Confidence in a connected world.

JavaScript Breaks Free

Zulfikar Ramzan
Symantec Security Response

Joint w/ Markus Jakobsson, Sid Stamm (Indiana Univ)

Outline

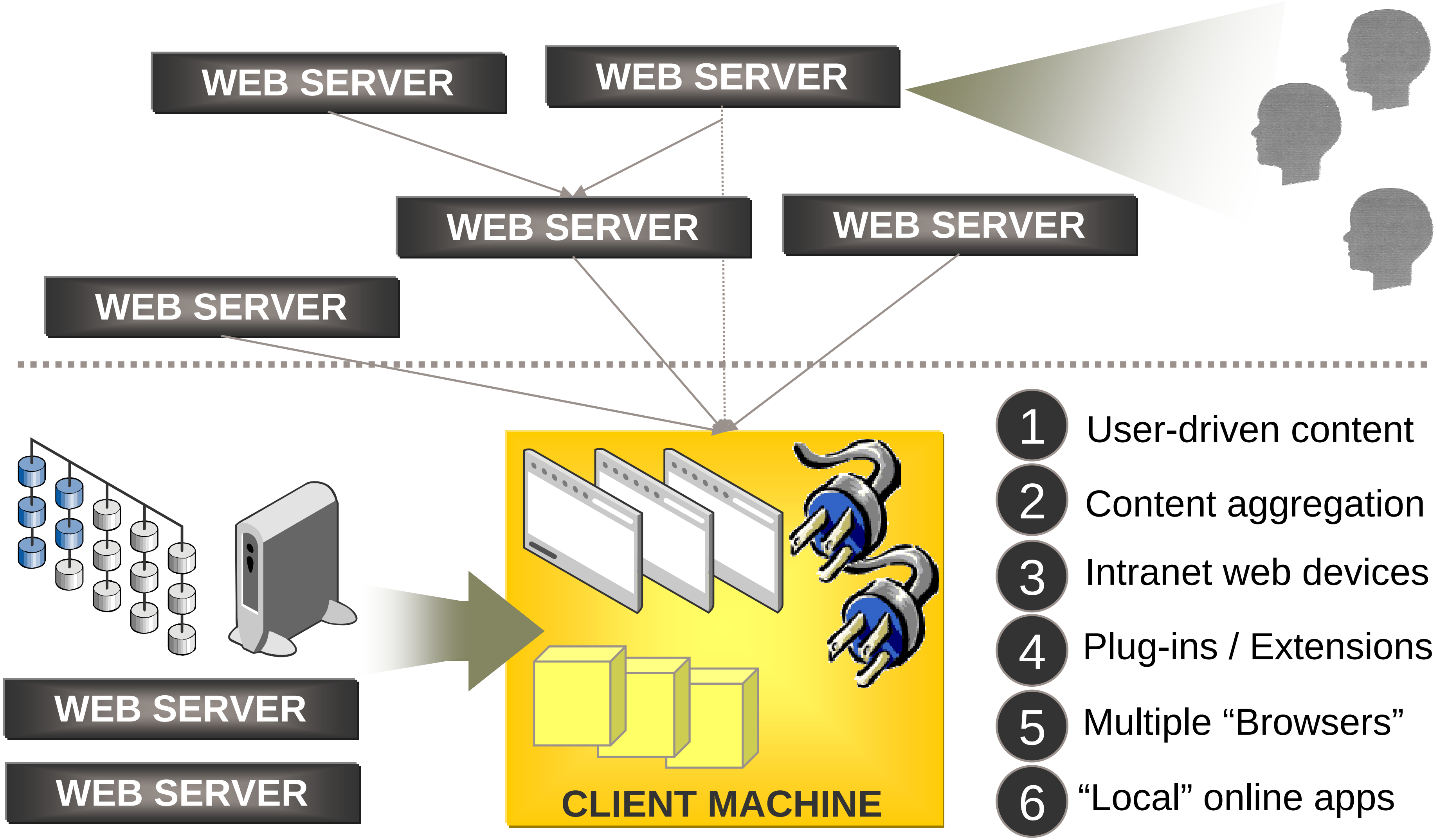
1 The Web 2.0 Security Picture

2 Position: Boundary Challenges

3 Example: Drive-by Pharming

4 Other Examples and Parting Thoughts

The Web 2.0 Picture

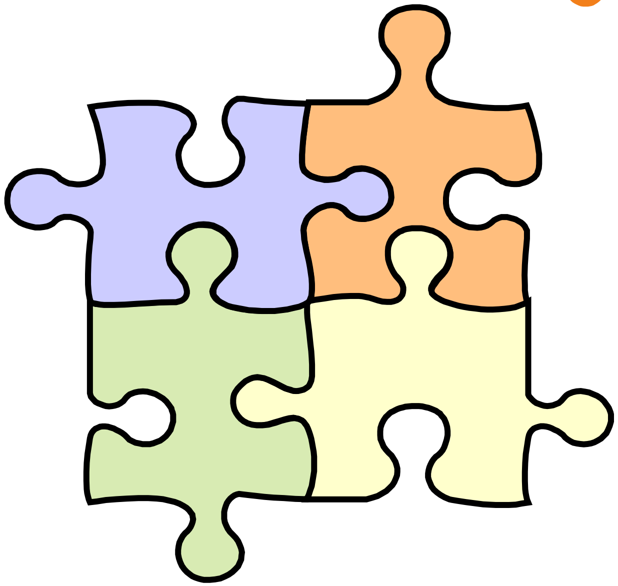


1. User-driven content
2. Content aggregation
3. Intranet web devices
4. Plug-ins / Extensions
5. Multiple “Browsers”
6. “Local” online apps

What Makes it Hard

- Unprecedented amount of content (not always trustworthy)
- Aggregation of content on local client and also by intermediaries (same-origin policy workarounds)
- Intranet devices often have web servers (internet/intranet boundary issues)
- Web browsers augmented with plug-ins (not always trustworthy & complicate interactions)
- Machines may have many local web browsers that communicate over HTTP, render HTML, and emulate JavaScript (increased attack surface).
- Some local client applications can interact with web browser and provide combined online / offline capabilities (compromises can lead to machine ownership).

Main Position Points and Examples

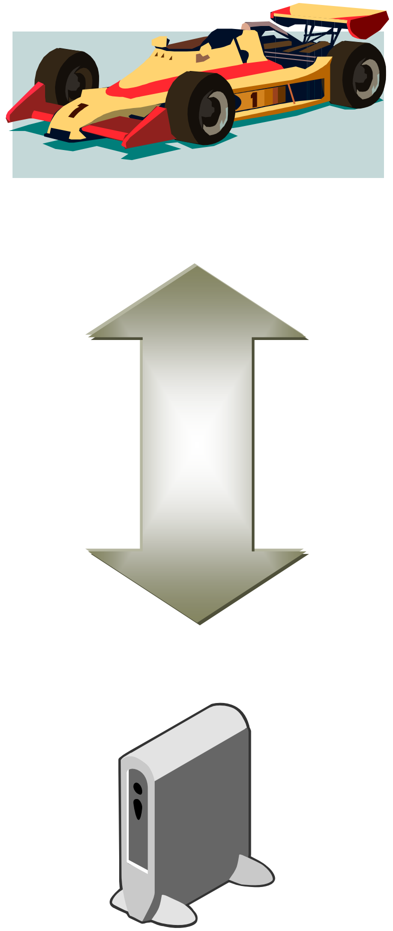


> *There are many pieces in the puzzle. The policies governing boundaries between these pieces needs to be better understood and better enforced.*

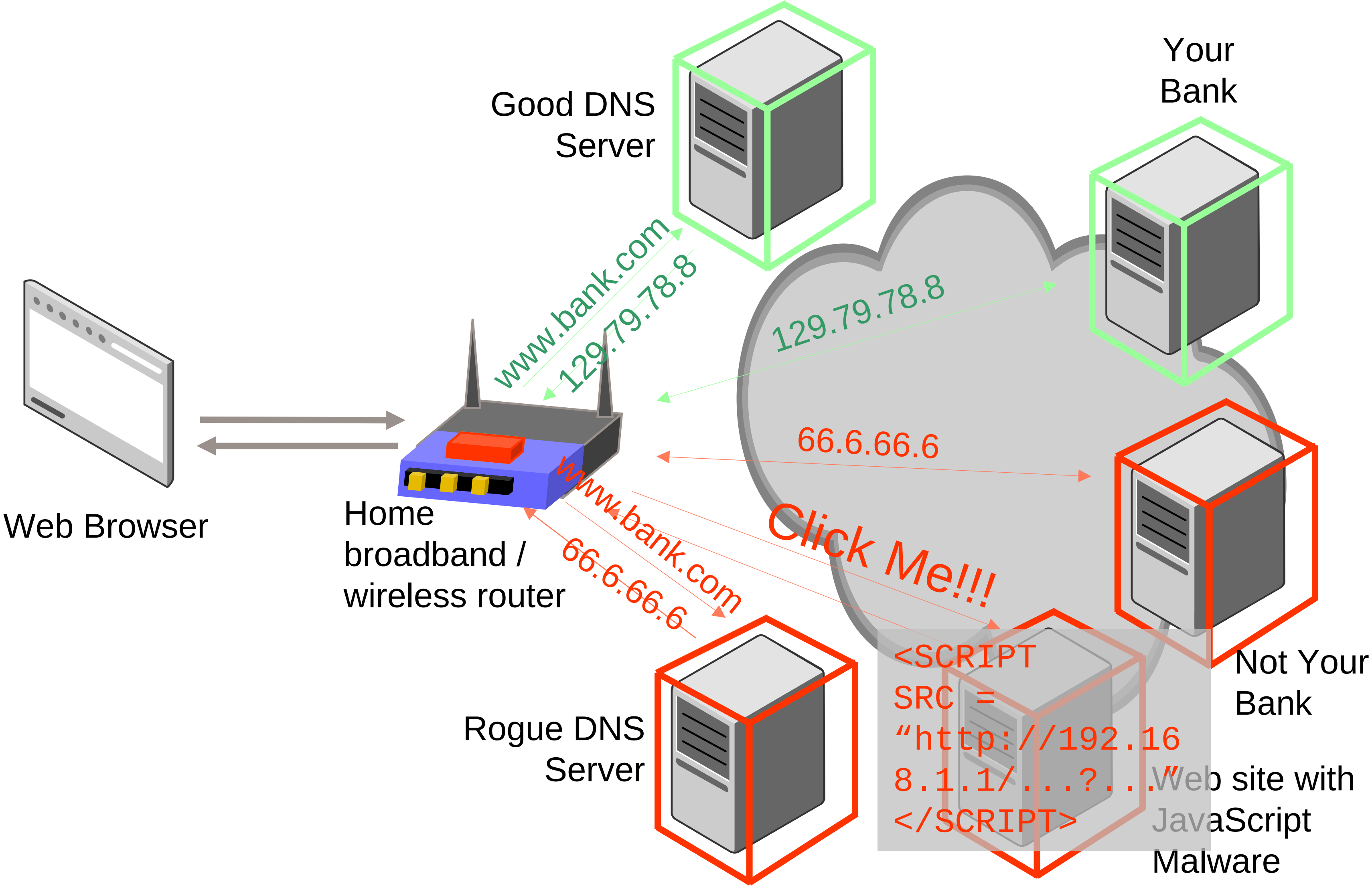
*If we get this wrong, *-script code running in one context, can affect another. Example: Drive-by Pharming.*

Drive-by Pharming Overview

- Attack concept developed by Sid Stamm, Markus Jakobsson, and me that strongly leverages prior work on JavaScript host scanning presented by Grossman at BlackHat.
- Local broadband routers (both wired and wireless) offer a web management interface for device configuration
  - Consequently, these devices contain a web server that runs a web app
- The web app is often susceptible to cross-site request forgeries (made easier since there is usually a default password that users often fail to change)
- Broadband routers govern DNS settings…
- Can change these settings from a remote location; victim only has to view web page containing malicious JavaScript to become infected



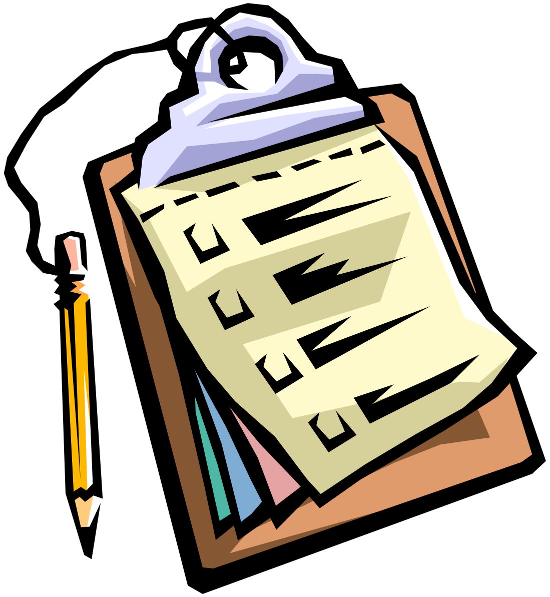
Drive-by Pharming Flow



```
<SCRIPT SRC = “http://192.168.1.1/...?...” </SCRIPT>
```

Drive-by Pharming Current Status

- Working proof of concept code for various Linksys, Netgear,and DLINK routers
- No known instances In the Wild yet
- Similar concept can be used to upgrade router firmware
- Solutions
  - Simple bandaid: change password on home router
  - More fundamental: protect the web app on the router from Cross-Site Request Forgeries
  - Way to implement second sol’n: web app requires and validates unpredictable value hidden somewhere on web page containing config. management interface



Other Examples and Parting Thoughts

- Other Examples:
  - Overtaking Google Desktop (Amit, Allan & Sharabani)
  - Universal XSS (Di Paola & Fedon)
- Not understanding boundaries associated with the plethora of component and failing to understand and enforce policies governing boundaries can have devastating consequences
- Things are getting more complex! New technologies like Silverlight, etc., are looming.