentications

- Status: 200 OK
- No login field displayed



Welcome to the White House - Windows Internet Explorer

http://www.whitehouse.gov/

Welcome to the White House

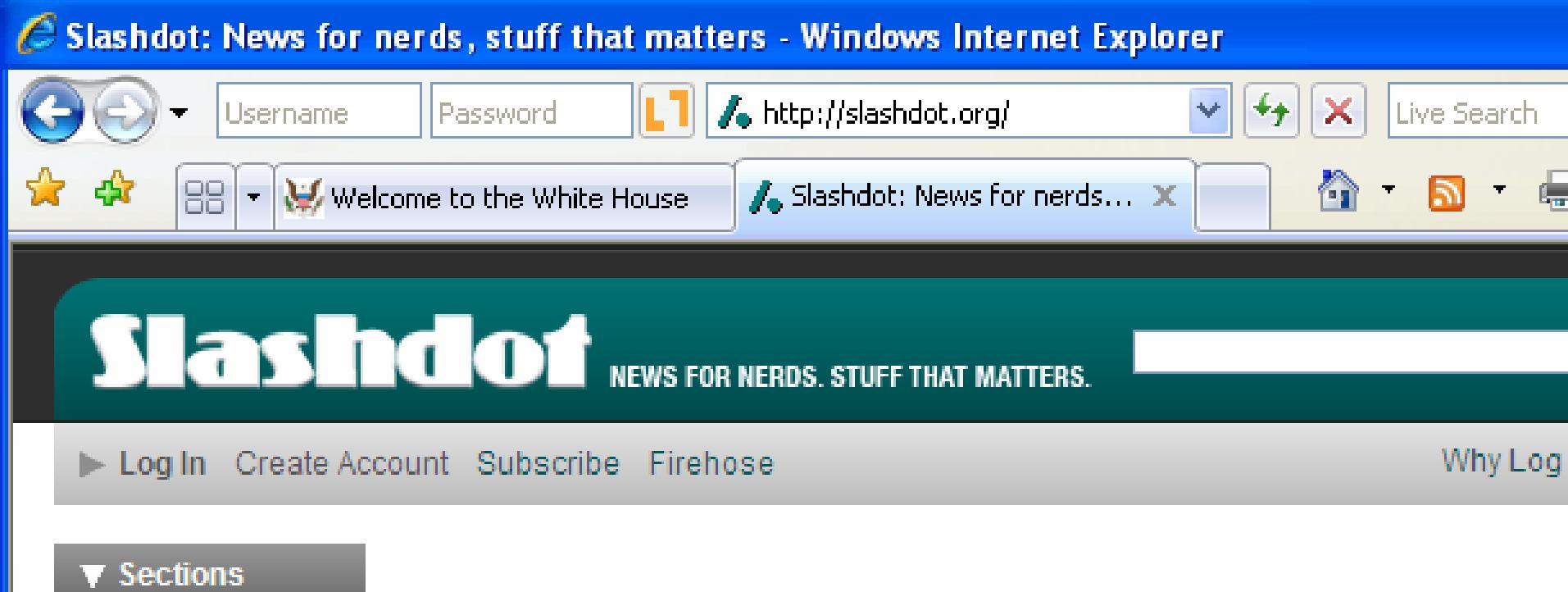
THE WHITE HOUSE

PRESIDENT GEORGE W. BUSH

The screenshot shows a Windows Internet Explorer window displaying the official website of the White House. The address bar shows the URL "http://www.whitehouse.gov/". The main content area displays the "Welcome to the White House" page, featuring the White House logo and the name "THE WHITE HOUSE" along with "PRESIDENT GEORGE W. BUSH". The browser interface includes standard navigation buttons (back, forward, stop, refresh), a search bar, and various toolbar icons.

Visiting Mutual-auth sites as guest

- Status: 200 OK
 - Optional-WWW-Authenticate: Mutual ...
- ID/Password box appears



The screenshot shows a Windows Internet Explorer window for the website <http://slashdot.org/>. The browser interface includes a toolbar with back, forward, search, and other navigation buttons. Below the toolbar, there are two input fields for 'Username' and 'Password'. The main content area displays the Slashdot homepage with the headline 'Welcome to the White House'.

Slashdot: News for nerds, stuff that matters - Windows Internet Explorer

Username Password <http://slashdot.org/>

Welcome to the White House Slashdot: News for nerds...

Slashdot NEWS FOR NERDS. STUFF THAT MATTERS.

Log In Create Account Subscribe Firehose Why Log

Sections

Switching Tabs

- Login field displayed/hidden, according to the status of each tab



Welcome to the White House - Windows Internet Explorer

http://www.whitehouse.gov/

Welcome to the White Ho... X

Slashdot: News for nerds, st...

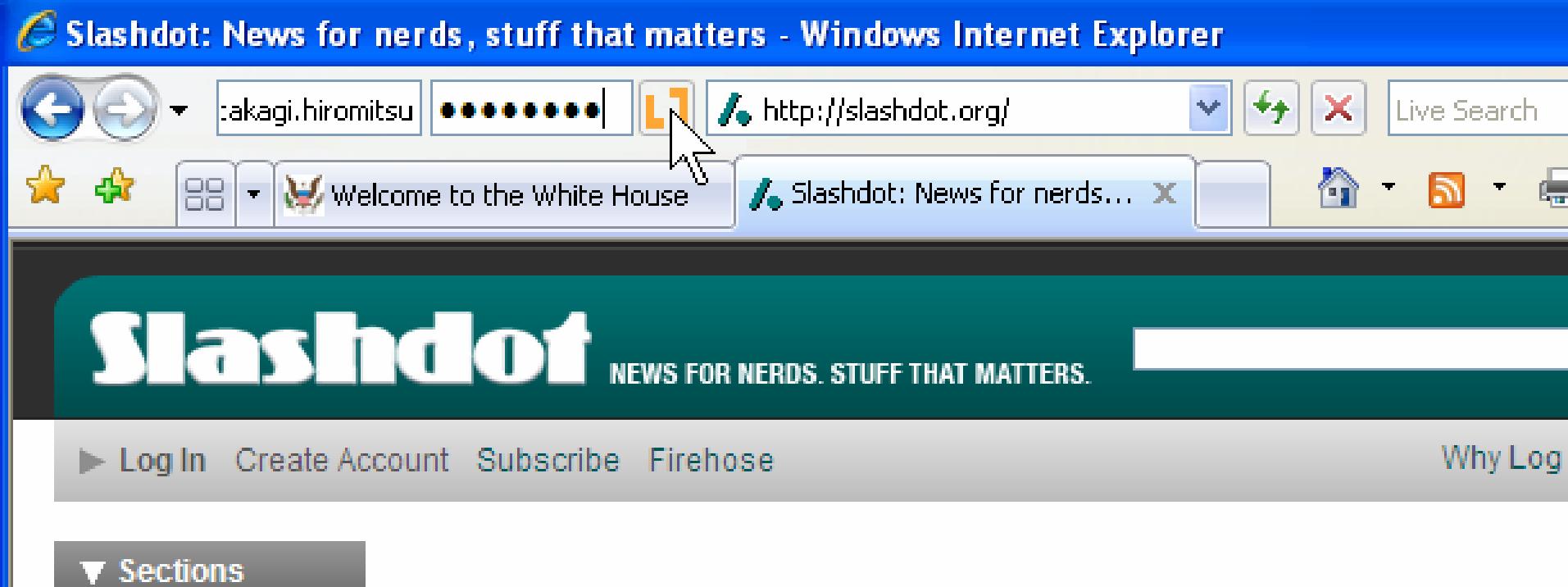
THE WHITE HOUSE

PRESIDENT GEORGE W. BUSH

The screenshot shows a Windows Internet Explorer window with two tabs open. The active tab is 'Welcome to the White House' (Windows Internet Explorer), which displays the official website for the White House. The second tab, 'Slashdot: News for nerds, st...', is visible in the background. The browser interface includes standard controls like back, forward, and search, as well as a toolbar with icons for favorite, new tab, and print.

Login!

■ Enter ID/password, click the button...



The screenshot shows a Windows Internet Explorer window with the following details:

- Title Bar:** "Slashdot: News for nerds, stuff that matters - Windows Internet Explorer"
- Address Bar:** Shows the URL `http://slashdot.org/`. To the left of the address bar is a text input field containing the placeholder `:akagi.hiromitsu`, followed by a password input field with several dots. A yellow "L1" button is positioned next to the password field, with a cursor arrow pointing towards it.
- Toolbar:** Standard IE toolbar icons for Back, Forward, Stop, Refresh, and Live Search.
- Taskbar:** Shows two open tabs: "Welcome to the White House" and "Slashdot: News for nerds...".
- Content Area:** The main content area displays the "Slashdot" logo and the tagline "NEWS FOR NERDS. STUFF THAT MATTERS."
- Navigation Bar:** At the bottom, there are links for "Log In", "Create Account", "Subscribe", "Firehose", and "Why Log".
- Footer:** A "Sections" menu is visible at the bottom left.

Login...

■ Waiting for authentication response



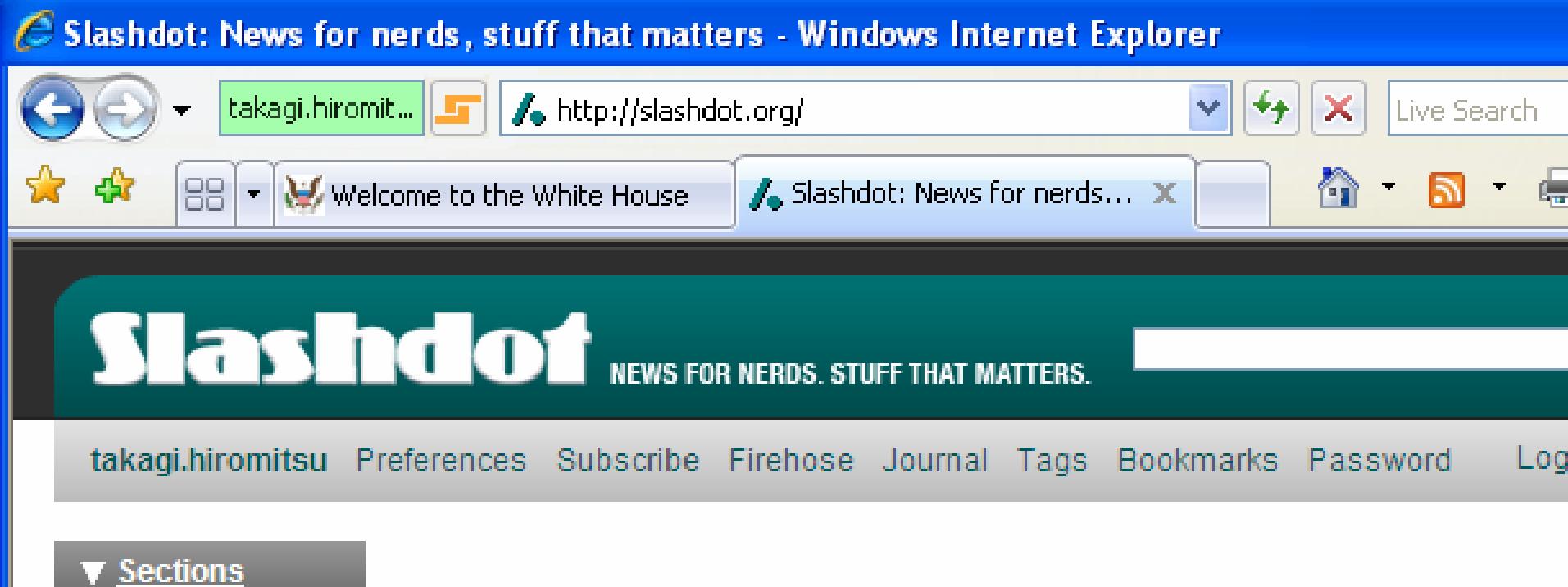
The screenshot shows a Windows Internet Explorer window. The title bar reads "Slashdot: News for nerds, stuff that matters - Windows Internet Explorer". The address bar shows the URL "http://slashdot.org/" and a user name "takagi.hiromitsu" followed by several dots. The toolbar includes standard buttons for back, forward, search, and live search. Below the toolbar, there are icons for bookmarks, windows, and a welcome message from the White House. The main content area displays the Slashdot homepage with the title "Slashdot" and the tagline "NEWS FOR NERDS. STUFF THAT MATTERS.". At the bottom, there are links for "Log In", "Create Account", "Subscribe", "Firehose", and "Why Log". A "Sections" menu is visible at the very bottom left.

Logged in

■ Status: 200 OK

■ Authentication-info: Mutual

■ ID indicated with green background



The screenshot shows a Windows Internet Explorer window displaying the Slashdot homepage. The browser's title bar reads "Slashdot: News for nerds, stuff that matters - Windows Internet Explorer". The address bar shows the URL "http://slashdot.org/" and the user's ID "takagi.hiromitsu". The main content area displays the "Welcome to the White House" banner and the "Slashdot: News for nerds..." news feed. The user's profile picture, "takagi.hiromitsu", is visible in the top right corner of the page. The browser interface includes standard buttons for back, forward, search, and refresh.

Switching Tabs

- Login status display changes still according to the status of each tab



Welcome to the White House - Windows Internet Explorer

http://www.whitehouse.gov/

Welcome to the White Ho... X

Slashdot: News for nerds, st...

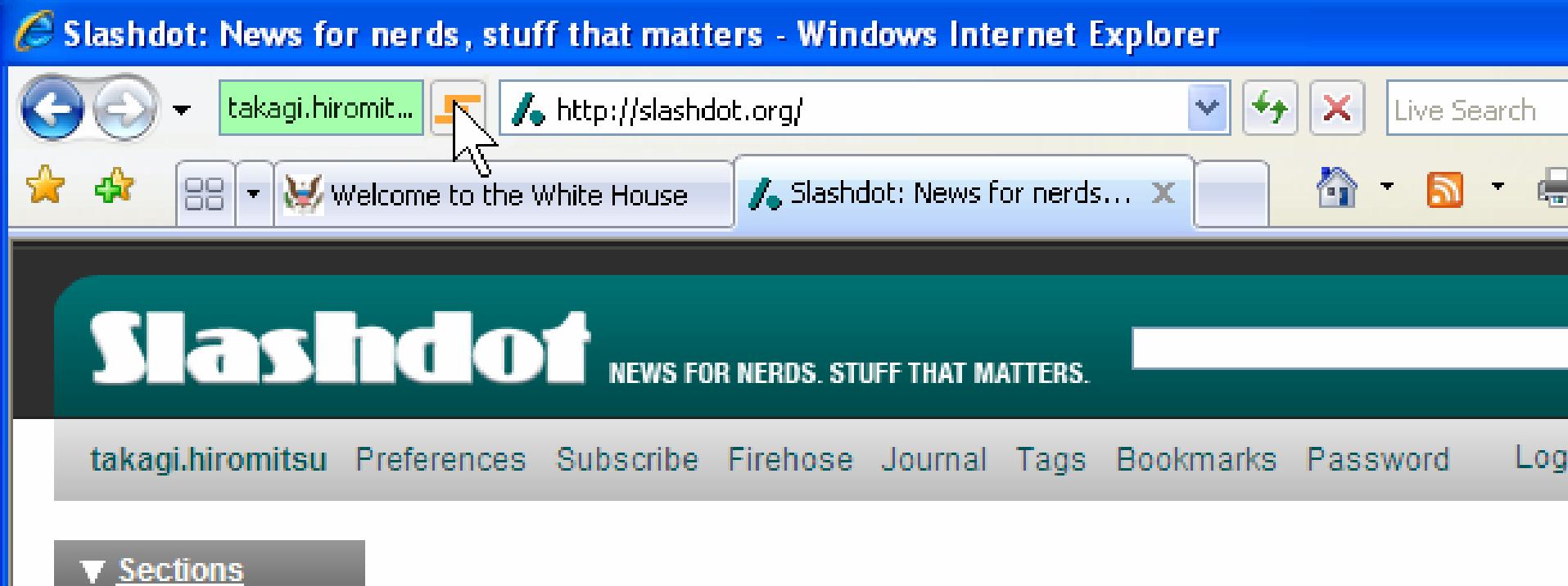
THE WHITE HOUSE

PRESIDENT GEORGE W. BUSH

The screenshot shows a Windows Internet Explorer window with two tabs open. The active tab is "Welcome to the White House" from the White House website. The second tab is "Slashdot: News for nerds, st..." from the Slashdot website. The browser interface includes standard controls like back, forward, and search, as well as icons for bookmarks and print.

Logout

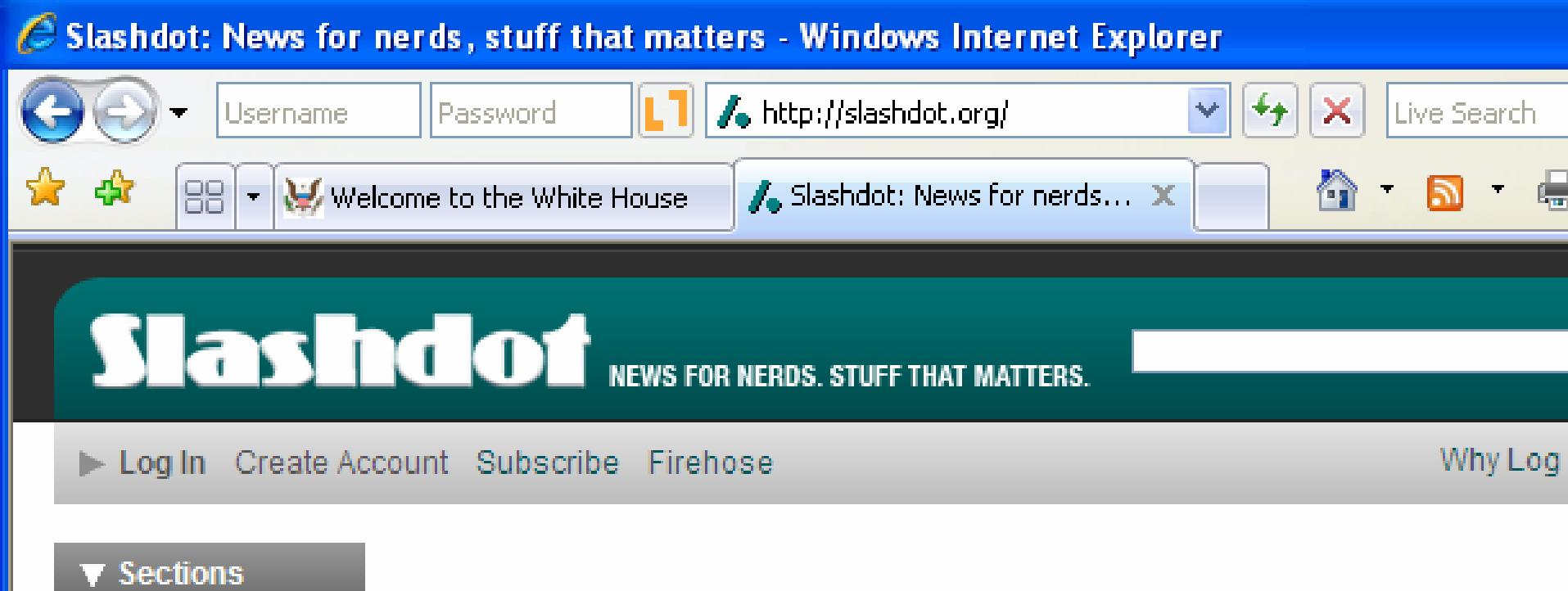
■ Click button to logout



The screenshot shows a Windows Internet Explorer window. The title bar reads "Slashdot: News for nerds, stuff that matters - Windows Internet Explorer". The address bar shows the URL "http://slashdot.org/" with a magnifying glass icon. Below the address bar are standard browser controls: back, forward, stop, refresh, and live search. The main content area displays the "Welcome to the White House" section of the Slashdot homepage. At the bottom of the page, there is a navigation menu with links: "takagi.hiromitsu", "Preferences", "Subscribe", "Firehose", "Journal", "Tags", "Bookmarks", "Password", and "Logout". A "Sections" button is located at the bottom left.

Logout

- Status: 200 OK
 - Optional-WWW-Authenticate: Mutual ...
- Contents reloaded, back to the guest state



The screenshot shows a Windows Internet Explorer window with the following details:

- Title Bar:** "Slashdot: News for nerds, stuff that matters - Windows Internet Explorer"
- Address Bar:** Shows the URL "http://slashdot.org/" with a "L1" icon.
- Toolbar:** Includes standard IE icons for Back, Forward, Stop, Refresh, and Live Search.
- Menu Bar:** Shows the "File" menu.
- Content Area:** Displays the "Welcome to the White House" banner from the Slashdot homepage.
- Bottom Navigation:** Includes links for "Log In", "Create Account", "Subscribe", "Firehose", "Why Log", and "Sections".