CSE 484 / CSE M 584: Computer Security and Privacy

Mobile Platform Security [finish]

Fall 2017

Franziska (Franzi) Roesner franzi@cs.washington.edu

Thanks to Dan Boneh, Dieter Gollmann, Dan Halperin, Yoshi Kohno, Ada Lerner, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...

Admin

- Project checkpoint #2 due tonight
- Keep letting us know of any fuzzing issues with HW3
 - Double check that you followed the instructions
 - Make sure to put things in C: instead of D:
 - It's possible to run into issues on the MS side, so let us know and we'll loop them in if needed (in the meantime you can relax ③)

This Week: Mac OS X High Sierra Issue

- Given physical access, if root password not set, can login (creating a root account?) without a password
- Manual fix: set root password

Security Update 2017-001
Released November 29, 2017
Directory Utility
Available for: macOS High Sierra 10.13 and macOS High Sierra 10.13.1
Not impacted: macOS Sierra 10.12.6 and earlier
Impact: An attacker may be able to bypass administrator authentication without supplying the administrator's password
Description: A logic error existed in the validation of credentials. This was addressed with improved credential validation.
CVE-2017-13872
Entry updated November 29, 2017

Back to Mobile Security: Challenges with Isolated Apps

So mobile platforms isolate applications for security, but...

- 1. Permissions: How can applications access sensitive resources?
- 2. Communication: How can applications communicate with each other?

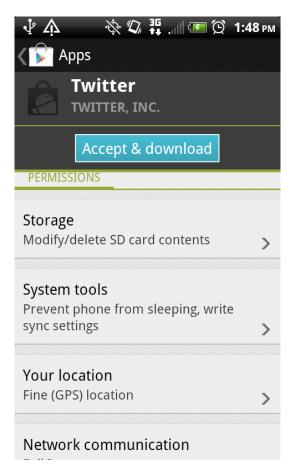
State of the Art

Prompts (time-of-use)

	"WhereIsMyCa to Use Your Cu		
	Don't Allow	OK	
acific	South America		

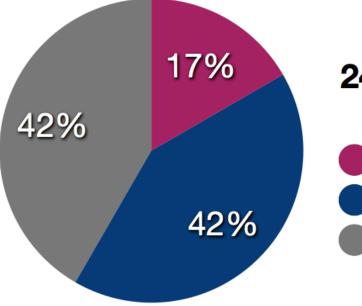


Manifests (install-time)



Are Manifests Usable?

Do users pay attention to permissions?



24 observed installations

Looked at permissions Didn't look, but aware Unaware of permissions

... but 88% of users looked at reviews.

Are Manifests Usable?

Do users understand the warnings?

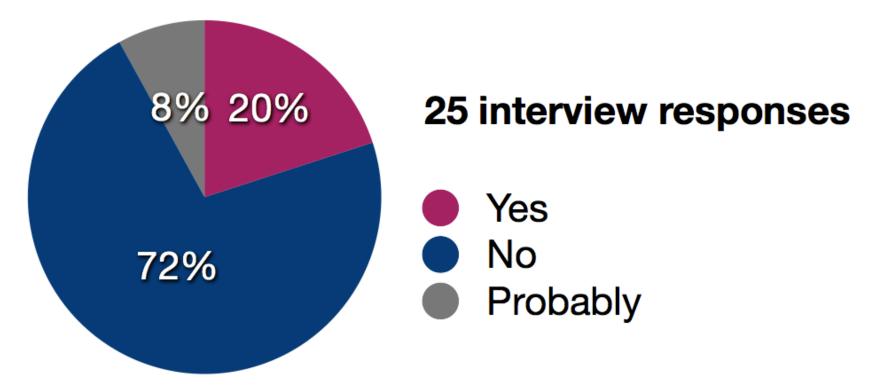
	Permission	$\mid n$	Correct Answers		
1 Choice	READ_CALENDAR	101	46	45.5%	
	CHANGE_NETWORK_STATE	66	26	39.4%	
	READ_SMS1	77	24	31.2%	
	CALL_PHONE	83	16	19.3%	
2 Choices	WAKE_LOCK	81	27	33.3%	
	WRITE_EXTERNAL_STORAGE	92	14	15.2%	
	READ_CONTACTS	86	11	12.8%	
	INTERNET	109	12	11.0%	
	READ_PHONE_STATE	85	4	4.7%	
	READ_SMS2	54	12	22.2%	
4	CAMERA	72	7	9.7%	

Table 4: The number of people who correctly answered a question. Questions are grouped by the number of correct choices. n is the number of respondents. (Internet Survey, n = 302)

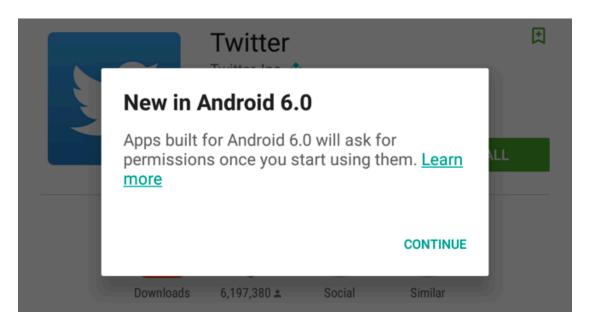
Are Manifests Usable?

Do users act on permission information?

"Have you ever not installed an app because of permissions?"



Android 6.0: Prompts!

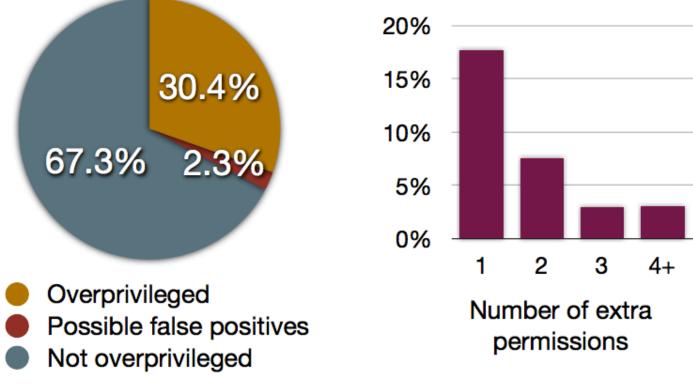


- First-use prompts for sensitive permission (like iOS).
- **Big change!** Now app developers need to check for permissions or catch exceptions.

Over-Permissioning

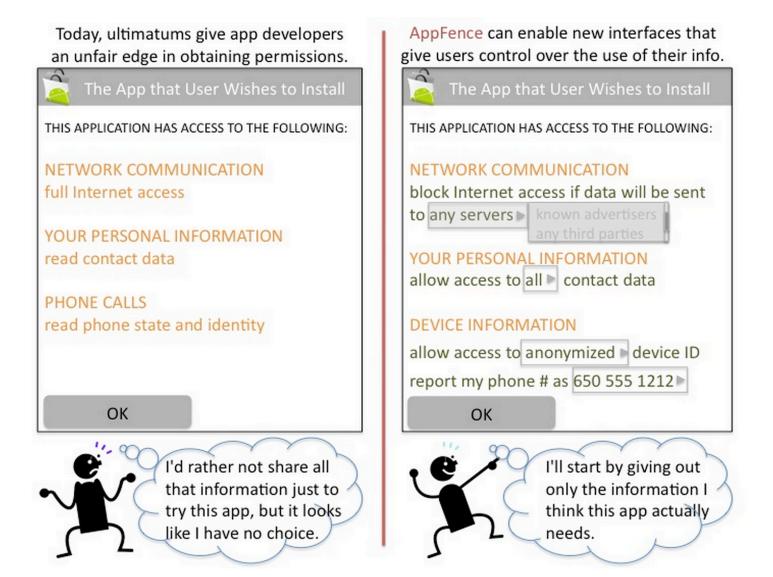
- Android permissions are badly documented.
- Researchers have mapped APIs \rightarrow permissions.

www.android-permissions.org (Felt et al.), <u>http://pscout.csl.toronto.edu</u> (Au et al.)



[Hornyack et al.]

Improving Permissions: AppFence



[our work]

Improving Permissions: User-Driven Access Control

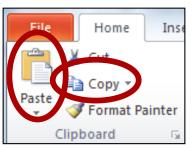


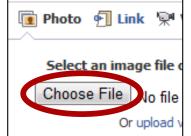
Let this application access my location now.

Insight:

A user's natural UI actions within an application implicitly carry permission-granting semantics.



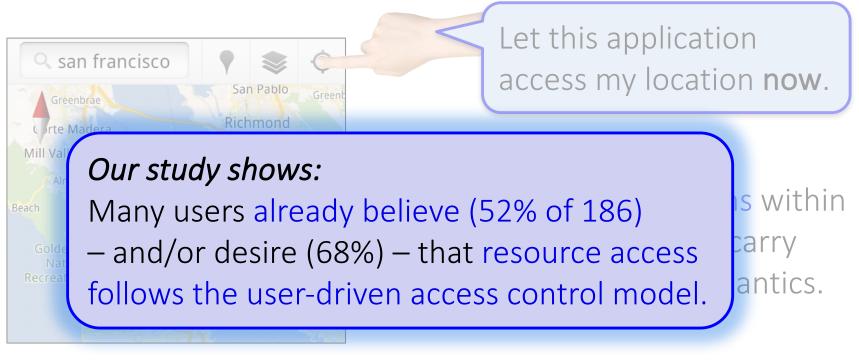




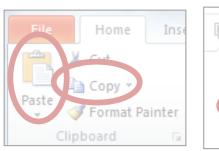


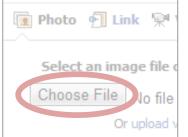
[our work]

Improving Permissions: User-Driven Access Control











New OS Primitive: Access Control Gadgets (ACGs)



Approach: Make resource-related UI elements first-class operating system objects (access control gadgets).

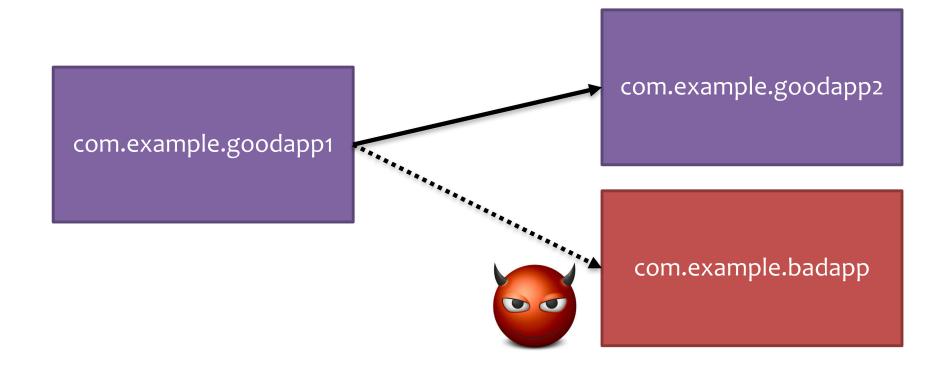
- To receive resource access, applications must embed a system-provided ACG.
- ACGs allow the OS to capture the user's permission granting intent in application-agnostic way.

(2) Inter-Process Communication

- Primary mechanism in Android: Intents
 - Sent between application components
 - e.g., with startActivity(intent)
 - Explicit: specify component name
 - e.g., com.example.testApp.MainActivity
 - Implicit: specify action (e.g., ACTION_VIEW) and/or data (URI and MIME type)
 - Apps specify Intent Filters for their components.

Unauthorized Intent Receipt

Attack #1: Eavesdropping / Broadcast Theft



Unauthorized Intent Receipt

Attack #2: Service/Activity Hijacking

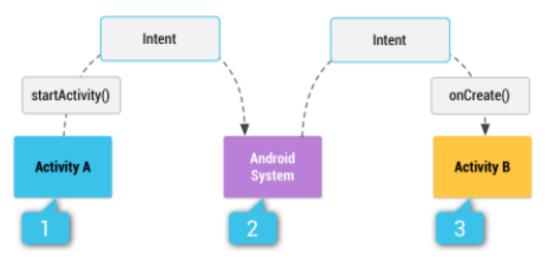
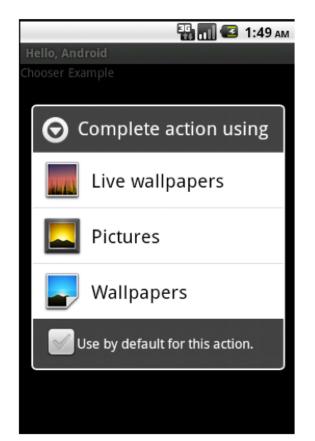


Figure 1. How an implicit intent is delivered through the system to start another activity: [1] Activity A creates an Intent with an action description and passes it to startActivity(). [2] The Android System searches all apps for an intent filter that matches the intent. When a match is found, [3] the system starts the matching activity (Activity B) by invoking its onCreate() method and passing it the Intent. "Caution: To ensure that your app is secure, always use an explicit intent when starting a Servier. Using an implicit intent to start a service is a security hazard because you can't be certain what service will respond to the intent, and the user can't see which service starts."

[Chin et al.]

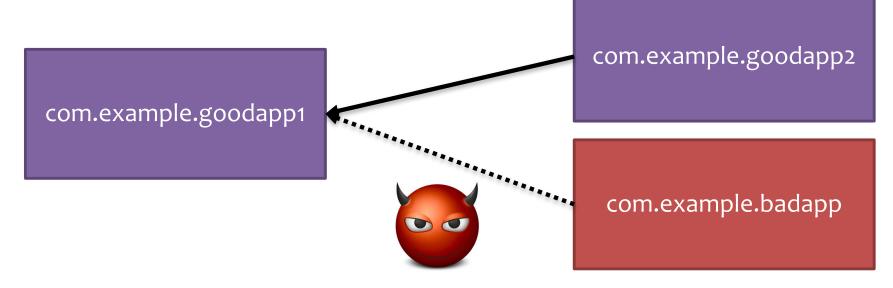
Unauthorized Intent Receipt

- Attack #1: Eavesdropping / Broadcast Thefts
 - Implicit intents make intra-app messages public.
- Attack #2: Activity Hijacking
 May not always work:
- Attack #3: Service Hijacking
 - Android picks one at random upon conflict!



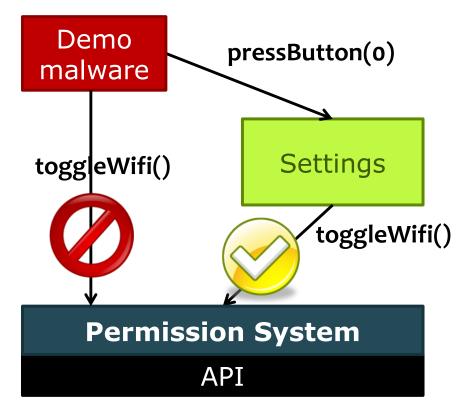
Intent Spoofing

- Attack #1: General intent spoofing
 - Receiving implicit intents makes component public.
 - Allows data injection.
- Attack #2: System intent spoofing
 - Can't directly spoof, but victim apps often don't check specific "action" in intent.



Permission Re-Delegation

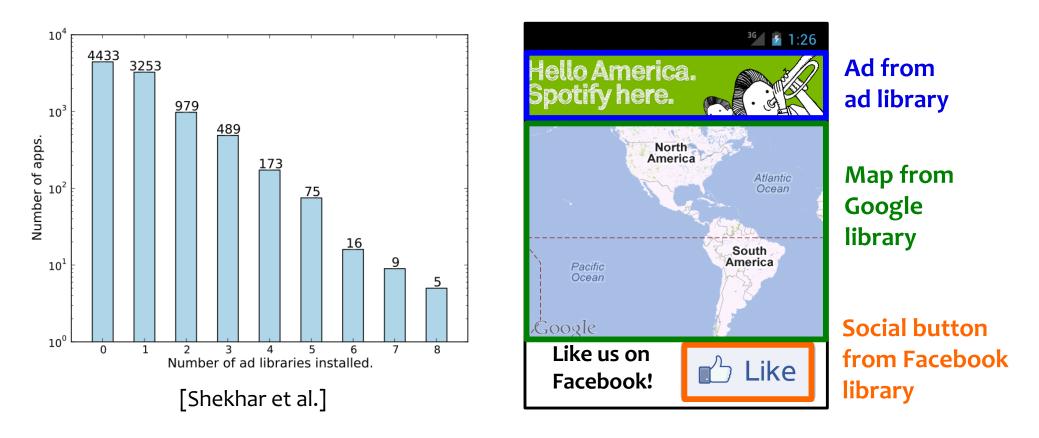
- An application without a permission gains additional privileges through another application.
- <u>Demo video</u>
- Settings application is deputy: has permissions, and accidentally exposes APIs that use those permissions.



More on Android...

Incomplete Isolation

Embedded UIs and libraries always run with the host application's permissions! (No same-origin policy here...)



Android Application Signing

- Apps are signed
 - Often with self-signed certificates
 - Signed application certificate defines which user ID is associated with which applications
 - Different apps run under different UIDs
- Shared UID feature
 - Shared Application Sandbox possible, where two or more apps signed with same developer key can declare a shared UID in their manifest

Shared UIDs

- App 1: Requests GPS / camera access
- App 2: Requests Network capabilities
- Generally:
 - First app can't exfiltrate information
 - Second app can't exfiltrate anything interesting
- With Shared UIDs (signed with same private key)
 - Permissions are a superset of permissions for each app
 - App 1 can now exfiltrate; App 2 can now access GPS / camera

File Permissions

- Files written by one application cannot be read by other applications
 - Previously, this wasn't true for files stored on the SD card (world readable!) Android cracked down on this
- It is possible to do full file system encryption
 Key = Password/PIN combined with salt, hashed

Memory Management

- Address Space Layout Randomization to randomize addresses on stack
- Hardware-based No eXecute (NX) to prevent code execution on stack/heap
- Stack guard derivative
- Some defenses against double free bugs (based on OpenBSD's dmalloc() function)
- etc.

[See http://source.android.com/tech/security/index.html]

Android Fragmentation

- Many different variants of Android (unlike iOS)
 - Motorola, HTC, Samsung, ...
- Less secure ecosystem
 - Inconsistent or incorrect implementations
 - Slow to propagate kernel updates and new versions

[https://developer.android.com/about/dashbo ards/index.html]

Version	Codename	API	Distribution
2.3.3 - 2.3.7	Gingerbread	10	1.0%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	0.8%
4.1.x	Jelly Bean	16	3.2%
4.2.x		17	4.6%
4.3		18	1.3%
4.4	KitKat	19	18.8%
5.0	Lollipop	21	8.7%
5.1		22	23.3%
6.0	Marshmallow	23	31.2%
7.0	Nougat	24	6.6%
7.1		25	0.5%

Data collected during a 7-day period ending on May 2, 2017. Any versions with less than 0.1% distribution are not shown.

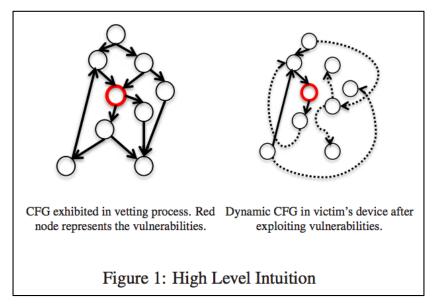
What about iOS?

- Apps are sandboxed
- Encrypted user data

– See recent news…

- App Store review process is (maybe) stricter
 - But not infallible: e.g., see
 Wang et al. "Jekyll on iOS:
 When Benign Apps Become
 Evil" (USENIX Security 2013)

No "sideloading" apps
 Unless you jailbreak



CSE 484 / CSE M 584: Computer Security and Privacy

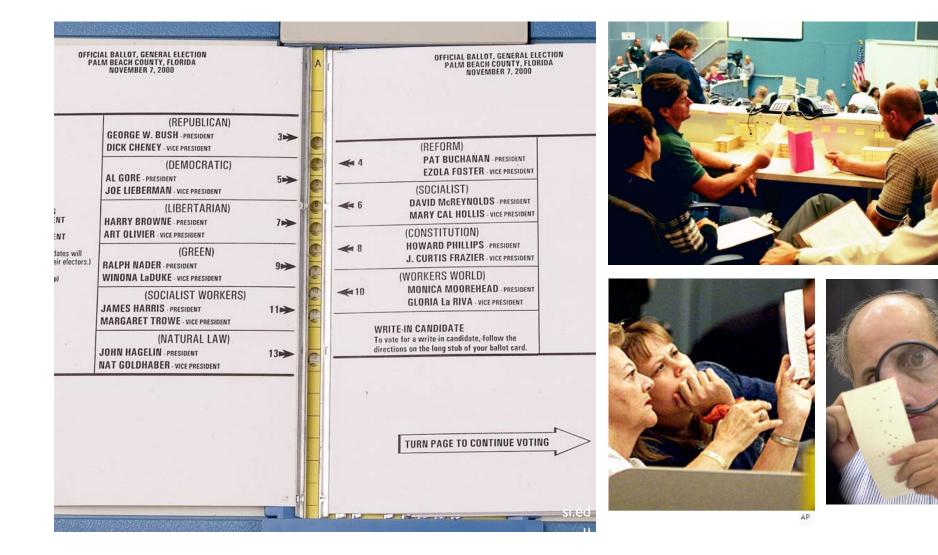
Usable Security [start]

Fall 2017

Franziska (Franzi) Roesner franzi@cs.washington.edu

Thanks to Dan Boneh, Dieter Gollmann, Dan Halperin, Yoshi Kohno, Ada Lerner, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...

Poor Usability Causes Problems



Importance in Security

- Why is usability important?
 - People are the critical element of any computer system
 - People are the real reason computers exist in the first place
 - Even if it is <u>possible</u> for a system to protect against an adversary, people may use the system in other, <u>less secure</u> ways

Usable Security Roadmap

- 2 case studies
 - Phishing
 - SSL warnings
- Step back: root causes of usability problems, and how to address

Case Study #1: Phishing

• Design question: How do you help users avoid falling for phishing sites?

A Typical Phishing Page



CSE 484 / CSE M 584 - Fall 2017

Safe to Type Your Password?

Bank of the West - Moz le <u>E</u> dit <u>V</u> iew Hi <u>s</u> tory	<u>B</u> ookmarks <u>T</u> ools <u>H</u> elp	http://www.	bankofthewest.com/ OW/home	☐ □ ×
BANK OF WE		Home Sign in ▼	Search GO Have a question? Contact Us.	Find us ZIP code or city & state GO
Products & Servi Checking Savings & CDs Credit Cards Loans Wealth Management & T Insurance	Buy a home Buy a new car Save for college Maximize home et Consolidate debt Try our financial ca	quity	Bank Online Apply for an account online Learn about online banking Enroll in eTimeBanker	eTimeBanker Login Where do I enter my password? Alternate Login
See all our Personal ba one	nking products »			www.bankofthewest.com

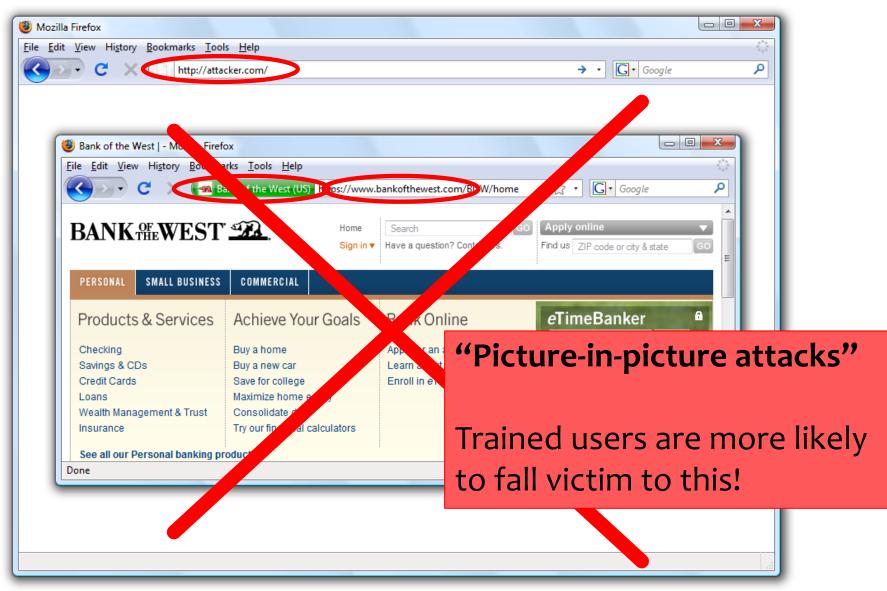
Safe to Type Your Password?

Bank of the West Phishing Page - Mozilla Firefox			
<u>File Edit V</u> iew Hi <u>s</u> tory <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp			
C X http://attacker.com/ogin	÷	• Google	٩
Bank of the West			
Gives me you pa55w0rds!			
User name:			
Password:			
Login			
Done			

Safe to Type Your Password?



Safe to Type Your Password?



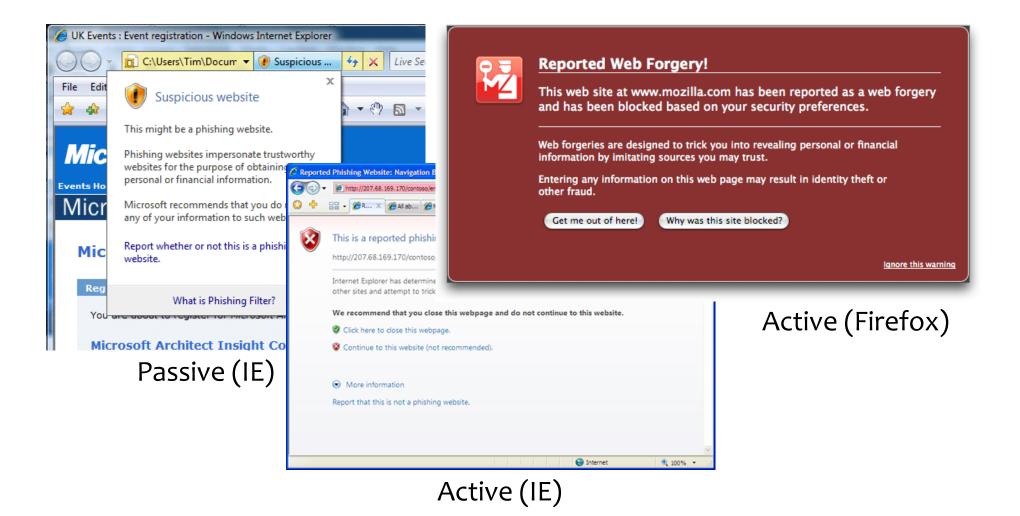
Experiments at Indiana University

- Reconstructed the social network by crawling sites like Facebook, MySpace, LinkedIn and Friendster
- Sent 921 Indiana University students a spoofed email that appeared to come from their friend
- Email redirected to a spoofed site inviting the user to enter his/her secure university credentials
 - Domain name clearly distinct from indiana.edu
- 72% of students entered their real credentials into the spoofed site

More Details

- Control group: 15 of 94 (16%) entered personal information
- Social group: 349 of 487 (72%) entered personal information
- 70% of responses within first 12 hours
- Adversary wins by gaining users' trust
- Also: If a site looks "professional", people likely to believe that it is legitimate

Phishing Warnings

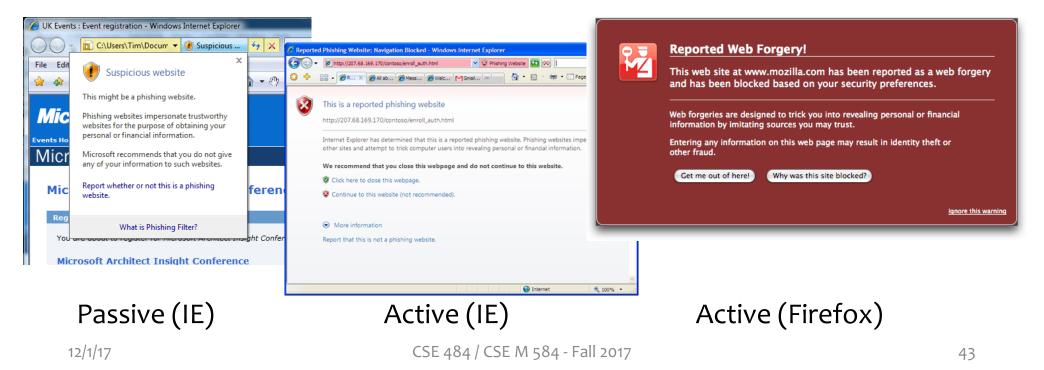


Are Phishing Warnings Effective?

- CMU study of 60 users
- Asked to make eBay and Amazon purchases
- All were sent phishing messages in addition to the real purchase confirmations
- Goal: compare <u>active</u> and <u>passive</u> warnings

Active vs. Passive Warnings

- Active warnings significantly more effective
 - Passive (IE): 100% clicked, 90% phished
 - Active (IE): 95% clicked, 45% phished
 - Active (Firefox): 100% clicked, 0% phished



User Response to Warnings

- Some fail to notice warnings entirely
 - Passive warning takes a couple of seconds to appear; if user starts typing, his keystrokes dismiss the warning
- Some saw the warning, closed the window, went back to email, clicked links again, were presented with the same warnings... repeated 4-5 times
 - Conclusion: "website is not working"
 - Users never bothered to read the warnings, but were still prevented from visiting the phishing site
 - Active warnings work!

Why Do Users Ignore Warnings?

- Don't trust the warning
 - "Since it gave me the option of still proceeding to the website, I figured it couldn't be that bad"
- Ignore warning because it's familiar (IE users)
 - "Oh, I always ignore those"
 - "Looked like warnings I see at work which I know to ignore"
 - "I thought that the warnings were some usual ones displayed by IE"
 - "My own PC constantly bombards me with similar messages"

Case Study #2: Browser SSL Warnings

- **Design question 1:** How to indicate encrypted connections to users?
- **Design question 2:** How to alert the user if a site's SSL certificate is untrusted?

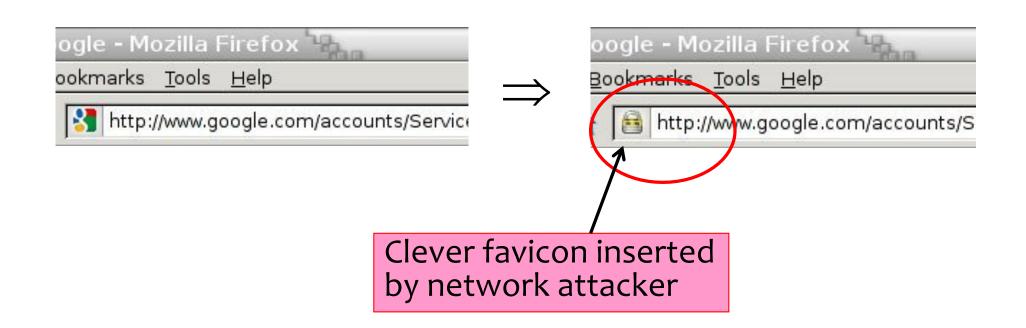
The Lock Icon

Secure https://mail.google.com/mail/u/0/#inbox

- Goal: identify secure connection
 - SSL/TLS is being used between client and server to protect against active network attacker
- Lock icon should only be shown when the page is secure against network attacker
 - Semantics subtle and not widely understood by users
 - Whose certificate is it??
 - Problem in user interface design

[Moxie Marlinspike]

Will You Notice?



Do These Indicators Help?

- "The Emperor's New Security Indicators"
 - http://www.usablesecurity.org/emperor/emperor.pdf

			Gr	oup		
Score	First chose not to enter password	1	2	3	$1\cup 2$	Total
0	upon noticing HTTPS absent	0 0%	0 0%	0 0%	0 0%	0 0%
1	after site-authentication image removed	0 0%	0 0%	2 9%	0 0%	2 4%
2	after warning page	8 47%	5 29%	12 55%	13 37%	25 44%
3	never (always logged in)	10 53%	12 71%	8 36%	22 63%	30 53%
	Total	18	17	22	35	57

Users don't notice the **absence** of indicators!

Aside (re: Phishing):

Site Authentication Image (SiteKey)

🖉 Bank of America Online Banking SiteKey V	/erify SiteKey - Windows Internet Explorer	
🚱 🗸 🖉 https://sitekey.bankofamerica.co	m/sas/signonSetup.do	
😤 🏶 🔊 Bank of America Online Banking		
Bank of America Higher Standards	Online Banking	
Confirm that your SiteKey is correct		
If you recognize your SiteKey, you'll know for sure that you are at the valid Bank of America site. Confirming your SiteKey is also how you'll know that it's safe to enter your Passcode and click t	the Sign In button.	
An asterisk (*) indicates a required field.	If you don't recognize yo	•
Your SiteKey: pelicans	SiteKey, don't enter you	r Passcode
If you don't recognize your don't enter your Passcode		
* Passcode: (4 - 20 Characters,case sensitiv	ve)	
Sign In		

Latest Design in Chrome

Secure https://mail.google.com/mail/u/0/#inbox

ntt	o-password	.badssl.cor	m × \					
\leftrightarrow \rightarrow C \bigcirc N	ot Secure	http-pa	ssword.ba	dssl.com				
🔴 🔴 🔵 De	veloper Too	ols - http:/	/http-pass	word.bads	ssl.com/			
Elements	Console	Sources	Network	Timeline	Profiles	>>	4 1	• • •
🛇 🍸 top	•	Preserve	log					
A This page include input in a non-se For more information	ecure cont	ext. A wa	arning has	been adde				<u>1</u>

Firefox vs. Chrome Warning

33% vs. 70% clickthrough rate



This Connection is Untrusted

You have asked Chrome to connect securely to reddit.com, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Get me out of here!

- Technical Details
- I Understand the Risks



This is probably not the site you are looking for!

You attempted to reach reddit.com, but instead you actually reached a server identifying itself as a248.e.akamai.net. This may be caused by a misconfiguration on the server or by something more serious. An attacker on your network could be trying to get you to visit a fake (and potentially harmful) version of reddit.com.

You should not proceed, especially if you have never seen this warning before for this site.

Proceed anyway Back to safety

Help me understand

Experimenting w/ Warning Design

#	Condition CTR	Ν
1	Control (default Chrome warning)	
2	Chrome warning with policeman	
3	Chrome warning with criminal	
4	Chrome warning with traffic light	
5	Mock Firefox	
6	Mock Firefox, no image	
7	Mock Firefox with corporate styling	
	Table 1. Click-through rates and sample size for condi	tions.

Experimenting w/ Warning Design

#	Condition	CTR	Ν
1	Control (default Chrome warning)	67.9%	17,479
2	Chrome warning with policeman		
3	Chrome warning with criminal		
4	Chrome warning with traffic light		
5	Mock Firefox		
6	Mock Firefox, no image		
7	Mock Firefox with corporate styling		
4	Table 1. Click-through rates and sample size This is probably not the site you are looking You attempted to reach reddit.com, but instead you actually reached a server identify a248.e.ekamal.net. This may be caused by a misconfiguration on the server or by sor An attacker on your network could be trying to get you to visit a fake (and potentially f	for! ring itself as mething more serious	
	reddit.com. You should not proceed, especially if you have never seen this warning before for this Proceed anyway Back to safety Help me understand	s sile.	-

Figure 1. The default Chrome SSL warning (Condition 1).

Experimenting w/ Warning Design

#	Condition	CTR	Ν
1	Control (default Chrome warning)	67.9%	17,479
2	Chrome warning with policeman	68.9%	17,977
3	Chrome warning with criminal	66.5%	18,049
4	Chrome warning with traffic light	68.8%	18,084
5	Mock Firefox		
-			

- 6 Mock Firefox, no image
- 7 Mock Firefox with corporate styling

Table 1. Click-through rates and sample size for conditions.

4	This is probably not the site you ar You attempted to reach reddit.com, but instead you actually reache a248.e.akumai.net. This may be caused by a misconfiguration on th An attacker on your network could be trying to get you to visit a fake reddit.com. You should not proceed, especially if you have never seen this ware	
	Proceed anyway Back to safety	Figure 4. The three images used in Conditions 2-4.
	Help me understand	rigure 4. The unice images used in Conditions 2.4.

Figure 1. The default Chrome SSL warning (Condition 1).

Experimenting w/ Warning Design

#	Condition	CTR	Ν
1	Control (default Chrome warning)	67.9%	17,479
2	Chrome warning with policeman	68.9%	17,977
3	Chrome warning with criminal	66.5%	18,049
4	Chrome warning with traffic light	68.8%	18,084
5	Mock Firefox	56.1%	20,023
6	Mock Firefox, no image	55.9%	19.297
7	Marte Einsfern mith an manufa stalling		

7 Mock Firefox with corporate styling

Table 1. Click-through rates and sample size for conditions.

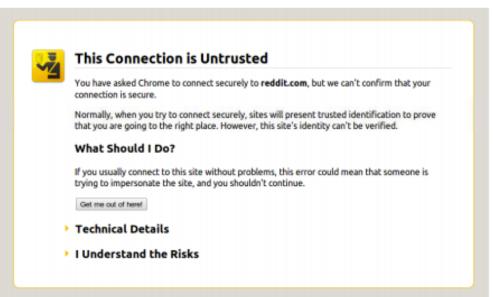


Figure 2. The mock Firefox SSL warning (Condition 5).

Experimenting w/ Warning Design

#	Condition	CTR	Ν
1	Control (default Chrome warning)	67.9%	17,479
2	Chrome warning with policeman	68.9%	17,977
3	Chrome warning with criminal	66.5%	18,049
4	Chrome warning with traffic light	68.8%	18,084
5	Mock Firefox	56.1%	20,023
6	Mock Firefox, no image	55.9%	19,297
7	Mock Firefox with corporate styling	55.8%	19,845

Table 1. Click-through rates and sample size for conditions.

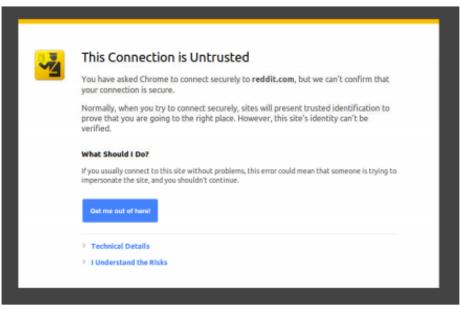


Figure 3. The Firefox SSL warning with Google styling (Condition 7).

Opinionated Design Helps!

The site's security certificate is not trusted!

You attempted to reach **192.168.17.129**, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications.

You should not proceed, especially if you have never seen this warning before for this site.

Proceed anyway Back to safety

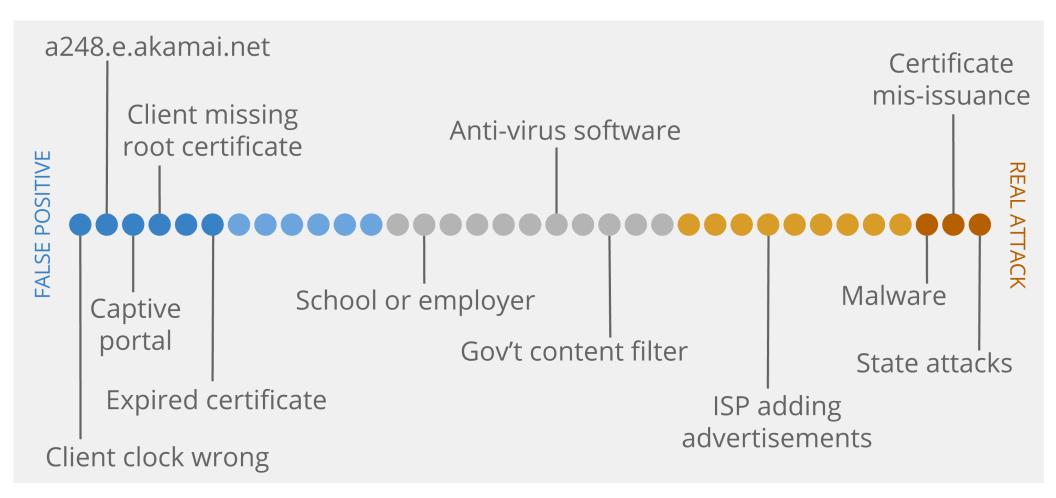
Help me understand

Adherence	Ν
30.9%	4,551

Opinionated Design Helps!

	The site's security certificate is not tru	isted!		
	You attempted to reach 192.168.17.129 , but the server presented a certi- trusted by your computer's operating system. This may mean that the se- credentials, which Chrome cannot rely on for identity information, or an a your communications. You should not proceed, especially if you have never seen this warning <u>Proceed anyway</u> <u>Back to safety</u>	Attaci mess Proc	ur connection is not private kers might be trying to steal your information from reddit.com ages, or credit cards). eed to the site (unsafe) Back to safety vanced	n (for example, passwords,
	► <u>Help me understand</u>			
×			Adherence	Ν
Your co	nnection is not private		Adherence 30.9%	N 4,551
Attackers mi	nnection is not private ight be trying to steal your information from www.example.com (for sswords, messages, or credit cards).			

Challenge: Meaningful Warnings



Stepping Back: Root Causes?

- Computer systems are complex; users lack intuition
- Users in charge of managing own devices
 - Unlike other complex systems, like healthcare or cars.
- Hard to gauge risks
 - "It won't happen to me!"
- Annoying, awkward, difficult
- Social issues
 - Send encrypted emails about lunch?...

How to Improve?

- Security education and training
- Help users build accurate mental models
- Make security invisible
- Make security the least-resistance path
- ?