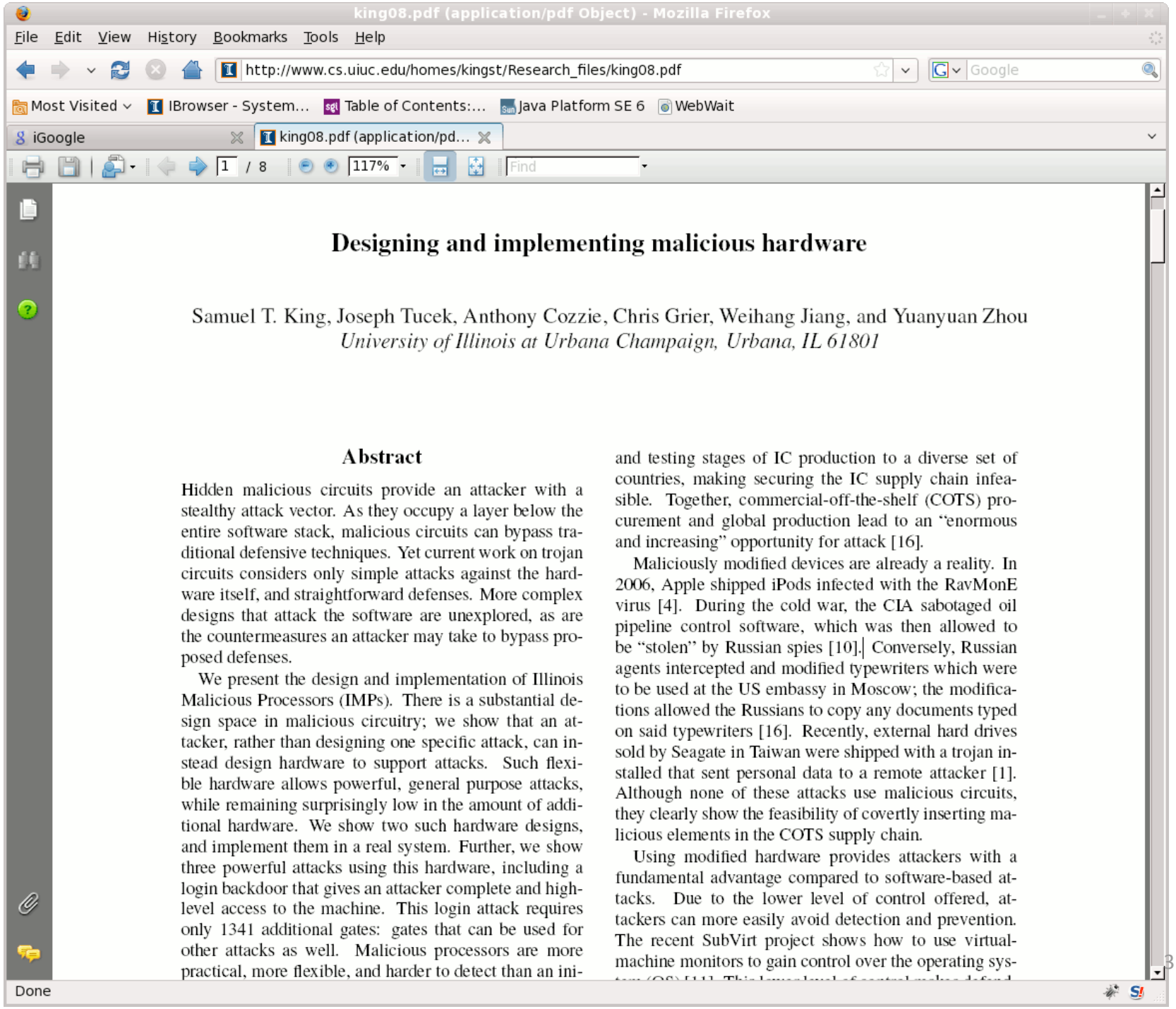
How I Learned to Stop Worrying and Love Plugins

Chris Grier, Samuel T. King, Dan S. Wallach

UIUC, Rice University

Browser Plugins

- Plugins enable new types of content to be displayed by browsers
- Rich media, interactivity
- Last year 419 disclosed plugin vulnerabilities
  - Acrobat, Flash, Java, etc…
- Plugins can provide a direct means to take over computer systems
  - 99% of Internet users have at least one plugin installed



Designing and implementing malicious hardware

Samuel T. King, Joseph Tucek, Anthony Cozzie, Chris Grier, Weihang Jiang, and Yuanyuan Zhou
University of Illinois at Urbana Champaign, Urbana, IL 61801

Abstract

Hidden malicious circuits provide an attacker with a stealthy attack vector. As they occupy a layer below the entire software stack, malicious circuits can bypass traditional defensive techniques. Yet current work on trojan circuits considers only simple attacks against the hardware itself, and straightforward defenses. More complex designs that attack the software are unexplored, as are the countermeasures an attacker may take to bypass proposed defenses.

We present the design and implementation of Illinois Malicious Processors (IMPs). There is a substantial design space in malicious circuitry; we show that an attacker, rather than designing one specific attack, can instead design hardware to support attacks. Such flexible hardware allows powerful, general purpose attacks, while remaining surprisingly low in the amount of additional hardware. We show two such hardware designs, and implement them in a real system. Further, we show three powerful attacks using this hardware, including a login backdoor that gives an attacker complete and high-level access to the machine. This login attack requires only 1341 additional gates: gates that can be used for other attacks as well. Malicious processors are more practical, more flexible, and harder to detect than an ini-

and testing stages of IC production to a diverse set of countries, making securing the IC supply chain infeasible. Together, commercial-off-the-shelf (COTS) procurement and global production lead to an "enormous and increasing" opportunity for attack [16].

Maliciously modified devices are already a reality. In 2006, Apple shipped iPods infected with the RavMonE virus [4]. During the cold war, the CIA sabotaged oil pipeline control software, which was then allowed to be "stolen" by Russian spies [10]. Conversely, Russian agents intercepted and modified typewriters which were to be used at the US embassy in Moscow; the modifications allowed the Russians to copy any documents typed on said typewriters [16]. Recently, external hard drives sold by Seagate in Taiwan were shipped with a trojan installed that sent personal data to a remote attacker [1]. Although none of these attacks use malicious circuits, they clearly show the feasibility of covertly inserting malicious elements in the COTS supply chain.

Using modified hardware provides attackers with a fundamental advantage compared to software-based attacks. Due to the lower level of control offered, attackers can more easily avoid detection and prevention. The recent SubVirt project shows how to use virtual-machine monitors to gain control over the operating sys-

Tuesday news

Drive-By Download Poisons Google Search Results

Posted by timothy on Tuesday May 19, @08:53AM
from the **monocultural-imperialism** dept.

snydeq writes

> "A new attack that peppers Google search results with malicious links is spreading quickly, CERT has warned. The attack, which can be found on several thousand legitimate Web sites, exploits flaws in Adobe software to install malware that steals FTP login credentials and hijacks the victim's browser, replacing Google search results with links chosen by the attackers. Known as Gumblar because at one point it used the Gumblar.cn domain, the attack is spreading quickly in part because its creators have been good at obfuscating their attack code and because they are using FTP login credentials to change folder permissions, leaving multiple ways they can get back into the server."

▶ google it worms noscript tech security story

Flash, Acrobat vulnerabilities used for drive-by download

CERT release says malware redirects Google search results

Yahoo! – Opus Palladianum

File Edit View History Bookmarks Window Tools Help

http://www.yahoo.com/

Google

UIUC CS Slashdot NYTimes ESPN Urbana Weather Forecast and Conditions Illinois (61801)

Yahoo!

Make Y! your home page

Netflix: $4.99/mo. Movies delivered, no late fees

YAHOO!

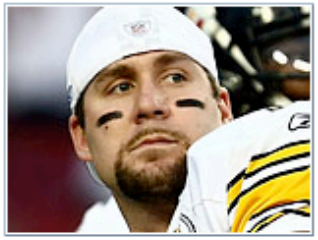
Web | Images | Video | Local | Shopping | more

Search: Web Search

Yahoo! Home My Yahoo! Feb 9, 2009 Page Options

- Answers
- Autos UPDATED!
- Finance
- Games
- Groups
- HotJobs
- Maps
- Mobile Web
- Movies | TV
- Music
- OMG
- Personals
- Real Estate
- Shine
- Shopping

Featured | Entertainment | Sports | Video



Stunning Super Bowl story

Ben Roethlisberger reveals that he played with a major injury when the Steelers won the title. » Details

- Fitzgerald wins MVP a week too late
- Ex-NFL star released from jail


QB's stunning revelation about the Super Bowl


Tiger Woods and wife welcome new baby


Companies that may not survive 2009


Best and worst dressed at the Grammy Awards

» More: Featured | Buzz

News | World | Local | Finance

As of 1:05 p.m. CST

- Obama: Stimulus package is the right size and scope
- Australia bushfires: 'It is a fiery hailstorm from hell' | Photos
- SEC, Madoff agree to settle civil lawsuit for $50B Ponzi scheme
- Italy Senate pushing bill to force life support for coma victim

Check your mail status: Sign In Free mail: Sign Up

Mail | Messenger | Puzzles | Weather | Events | Horoscopes

http://www.yahoo.com/s/1027905

Redressing Flash

UI Redress attack against Flash

- http://www.flickr.com/photos/24967759@N00/2924995732/

Current state of the art

- FF/IE8
  - No control over plugins
  - ActiveX still poses substantial security risks
- Chrome, OP, Gazelle
  - Plugins isolated from browser
  - OP/Gazelle -- plugins use browser kernel
  - Chrome supports using sandbox for plugins
  - What policies to enforce?

Plugin policies

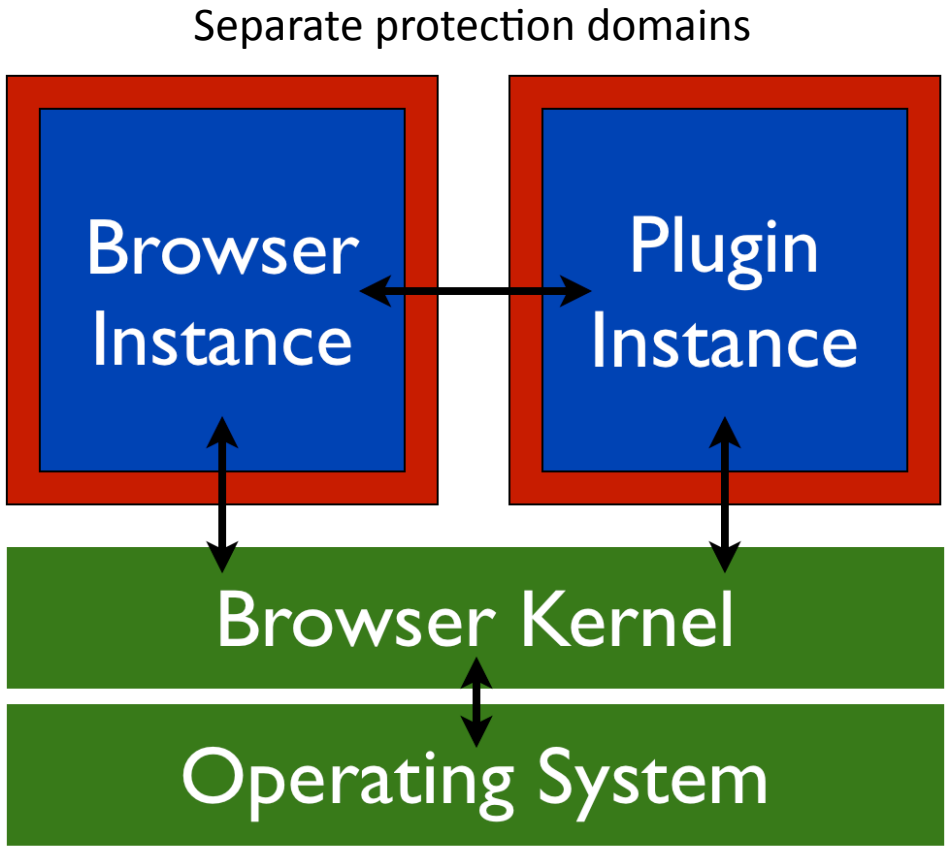
- What plugin policies should we use?
- Start looking at tradeoffs with security vs. functionality and compatibility

Outline

- Browser and plugin architectures
- Plugin capabilities
- Proposed policies
- Preliminary Flash study

Isolating plugins

- Plugin in a sandbox
  - Required to use browser
  - Prevent system damage
- Browser handles plugin access
- Possible sandboxes include
  - NaCl, OS-level sandboxes, others

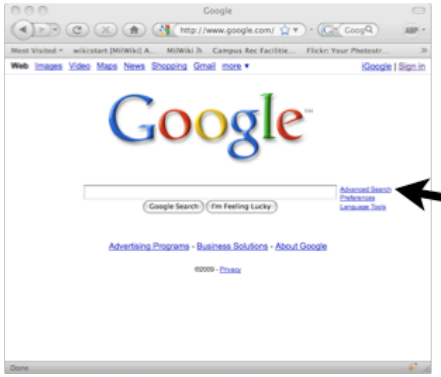


Benefits of using browser

- Browser has semantic information from parsing page
  - Can use HTML attributes, tags
- Users have a single place for configuration of security policy

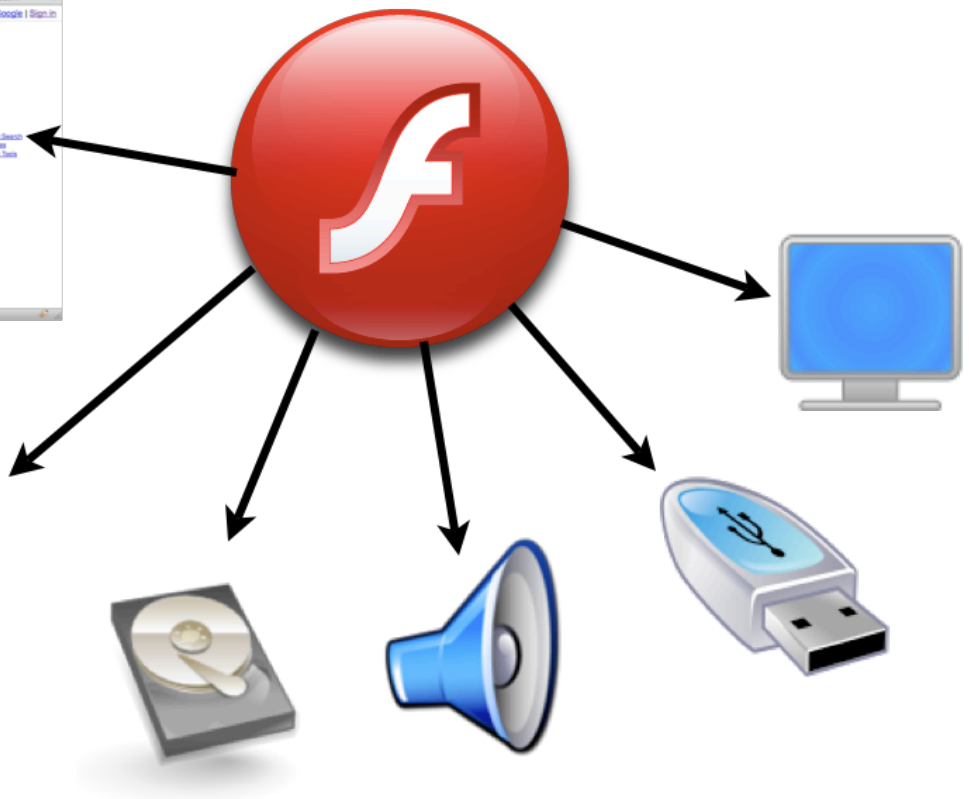
Plugin capabilities

- DOM
- Network
- Storage
- Devices



web page

(the internet)



Proposed policies

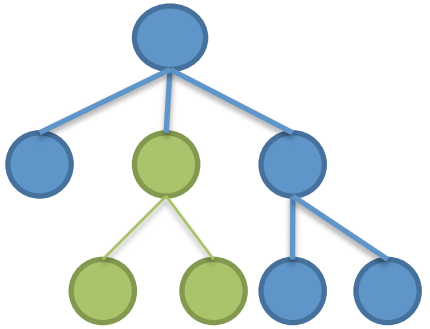
- Goal: Determine acceptable policies for plugins

- Policy for each of the different areas of access
- The mechanism exists, we need to develop policies that are reasonable
  - Allow functionality
  - Use browser to enforce security

- Many possibilities, more detail in paper

Document access

- Rooted subtree
  - Web page author specifies an element for plugin
  - Plugin has access to the element, can modify subtree



- Clean document
  - Provide the plugin with access to the tags and structure
  - Remove text, attributes

Persistent state

- Jailed access
  - Filesystem is accessed through chroot type jails
- Automatic
  - Determine global vs. local state automatically
  - Partition the plugins accesses

Network access

- Same-company
  - Origin too fine, should abstract to handle popular use like content delivery networks
  - DNS lookups provide hints for domain ownership
- All-or-one
  - Plugins can choose: any network access or local system access but not both

Device access

- Don’t let plugins determine access on their own
  - Page, user, and plugin can provide hints
- Capabilities
  - Page defines a set of capabilities a plugin can request, browser policy can be more or less restrictive
  - Embedding an ad? No device access.
  - Embedding a game? Sound playback only.

What to fix first

- A quick look at what Flash does online
- Minimize impact on backwards compatibility - get the mechanisms and policy in place.
- Download random SWFs, decode and inspect which APIs are used
  - Networking/Socket: 68%
  - ExternalInterface, LocalConnection: 1%
  - FileReference: <1%
  - Media APIs for camera/mic access: 2%
  - Shared objects (flash cookies): 2%

Conclusion

- Plugins significantly enhance the web experience
  - Adds great functionality
  - With significant security problems
- Browser controls can enable security without losing functionality
- Commercial and research browsers have mechanisms but we need good policies

Questions?

Specific Flash use

- Advertisement (MS Flash ad on Facebook)
  - No network, filesystem, document
  - Sound device opened
- Game (Pandemic 2)
  - No document, fs access
  - Plays sound, opens new tabs for web pages
- Video (Hulu)
  - Stores settings using flash cookies
  - Fetches video content with networking API
  - No document access
  - Full-screen, video and sound