Evolution of browser security

Yngve N. Pettersen

Opera Software ASA

Security concerns 10 years ago

Main concerns revolved around problems with the technology, such as:

- Online tracking by cookies and referrers
- Shopping and payment online
- Security of transaction

Remedies

- Options in the client
- Best practices
- User education

Security concerns 5 years ago

Main focus turned to the client's own security and privacy

- Buffer overflows
- Vulnerabilties in image decoders
- Scripting engines
- Web beacons in HTML email

Solutions

- Better coding and testing
- Disabling problematic features by default

Security concerns at present

Primary concern now is organized crime

- Fraud using spoofing and XSS attacks
- Drive-by malware, such as keyloggers
- DNS cache poisoning to facilitate crime

Current solutions being tested

- Blacklists
- Detecting and blocking problematic behavior
- Upgrading infrastructure

Current security projects

- Standardizing security UI (W3C Web Security Context)
- Securing JavaScript
- Securing against some XSS methods
- Encouraging good use of encryption

On the horizon

- Phorm-type networks
- Securing Web 2.0 sites
- Browsers already complex, plug-ins creating more complexity
- Government tracking of online activity

Proper use of encryption

Using encryption properly can be hard, and a group of problems is constantly recurring

- Log-in from unsecure page
- Mixing secure and unsecure content

Login from unsecure page

- No good way to tell how credential will be sent
- Login form can be hijacked, no way to tell
- Convenience vs. security
- Have been used by many banks

Mixing secure and unsecure content

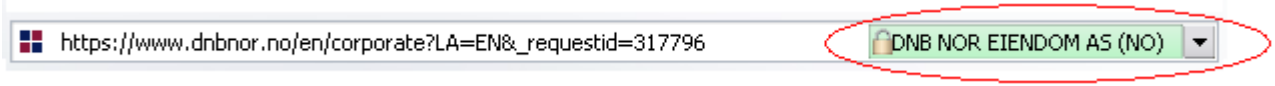
- Unsecure images and frames can leak information about activities
- Scripts and CSS can give an attacker full control over a page
- Observed on banks and shopping sites
- Still prevalent despite several major clients displaying warnings
- Hard blocking by clients may be necessary

Extended Validation (EV) Certificates

EV was developed by CAs and browser vendors for validating information in SSL certificates

The purpose is to provide better assurance of Web site identity

- The validation process is audited regularly
- Issued certificates contain special flags recognized by clients
- Client recognizing an EV certificate enable visually distinct UI



- Currently deployed in (at least) Firefox 3, MSIE 7, Opera 9.50

Plug-ins

Plug-ins are thirdparty application running in the context of the browser.

- Security problems in a plug-in affects the browser directly
- Primary problem is that plug-ins are not updated by users
- Possible solution: Version blacklists used by clients

The next wave of security problems?

Possible candidates:

- Phorm-type Deep Packet inspection advertising
- Attacks on *implementations* of popular new technologies. Examples of current candidates: SVG and Webfonts
- Attacks on infrastructure, such as DNS
- Goverment surveillance and record keeping

yngve@opera.com

http://www.opera.com/

http://my.opera.com/yngve/