By Tobias Pulls

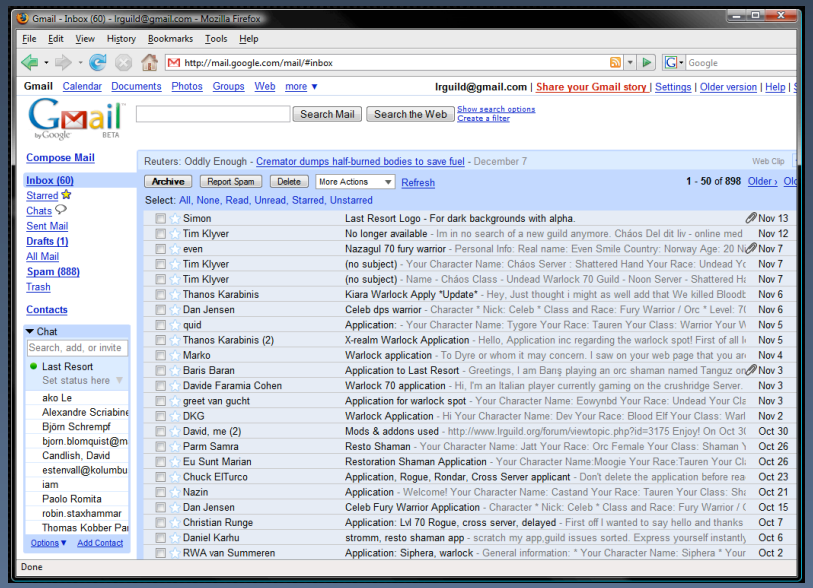
RICH INTERNET APPLICATIONS SUCK (FROM A SECURITY PERSPECTIVE)

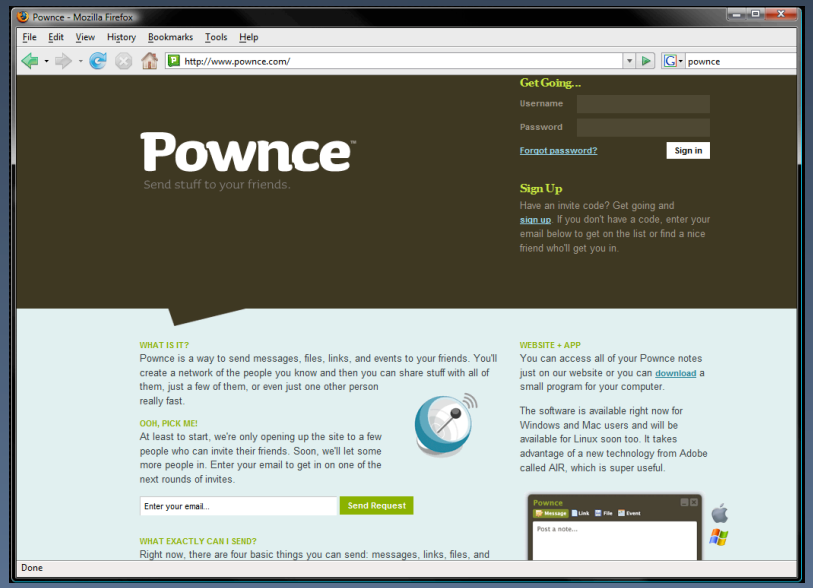
Index

- The problem and background information.
- Examples of why it’s really a problem.
- Scope and protection.
- Reflections and summary.

Rich Internet Applications

- "Rich Internet applications (RIA) are web applications that have the features and functionality of traditional desktop applications. RIAs typically transfer the processing necessary for the user interface to the web client but keep the bulk of the data (i.e., maintaining the state of the program, the data etc) back on the application server."
  – http://en.wikipedia.org/wiki/Rich_Internet_application





The web model ”web 1.0”

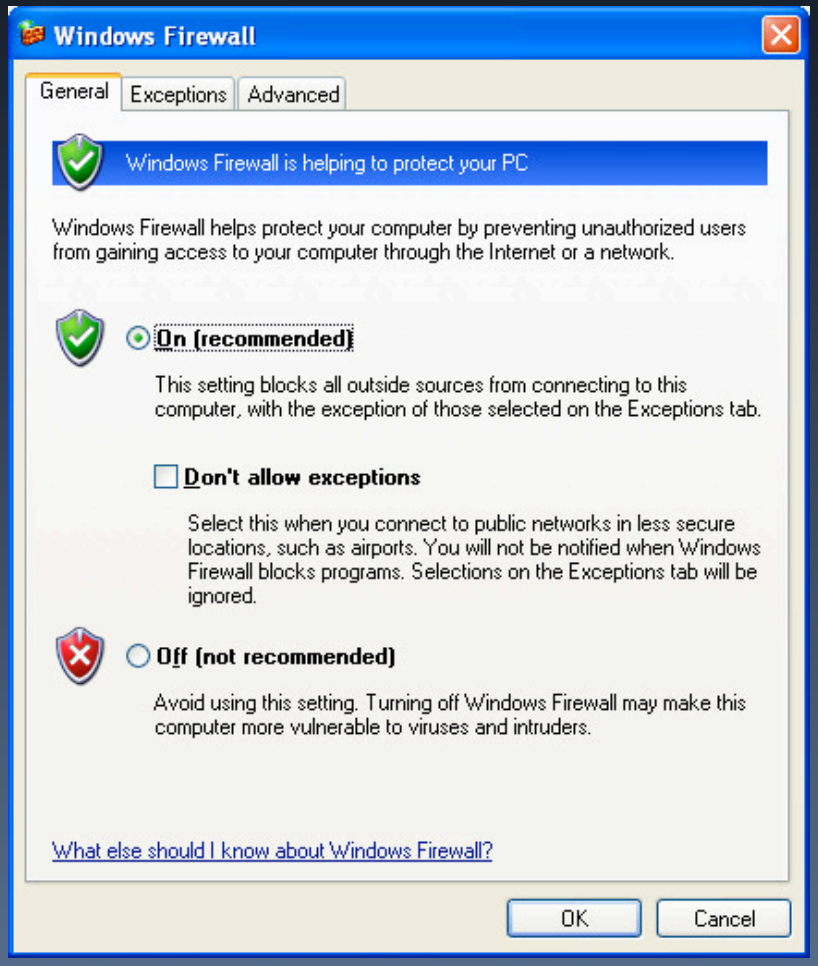
- The browser fetches static content (HTML or images) and renders.
- Forms and special URLs used to send data back to the server.
- Lacks a lot of features.

New technologies ”web 2.0”

- ActiveX
  - Download and execute, by design!
- Java
  - Sandboxed, more security aware.
- Javascript
  - Sandboxed and constrained.
- Flash/Flex/AIR
  - Sandboxed and constrained.

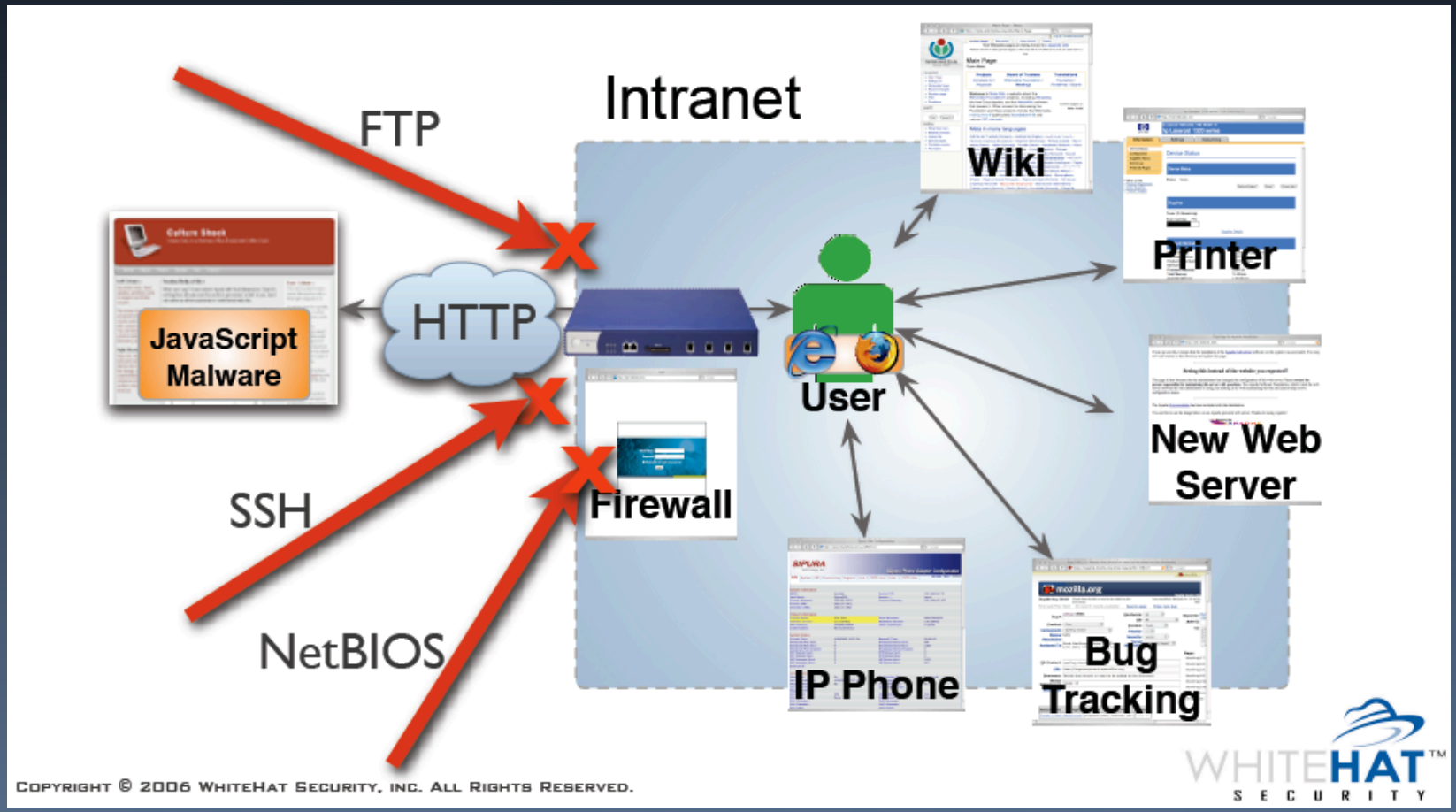
- These techniques **break** the 1.0 model.

Why are RIAs so important?



- Windows XP SP2.
  - The firewall on by default!
- NAT routers are common.
- Reduces the attack surface significantly.
  - E-mail and the web browser the new

How RIAs are dangerous



Fun with Javascript

- Port scan.
  - Use an IP as a source of a script, if it returns any HTML the JS interpreter will generate an error.
- Identifty running web servers (fingerprinting).
  - URL's to images that are unique.

- Find out if a user has accessed a specific site.
  - Read the color of the link.
- Configure routers, printers etc.
  - http://admin:password@192.168.0.1

Fun with Javascript contd.

- Click-fraud.
- DDoS.
- Hijack sessions.
  - Steal cookies.
- Force access of illegal content or restricted area.
- Distributed blog or e-mail spam.
  - Any POST or GET data.

Fun with Java and Flash

- De-anonymize people.
  - Javascript generates Java that opens a socket.
  - Java doesn't use the browsers proxy settings.
- Flash cookies.
  - Like regular cookies but bigger (4kb vs 100kb).
  - Not removed together with other cookies.
- Portscan with Flash.

Anybody can be a victim

- Cross-site scripting (XSS).
  - Code injection into web pages viewed by others.
- Myspace ”Samy worm” – first XSS worm.
  - Over 1 million effected in 24h.
  - ”Samy is my hero”.
- Advertisement often included from

Cross-site request forgery

- Denoted CSRF or XSRF.
- Almost the opposite to XSS.
  - Exploits the trust a website has in a user.
  - Even more common then XSS vulnerabilities.
-

Protection

- XSS and CSRF prevention is entirely up to developers.
  - Frameworks.
- Same origin policy.
  - Protocol, domain name and port.
  - Issues with file:// and dynamic objects.
- Security Zones in IE or extensions like NoScript for Firefox.
  - Opt-in.

Not present by default

- Why not?
  - It's tedious to whitelist sites all the time.
  - It will break a lot of sites.
  - Not enough bad stuff taking place, yet.
  - Advertisement.

Summary and reflections

- RIA technologies break the old ”web model”.
  - Executes code on the client.
- You can do a lot of evil stuff with Javascript, Java and Flash.
- Windows XP SP2 firewall enabled by default.

Sources

- Hacking intranet websites from the outside.
  - By Jeremiah Grossman.
  - Presented during Blackhat 2006.
  - http://www.blackhat.com/presentations/bh-jp-06/BH-JP-06-Grossman.pdf
- (IN)SECURE Magazine #14 – page 29 to 32.
  - http://www.net-security.org/dl/insecure/