



SECURITY AND PRIVACY ISSUES OF MODERN WEB BROWSERS

Nick Nikiforakis

April 2018



We've come a long way

The image shows a desktop environment with two windows. The background window is a web browser displaying the GNU Operating System website. The foreground window is the NCSA Mosaic browser, showing its home page.

GNU Operating System - Free Software Foundation (FSF)

FSF | [FSF Europe](#) | [FSF India Translations](#) of this page

GNU Operating System - Free Software Foundation

[Free as in Freedom](#)

Welcome to the GNU Project web server, [www.gnu.org](#). The [GNU Project](#) was launched in 1984 to develop a complete UNIX style operating system which is [free software](#): the GNU system. (GNU is a recursive acronym for "GNU's Not UNIX"; it is pronounced "guh-noo".) Variants of the GNU operating system, which use the kernel Linux, are now widely used; though these systems are often referred to as "Linux", they are more accurately called [GNU/Linux systems](#).

This is also the web site of the [Free Software Foundation](#) (FSF). FSF is the principal organizational sponsor of the GNU Project. FSF receives very little funding from corporations or grant-making foundations. We rely on support from individuals like you who support FSF's mission to preserve, protect and promote the freedom to use, study, copy, modify, and redistribute computer software, and to defend the rights of Free

NCSA Mosaic Home Page - NCSA Mosaic

File Edit Source Manager View Navigate Tools Hotlists Help

<http://www.ncsa.uiuc.edu/SDG/Software/Mosaic/>

N C S A
MOSAIC
X Window System • Microsoft Windows • Macintosh

Welcome to NCSA Mosaic, an Internet information browser and [World Wide Web](#) client. NCSA Mosaic was developed at the [National Center for Supercomputing Applications](#) at the [University of Illinois](#) in Urbana-Champaign. NCSA Mosaic software is [copyrighted](#) by The Board of Trustees of the University of Illinois (UI), and ownership remains with the UI.

NCSA Mosaic Photo CD Metasearch

Modern browsers are all-inclusive software platforms

- Modern browsers are constantly evolving
 - Streamlined extension frameworks
 - Push notifications
 - Custom web components
 - WebRTC
 - Payment Request API
- Rough size statistics (LOC = Lines of Code)
 - Google Chrome: 16 M. LOC
 - Mozilla Firefox: 18 M. LOC
 - Linux Kernel: 16.8 M. LOC

More features, greater attack surface

- As we keep on adding more and more features, we are expanding the attack surface of the browser
 - We are also increasing the chance of unpredicted interactions between software components
- Security 101: Where do flaws arise from?
 - Design flaws
 - Flaws that arise during the design phase of software
 - Implementation flaws
 - Buffer overflows, dangling pointers, XSS
 - Configuration flaws
 - Setting up software with guessable passwords



More features, greater attack surface

- As we keep on adding more and more features, we are expanding the attack surface of the browser
 - We are also increasing the chance of unpredicted interactions between software components
- Security 101: Where do flaws arise from?
 - Design flaws
 - Flaws that arise during the design phase of software
 - Implementation flaws
 - Buffer overflows, dangling pointers, XSS
 - Configuration flaws
 - Setting up software with guessable passwords



XHOUND: Quantifying the Fingerprintability of Browser Extensions

Oleksii Starov
Stony Brook University
ostarov@cs.stonybrook.edu

Nick Nikiforakis
Stony Brook University
nick@cs.stonybrook.edu

IEEE S&P 2017

Hindsight: Understanding the Evolution of UI Vulnerabilities in Mobile Browsers

Meng Luo, Oleksii Starov, Nima Honarmand, Nick Nikiforakis
Stony Brook University
{meluo, ostarov, nhonarmand, nick}@cs.stonybrook.edu

CCS 2017

XHOUND: Quantifying the Fingerprintability of Browser Extensions

Oleksii Starov
Stony Brook University
ostarov@cs.stonybrook.edu

Nick Nikiforakis
Stony Brook University
nick@cs.stonybrook.edu

IEEE S&P 2017

Hindsight: Understanding the Evolution of UI Vulnerabilities in Mobile Browsers

Meng Luo, Oleksii Starov, Nima Honarmand, Nick Nikiforakis
Stony Brook University
{meluo, ostarov, nhonarmand, nick}@cs.stonybrook.edu

CCS 2017

Browser extensions are popular!



> 10M users



grammarly

> 10M users



> 5.7M users



> 2.6M users



> 4.3M users



> 2.8M users



> 10M users



> 1.4M users



> 10M users



> 1.3M users



> 1.6M users



> 0.6M users

+ Extensions are “more private” ...

- Previous research showed that **plugins** were one of the most powerful features for browser fingerprinting:
 - <https://panopticklick.eff.org>
 - <https://amiunique.org>
- Plugins are fading away...
- **In comparison to plugins, there is no API for a web page to enumerate available browser extensions!**

Are extensions really undetectable?

No browser
extensions



The image shows a YouTube video player interface. At the top, there is a search bar with the text "Search" and a magnifying glass icon. Below the search bar is the YouTube logo. The video player itself shows a man with glasses working at a computer in a dimly lit room. The video progress bar indicates 0:28 / 2:45. Below the video player, the title "Hackers Official Trailer #1 - Matthew Lillard Movie (1995) HD" is displayed. The channel name "Movieclips Trailer Vault" is shown with a checkmark, and a "Subscribe" button with "214K" subscribers is visible. The view count "169,194 views" is shown on the right. At the bottom, there are icons for "Add to", "Share", and "More", along with like and comment counts of 292 and 13 respectively.

YouTube

Search

0:28 / 2:45

Hackers Official Trailer #1 - Matthew Lillard Movie (1995) HD

Movieclips Trailer Vault ✓

Subscribe 214K

169,194 views

+ Add to Share ... More

292 13

“Magic Actions for YouTube” extension



The screenshot shows a YouTube video player interface. At the top, there is a search bar with the text "Search" and a magnifying glass icon. Below the search bar is the YouTube logo. The video player itself shows a man with glasses and a dark shirt sitting at a desk, looking at a computer monitor. The video progress bar indicates 0:28 / 2:45. Below the video player, there is a row of icons for various actions: play, volume, settings, full screen, and share. The video title is "Hackers Official Trailer #1 - Matthew Lillard Movie (1995) HD". Below the title, there is a channel name "Movieclips Trailer Vault" with a verified badge and a "Subscribe" button showing 214K subscribers. The view count is 169,194 views.

YouTube

Search

0:28 / 2:45

Hackers Official Trailer #1 - Matthew Lillard Movie (1995) HD

Movieclips Trailer Vault ✓

Subscribe 214K

169,194 views

Extensions have visible side-effects!



> 10M users



grammarly

> 10M users

LastPass



> 5.7M users



> 2.6M users



> 4.3M users



> 2.8M users



> 10M users



> 1.4M users



> 10M users



> 1.3M users



> 1.6M users

HubSpot
SALES

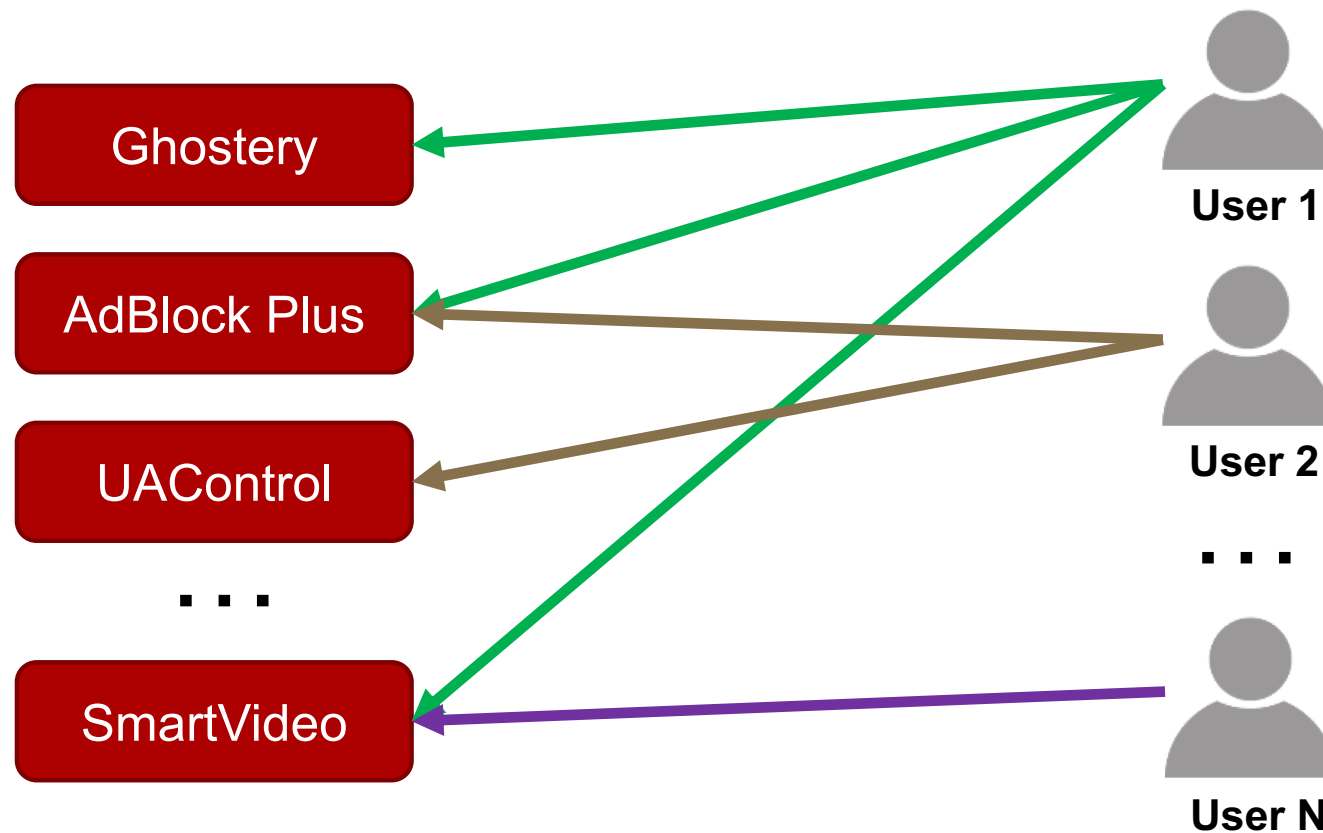
> 0.6M users

Privacy and Security implications

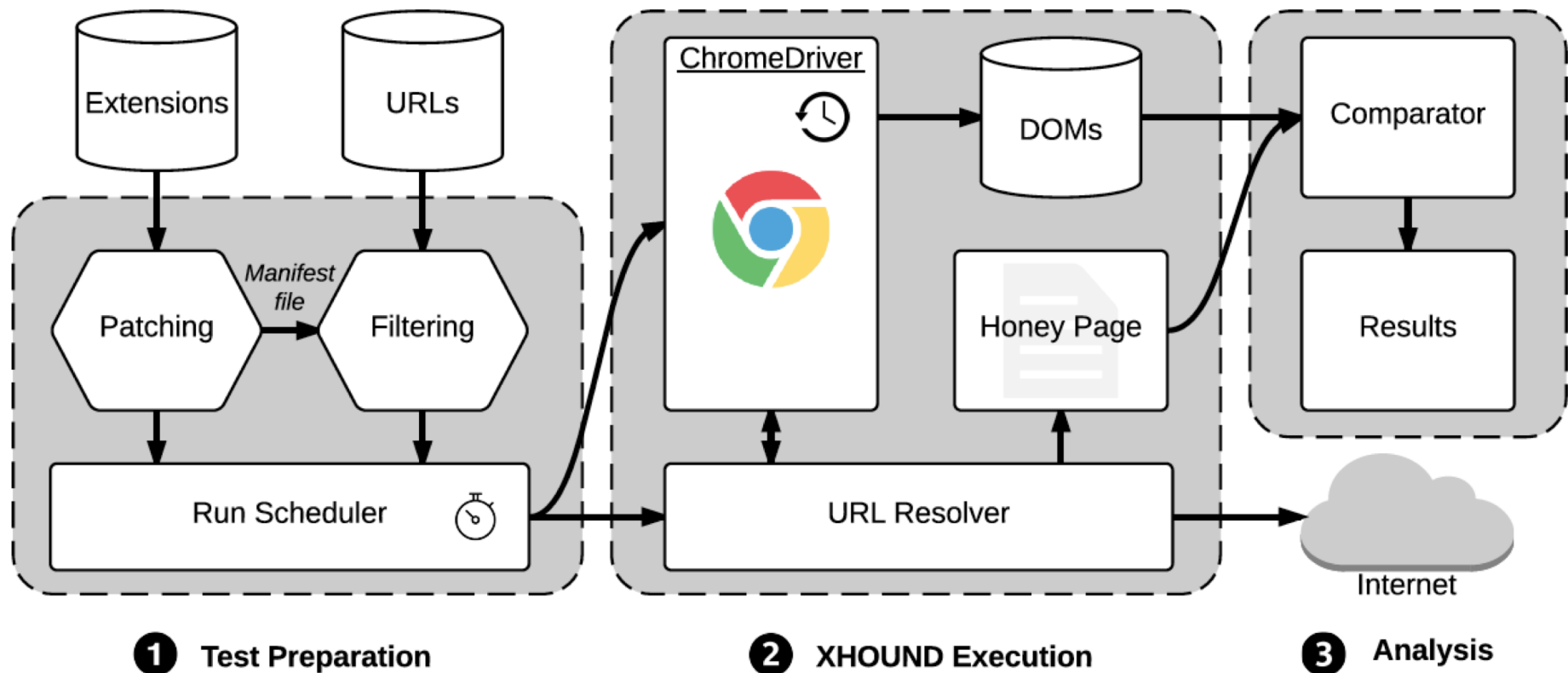
- Discovering targets for known exploits in browser extensions
 - E.g. popular password managers (*LastPass*, *Blur*, etc.)
- Exposing sensitive extensions installed by browser users
 - E.g., *Mailvelope*, VPN extensions, discount alerts, political add-ons, etc.



Extensions as a fingerprinting feature?!



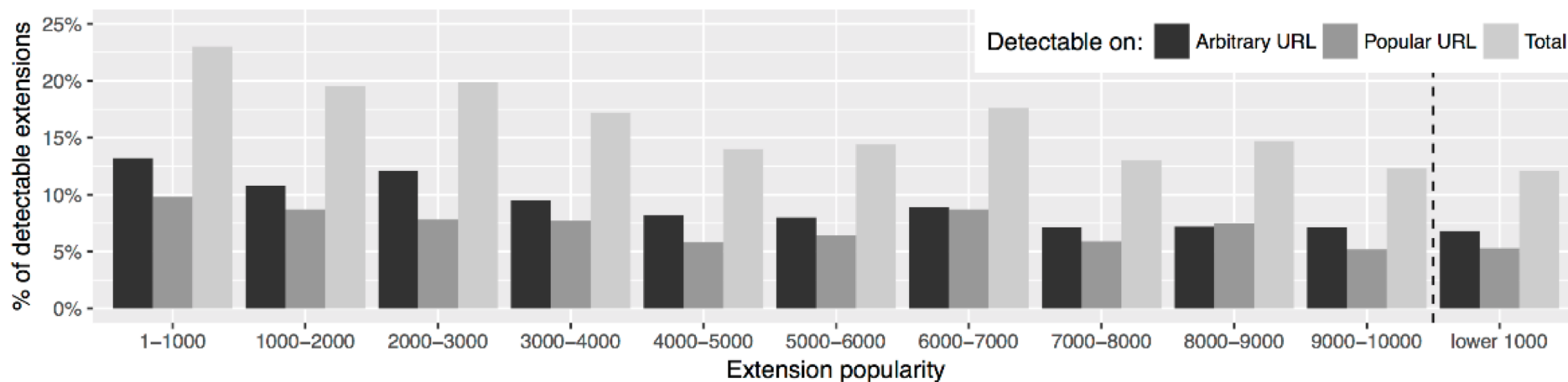
XHOUND's architecture





Results for top 10K Chrome extensions

- **9.2%** introduce detectable changes on any arbitrary URL
(*any webpage can fingerprint*)
- **16.6%** introduce detectable changes on popular domains
(*popular websites can fingerprint*)



Detectable extensions per category

Category	# Extensions	On Some URLs	On Any URL
Productivity	3,438	14.95%	10.01%
Social & Commun.	1,397	27.06%	9.81%
Fun	1,300	12.92%	6.31%
Accessibility	952	17.02%	11.87%
Developer Tools	936	9.29%	8.23%
Search Tools	595	13.28%	5.71%
Shopping	444	34.68%	17.57%
News & Weather	336	4.76%	3.87%
Photos	208	19.71%	11.54%
Blogging	144	14.58%	5.56%
Unknown	129	23.26%	4.65%
Sports	121	4.96%	4.13%

XHOUND: Quantifying the Fingerprintability of Browser Extensions

Oleksii Starov
Stony Brook University
ostarov@cs.stonybrook.edu

Nick Nikiforakis
Stony Brook University
nick@cs.stonybrook.edu

IEEE S&P 2017

Hindsight: Understanding the Evolution of UI Vulnerabilities in Mobile Browsers

Meng Luo, Oleksii Starov, Nima Honarmand, Nick Nikiforakis
Stony Brook University
{meluo, ostarov, nhonarmand, nick}@cs.stonybrook.edu

CCS 2017

Smartphones are overtaking traditional computing platforms

- More and more users rely on mobile devices for part of their daily computing needs
- ComScore report from 2017 shows that, for some countries, users spend the majority of their “total digital minutes” on a mobile device:
 - 91% Indonesia
 - 71% China
 - 71% USA
 - 62% Canada
 - 61% UK

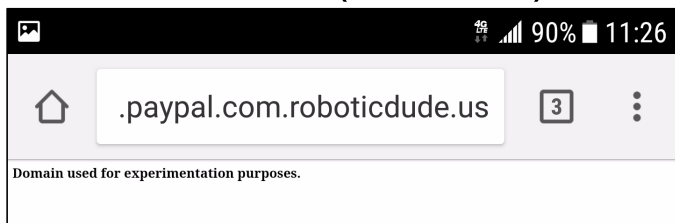
What is the security stance of mobile web browsers?

- Most research about security on mobile devices has revolved around
 - Malicious apps
 - Isolation of content and permissions from the different stakeholders present in a single app
- As mobile usage increases, it is almost guaranteed that attacks targeting specifically mobile browsers will increase
- Idiosyncrasies of the mobile platform allow novel attacks against mobile web browsers (in addition to all the standard ones)
 - Limited screen real-estate
 - The desire of mobile browser vendors to maximize the real-estate allotted to websites
 - Limited computing power and battery life

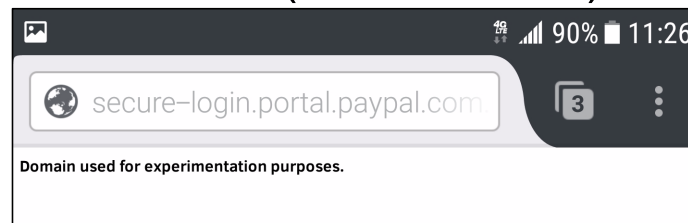
Limited real-estate example

- What happens when users clicks on a URL that is “longer” than the physical width of their device:
 - secure-login.portal.paypal.com.roboticdude.us

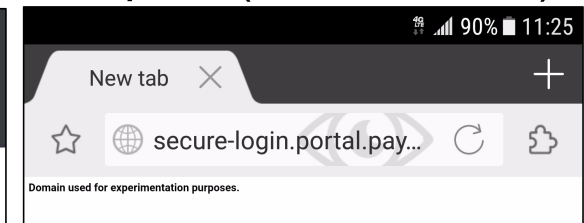
Chrome (1B – 5B)



Firefox (100M- 500M)



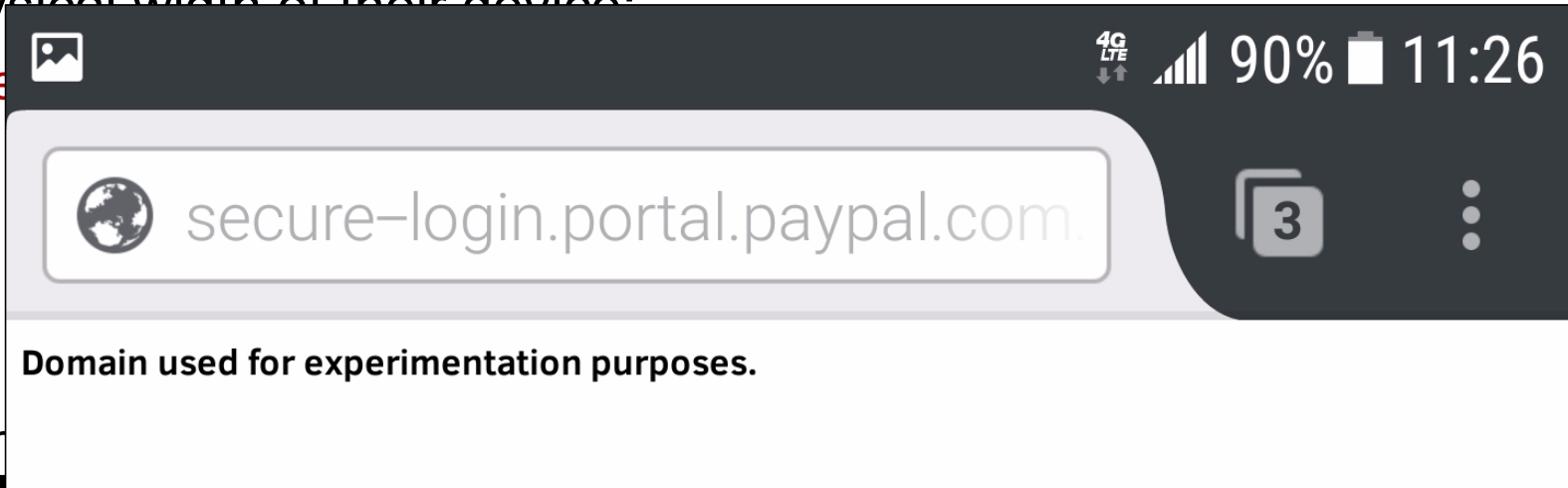
Dolphin (50M – 100M)



Limited real-estate example

- What happens when users clicks on a URL that is “longer” than the physical width of their device:

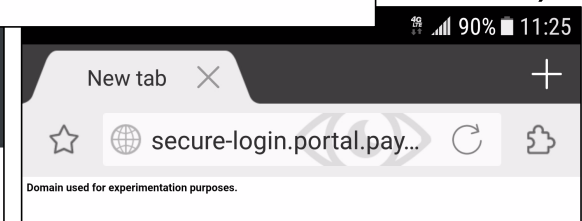
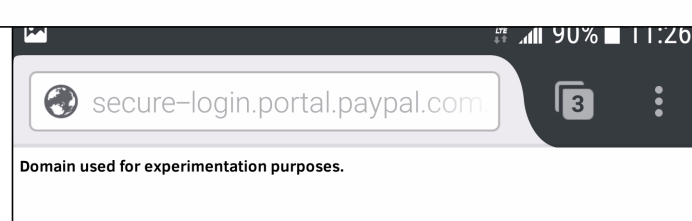
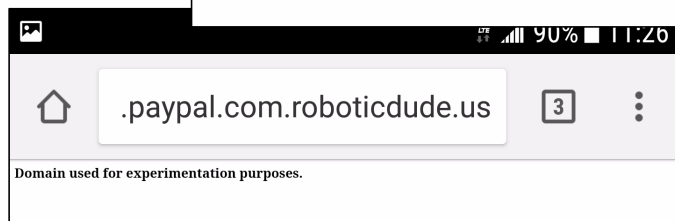
- se



Domain used for experimentation purposes.

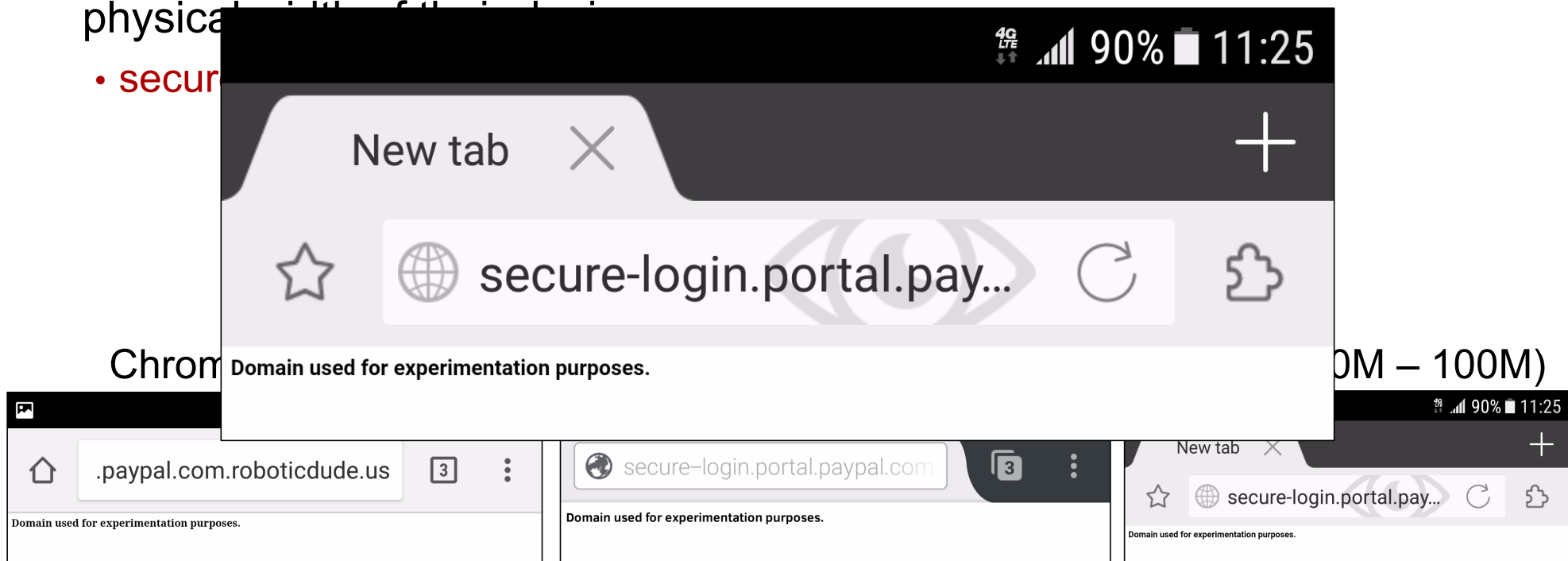
Ch

- 100M)



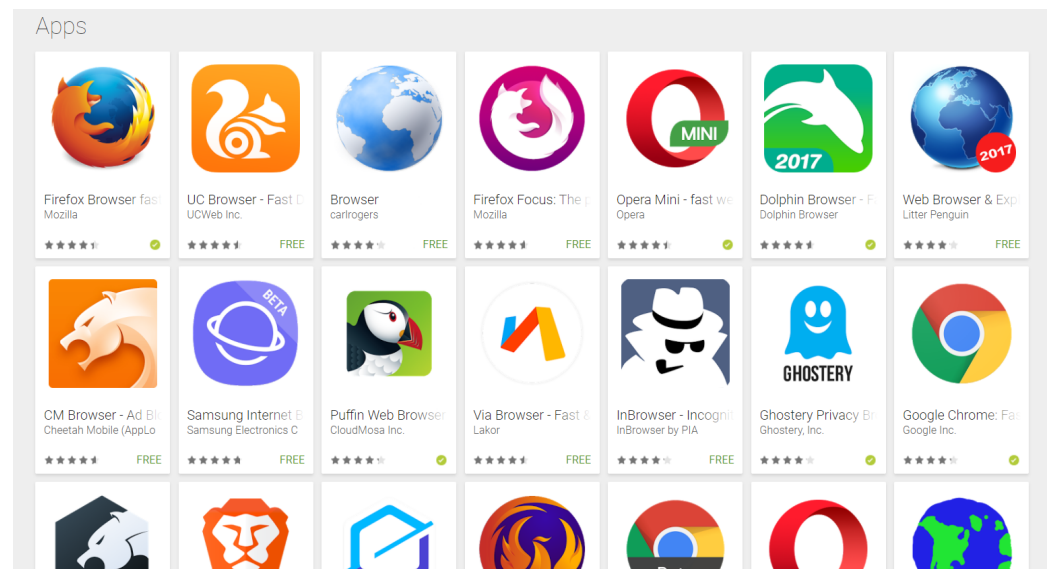
Limited real-estate example

- What happens when users clicks on a URL that is “longer” than the physical width of the browser?
- secure



Manual analysis does not scale

- Number of browsers in the market
 - More than a hundred browser families
- Speed of new releases and updates
 - Tens of updates every year
- Number of attacks
- Most secure browser?
- Least secure browser?
- Which browser has stopped fixing bugs?



Automation is your friend

- Design and develop the first browser-agnostic, vulnerability testing framework for mobile browsers (Hindsight)
- High-level idea:
 - Collect as many mobile-browser-specific attacks as possible
 - Experiment with them to arrive at novel variations
 - Collect as many mobile browser versions from as many browser families as possible
 - Install each browser on a test device
 - Expose it to your collect attacks
 - Analyze collected data

Attack Building Blocks

Class	Test#	Explanation	Prior Work	Potential Attacks
Event Routing	1-6	Do cross-origin, overlapping elements receive events when they are not the topmost ones? (Different tests for combinations of overlapped images and buttons, links, forms, and other images)	[3, 6]	Clickjacking, CSRF
URL	7-9	When presented with a long URL (long subdomain, long filepath, or a combination of both), does a browser render that URL in a way that could be abused for spoofing attacks?	[30, 38]	Phishing, malware/scam delivery
	10	When presented with an Internationalized Domain Name (IDN), will a browser display the IDN format?	[16]	Phishing, malware/scam delivery
Address Bar	11	Is the address bar hidden if the top-level frame is navigated by a child frame?	[3, 6]	Phishing, malware/scam delivery
	12	Does a browser show a page's title instead of its URL?	[8]	Phishing, malware/scam delivery
	13	Is the address bar hidden if the visited website has a lot of content?	Novel	Phishing, malware/scam delivery
	14	Is the address bar hidden when switching the device to "landscape" mode?	Novel	Phishing, malware/scam delivery
	15-16	Is the address bar hidden upon manual/automatic page scrolling?	[30, 32]	Phishing, malware/scam delivery
	17-18	Is the address bar hidden when typing in a textbox and tapping on a button?	[15, 38]	Phishing, malware/scam delivery
Security Indicators	19	Is the address bar hidden when typing to a fake (e.g., canvas-created) textbox?	Novel	Phishing, malware/scam delivery
	20	Is the favicon placed next to padlock icon?	[4, 5, 14, 37]	MITM attack, Phishing
	21-22	When rendering an HTTPS page, is the address bar displayed the same in the presence of mixed content (image and JavaScript) as in its absence?	[9]	MITM attack
Content	23	Is a webpage with self-signed certificate rendered without warnings?	[4, 5, 14, 37]	MITM attack, Phishing
	24	Can an iframe expand its size past the one defined by its parent frame?	[3, 6]	Phishing
	25	Is a mixed-content image resource loaded?	[9]	MITM attack
	26	Is a mixed-content JavaScript script executed?	[9]	MITM attack
	27	Is JavaScript code included in a self-signed website executed before the warning is accepted?	Novel	Phishing, MITM attack

Attack Building Blocks

Class	Test#	Explanation	Prior Work	Potential Attacks
Event Routing	1-6	Do cross-origin, overlapping elements receive events when they are not the topmost ones? (Different tests for combinations of overlapped images and buttons, links, forms, and other images)	[3, 6]	Clickjacking, CSRF
URL	7-9	When presented with a long URL (long subdomain, long filepath, or a combination of both), does a browser render that URL in a way that could be abused for spoofing attacks?	[30, 38]	Phishing, malware/scam delivery
	10	When presented with an Internationalized Domain Name (IDN), will a browser display the IDN format?	[16]	Phishing, malware/scam delivery
Address Bar	11	Is the address bar hidden if the top-level frame is navigated by a child frame?	[3, 6]	Phishing, malware/scam delivery
	12	Does a browser show a page's title instead of its URL?	[8]	Phishing, malware/scam delivery
	13	Is the address bar hidden if the visited website has a lot of content?	Novel	Phishing, malware/scam delivery
	14	Is the address bar hidden when switching the device to "landscape" mode?	Novel	Phishing, malware/scam delivery
	15-16	Is the address bar hidden upon manual/automatic page scrolling?	[30, 32]	Phishing, malware/scam delivery
	17-18	Is the address bar hidden when typing in a textbox and tapping on a button?	[15, 38]	Phishing, malware/scam delivery
Security Indicators	19	Is the address bar hidden when typing to a fake (e.g., canvas-created) textbox?	Novel	Phishing, malware/scam delivery
	20	Is the favicon placed next to padlock icon?	[4, 5, 14, 37]	MITM attack, Phishing
	21-22	When rendering an HTTPS page, is the address bar displayed the same in the presence of mixed content (image and JavaScript) as in its absence?	[9]	MITM attack
Content	23	Is a webpage with self-signed certificate rendered without warnings?	[4, 5, 14, 37]	MITM attack, Phishing
	24	Can an iframe expand its size past the one defined by its parent frame?	[3, 6]	Phishing
	25	Is a mixed-content image resource loaded?	[9]	MITM attack
	26	Is a mixed-content JavaScript script executed?	[9]	MITM attack
	27	Is JavaScript code included in a self-signed website executed before the warning is accepted?	Novel	Phishing, MITM attack

Attack Building Blocks

Class	Test#	Explanation	Prior Work	Potential Attacks
Event Routing	1-6	Do cross-origin, overlapping elements receive events when they are not the topmost ones? (Different tests for combinations of overlapped images and buttons, links, forms, and other images)	[3, 6]	Clickjacking, CSRF
URL	7-9	When presented with a long URL (long subdomain, long filepath, or a combination of both), does a browser render that URL in a way that could be abused for spoofing attacks?	[30, 38]	Phishing, malware/scam delivery
	10	When presented with an Internationalized Domain Name (IDN), will a browser display the IDN format?	[16]	Phishing, malware/scam delivery
Address Bar	11	Is the address bar hidden if the top-level frame is navigated by a child frame?	[3, 6]	Phishing, malware/scam delivery
	12	Does a browser show a page's title instead of its URL?	[8]	Phishing, malware/scam delivery
	13	Is the address bar hidden if the visited website has a lot of content?	Novel	Phishing, malware/scam delivery
	14	Is the address bar hidden when switching the device to "landscape" mode?	Novel	Phishing, malware/scam delivery
	15-16	Is the address bar hidden upon manual/automatic page scrolling?	[30, 32]	Phishing, malware/scam delivery
	17-18	Is the address bar hidden when typing in a textbox and tapping on a button?	[15, 38]	Phishing, malware/scam delivery
Security Indicators	19	Is the address bar hidden when typing to a fake (e.g., canvas-created) textbox?	Novel	Phishing, malware/scam delivery
	20	Is the favicon placed next to padlock icon?	[4, 5, 14, 37]	MITM attack, Phishing
	21-22	When rendering an HTTPS page, is the address bar displayed the same in the presence of mixed content (image and JavaScript) as in its absence?	[9]	MITM attack
Content	23	Is a webpage with self-signed certificate rendered without warnings?	[4, 5, 14, 37]	MITM attack, Phishing
	24	Can an iframe expand its size past the one defined by its parent frame?	[3, 6]	Phishing
	25	Is a mixed-content image resource loaded?	[9]	MITM attack
	26	Is a mixed-content JavaScript script executed?	[9]	MITM attack
	27	Is JavaScript code included in a self-signed website executed before the warning is accepted?	Novel	Phishing, MITM attack

Attack Building Blocks

Class	Test#	Explanation	Prior Work	Potential Attacks
Event Routing	1-6	Do cross-origin, overlapping elements receive events when they are not the topmost ones? (Different tests for combinations of overlapped images and buttons, links, forms, and other images)	[3, 6]	Clickjacking, CSRF
URL	7-9	When presented with a long URL (long subdomain, long filepath, or a combination of both), does a browser render that URL in a way that could be abused for spoofing attacks?	[30, 38]	Phishing, malware/scam delivery
	10	When presented with an Internationalized Domain Name (IDN), will a browser display the IDN format?	[16]	Phishing, malware/scam delivery
Address Bar	11	Is the address bar hidden if the top-level frame is navigated by a child frame?	[3, 6]	Phishing, malware/scam delivery
	12	Does a browser show a page's title instead of its URL?	[8]	Phishing, malware/scam delivery
	13	Is the address bar hidden if the visited website has a lot of content?	Novel	Phishing, malware/scam delivery
	14	Is the address bar hidden when switching the device to "landscape" mode?	Novel	Phishing, malware/scam delivery
	15-16	Is the address bar hidden upon manual/automatic page scrolling?	[30, 32]	Phishing, malware/scam delivery
	17-18	Is the address bar hidden when typing in a textbox and tapping on a button?	[15, 38]	Phishing, malware/scam delivery
Security Indicators	19	Is the address bar hidden when typing to a fake (e.g., canvas-created) textbox?	Novel	Phishing, malware/scam delivery
	20	Is the favicon placed next to padlock icon?	[4, 5, 14, 37]	MITM attack, Phishing
	21-22	When rendering an HTTPS page, is the address bar displayed the same in the presence of mixed content (image and JavaScript) as in its absence?	[9]	MITM attack
Content	23	Is a webpage with self-signed certificate rendered without warnings?	[4, 5, 14, 37]	MITM attack, Phishing
	24	Can an iframe expand its size past the one defined by its parent frame?	[3, 6]	Phishing
	25	Is a mixed-content image resource loaded?	[9]	MITM attack
	26	Is a mixed-content JavaScript script executed?	[9]	MITM attack
	27	Is JavaScript code included in a self-signed website executed before the warning is accepted?	Novel	Phishing, MITM attack

Attack Building Blocks

Class	Test#	Explanation	Prior Work	Potential Attacks
Event Routing	1-6	Do cross-origin, overlapping elements receive events when they are not the topmost ones? (Different tests for combinations of overlapped images and buttons, links, forms, and other images)	[3, 6]	Clickjacking, CSRF
URL	7-9	When presented with a long URL (long subdomain, long filepath, or a combination of both), does a browser render that URL in a way that could be abused for spoofing attacks?	[30, 38]	Phishing, malware/scam delivery
	10	When presented with an Internationalized Domain Name (IDN), will a browser display the IDN format?	[16]	Phishing, malware/scam delivery
Address Bar	11	Is the address bar hidden if the top-level frame is navigated by a child frame?	[3, 6]	Phishing, malware/scam delivery
	12	Does a browser show a page's title instead of its URL?	[8]	Phishing, malware/scam delivery
	13	Is the address bar hidden if the visited website has a lot of content?	Novel	Phishing, malware/scam delivery
	14	Is the address bar hidden when switching the device to "landscape" mode?	Novel	Phishing, malware/scam delivery
	15-16	Is the address bar hidden upon manual/automatic page scrolling?	[30, 32]	Phishing, malware/scam delivery
	17-18	Is the address bar hidden when typing in a textbox and tapping on a button?	[15, 38]	Phishing, malware/scam delivery
	19	Is the address bar hidden when typing to a fake (e.g., canvas-created) textbox?	Novel	Phishing, malware/scam delivery
Security Indicators	20	Is the favicon placed next to padlock icon?	[4, 5, 14, 37]	MITM attack, Phishing
	21-22	When rendering an HTTPS page, is the address bar displayed the same in the presence of mixed content (image and JavaScript) as in its absence?	[9]	MITM attack
	23	Is a webpage with self-signed certificate rendered without warnings?	[4, 5, 14, 37]	MITM attack, Phishing
Content	24	Can an iframe expand its size past the one defined by its parent frame?	[3, 6]	Phishing
	25	Is a mixed-content image resource loaded?	[9]	MITM attack
	26	Is a mixed-content JavaScript script executed?	[9]	MITM attack
	27	Is JavaScript code included in a self-signed website executed before the warning is accepted?	Novel	Phishing, MITM attack

Attack Building Blocks

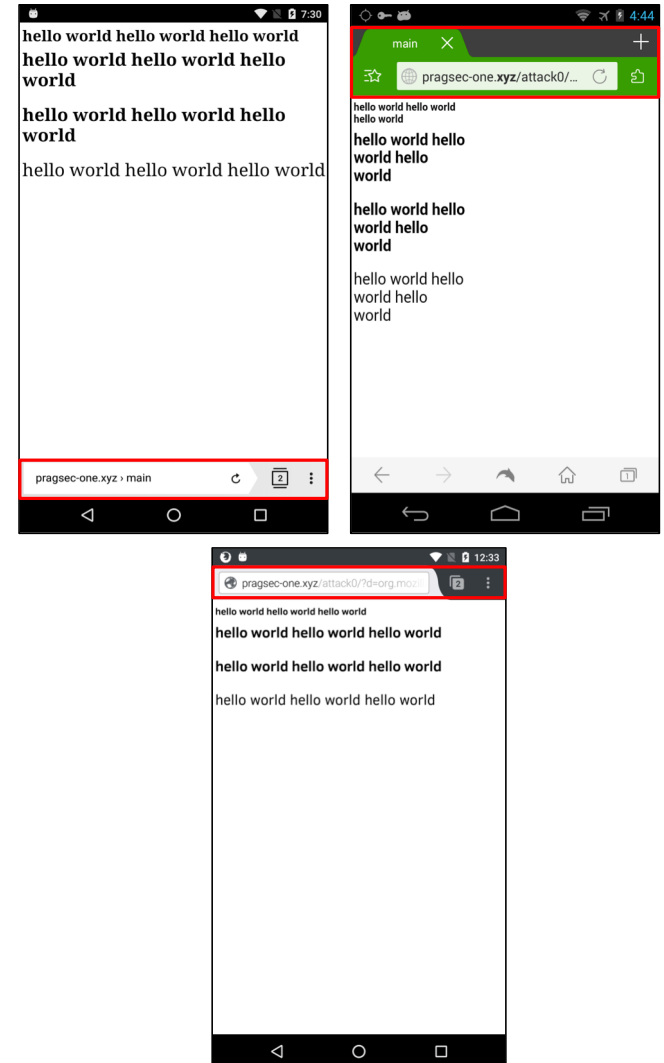
Class	Test#	Explanation	Prior Work	Potential Attacks
Event Routing	1-6	Do cross-origin, overlapping elements receive events when they are not the topmost ones? (Different tests for combinations of overlapped images and buttons, links, forms, and other images)	[3, 6]	Clickjacking, CSRF
URL	7-9	When presented with a long URL (long subdomain, long filepath, or a combination of both), does a browser render that URL in a way that could be abused for spoofing attacks?	[30, 38]	Phishing, malware/scam delivery
	10	When presented with an Internationalized Domain Name (IDN), will a browser display the IDN format?	[16]	Phishing, malware/scam delivery
Address Bar	11	Is the address bar hidden if the top-level frame is navigated by a child frame?	[3, 6]	Phishing, malware/scam delivery
	12	Does a browser show a page's title instead of its URL?	[8]	Phishing, malware/scam delivery
	13	Is the address bar hidden if the visited website has a lot of content?	Novel	Phishing, malware/scam delivery
	14	Is the address bar hidden when switching the device to "landscape" mode?	Novel	Phishing, malware/scam delivery
	15-16	Is the address bar hidden upon manual/automatic page scrolling?	[30, 32]	Phishing, malware/scam delivery
	17-18	Is the address bar hidden when typing in a textbox and tapping on a button?	[15, 38]	Phishing, malware/scam delivery
Security Indicators	19	Is the address bar hidden when typing to a fake (e.g., canvas-created) textbox?	Novel	Phishing, malware/scam delivery
	20	Is the favicon placed next to padlock icon?	[4, 5, 14, 37]	MITM attack, Phishing
	21-22	When rendering an HTTPS page, is the address bar displayed the same in the presence of mixed content (image and JavaScript) as in its absence?	[9]	MITM attack
Content	23	Is a webpage with self-signed certificate rendered without warnings?	[4, 5, 14, 37]	MITM attack, Phishing
	24	Can an iframe expand its size past the one defined by its parent frame?	[3, 6]	Phishing
	25	Is a mixed-content image resource loaded?	[9]	MITM attack
	26	Is a mixed-content JavaScript script executed?	[9]	MITM attack
	27	Is JavaScript code included in a self-signed website executed before the warning is accepted?	Novel	Phishing, MITM attack

Combination of multiple ABBs in a single attack

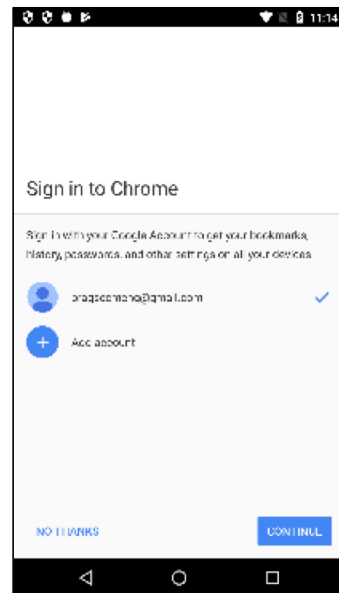
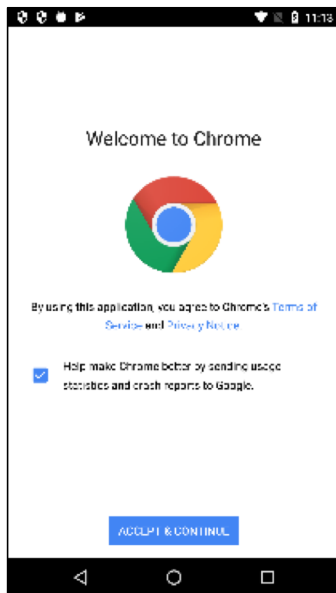


Browser-Agnostic UI Analysis

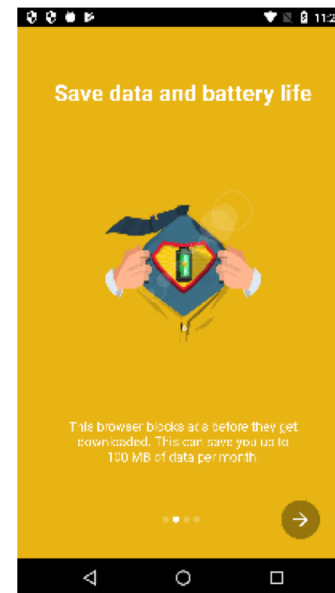
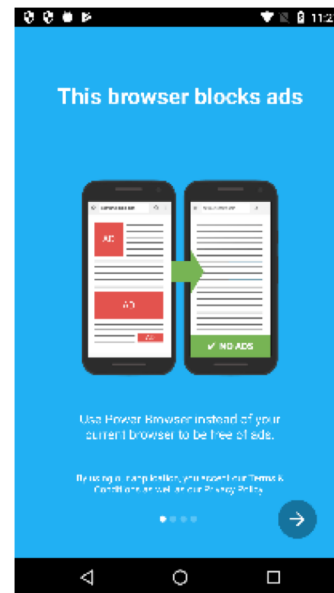
- Application-level UI
 - i.e., address bar, favicon, padlock
- Web page content
 - E.g., user interactions to HTML elements
 - Lacks in pixel-level mapping for web page and device
- Techniques: UIAutomator, OCR and image comparison algorithms



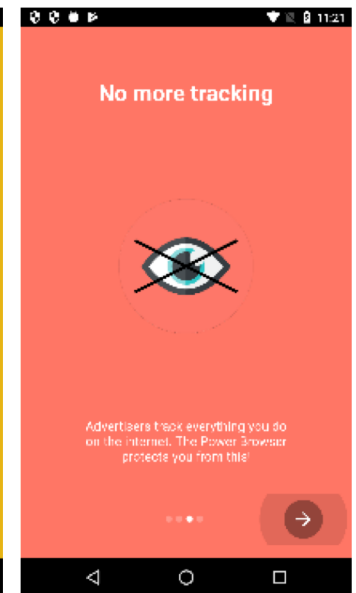
Splash screens of mobile browsers



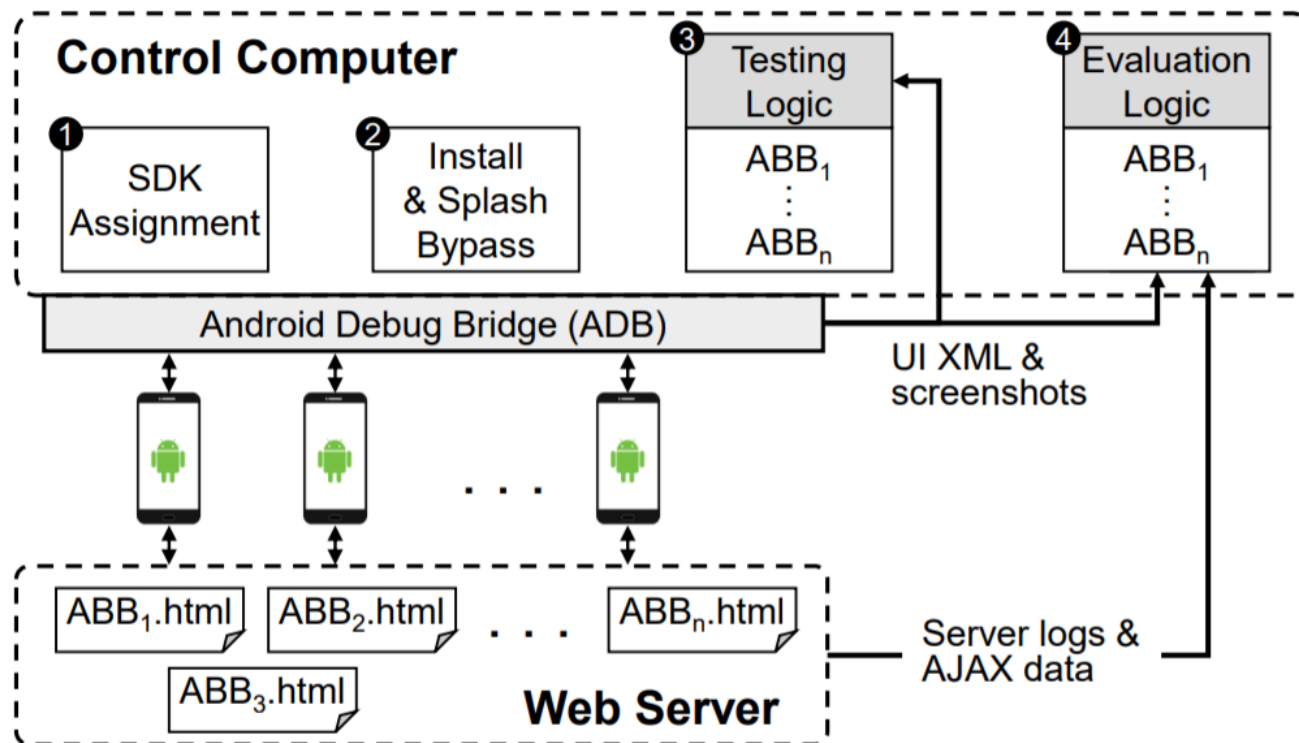
Google Chrome



Power Browser



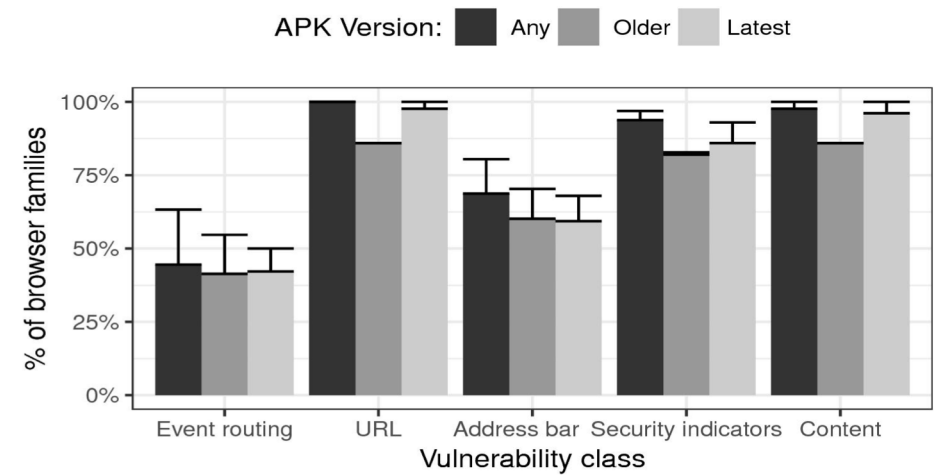
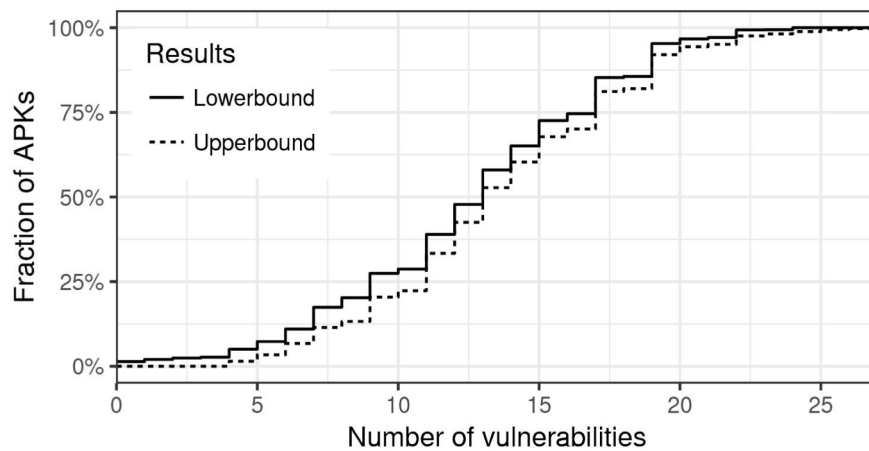
Architecture of Hindsight framework



Hindsight in action

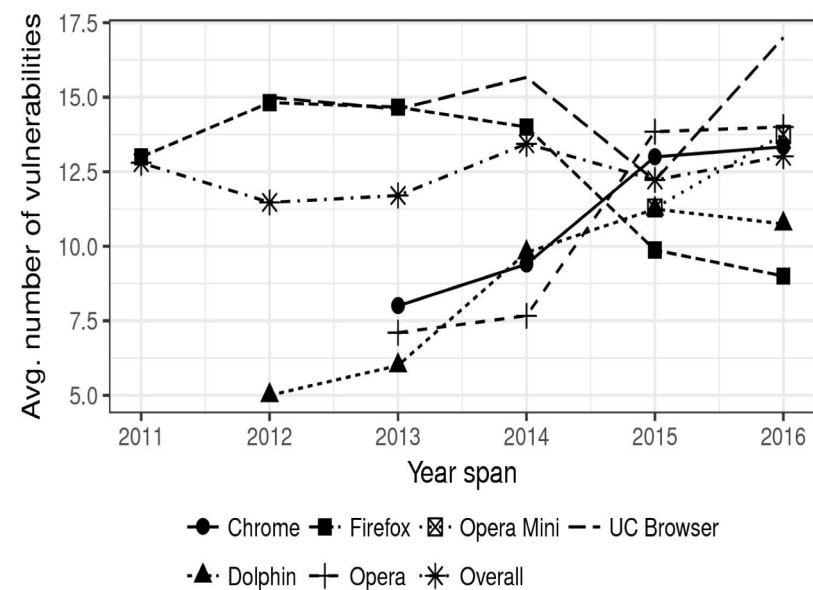
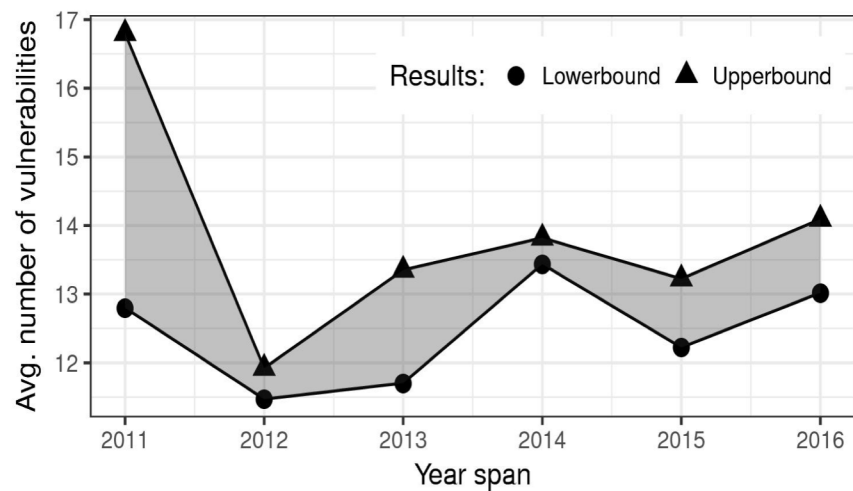


Hindsight: Results from 2,324 browser APKs



- 98.6% of the evaluated browser APKs are vulnerable to at least one ABB.
- 50% of APKs are vulnerable to more than 12 ABBs.
- URL ABBs more potent than the rest

Hindsight: Longitudinal analysis of vulnerabilities



Other things we do...

- Identify ways that malware can bypass modern sandboxes
 - Joint work with Professor Michalis Polychronakis
- Construct more realistic honeypots
 - Get attacks to spend more time on them
 - Understand how they are evaded
- Study abuse of the Domain Name System
 - Domain squatting
 - Domain name hijacking
 - Malicious domain registrations
- Track cybercrime campaigns
 - Technical support scams
 - Affiliate abuse



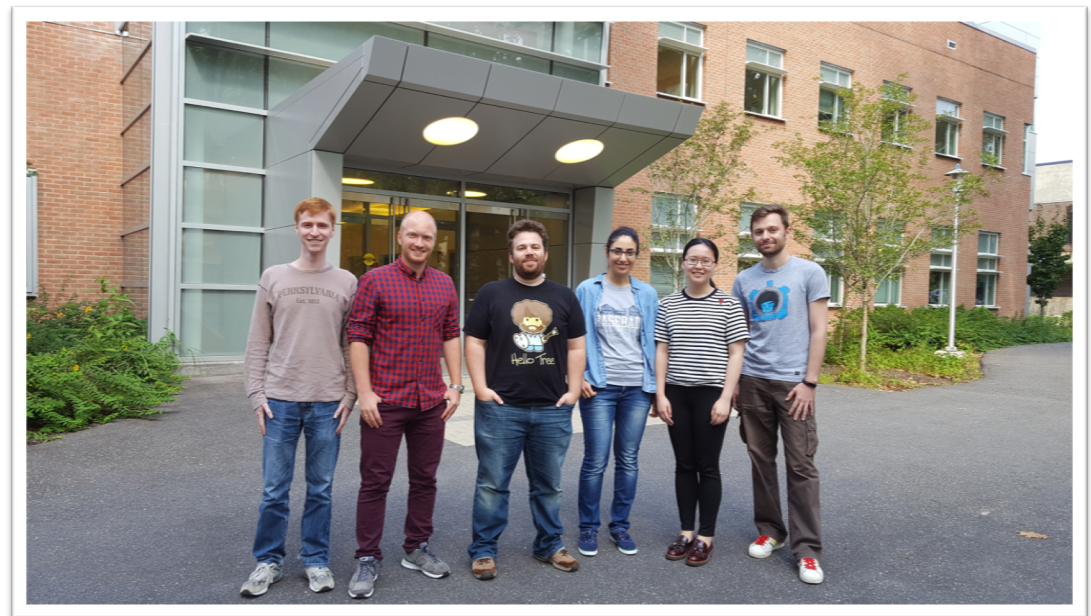
Conclusion

- As the functionality of browsers expand, so does their attack surface
- Whenever a new feature is added, we must try to reason about the interaction of that feature with existing security policies and mechanisms
 - Automation is key



Stony Brook University

PragSec
Lab



nick@cs.stonybrook.edu
www.securitee.org

