CSE 484: Computer Security and Privacy

Vulnerability Finding + Patching Usability

Spring 2023

David Kohlbrenner
dkohlbre@cs

Thanks to Franzi Roesner, Dan Boneh, Dieter Gollmann, Dan Halperin, David Kohlbrenner, Yoshi Kohno, Ada Lerner, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials...
Exploit RCA and Patching
Root-Cause Analysis (RCA)

• Basically debugging, but you didn’t generate the input

• Consider:
  • What is different between a ‘normal’ interaction and the exploit?
  • What part(s) of the program are relevant to that interaction
    • Add logging/debugging here! But consider that it might affect the exploit...
  • What specifically happened that was ‘unusual’
  • Develop theories about what is happening
  • Test your theories!
The goals for RCAs

• Identify what the exploit accomplishes
• Identify the major steps the exploit takes
• Find the specific code components (if any exist) that are responsible
  • Aka: the vulnerability
  • Consider that an exploit might leverage missing features!
• Find ‘nearby’ bugs
  • Ie. If you fix the most-responsible line of code, is it still vulnerable?
• Plan out a patch
Project 0 (p0) RCAs

• Google Project 0 (aka p0) is the premiere publicly-disclosing bug hunting team

• They produce detailed writeups of many bugs, and work with Google’s Threat Analysis Group (aka TAG) to produce RCAs of in-the-wild bugs.

• You should read some p0 RCAs!
Patch writing goals

• Break the *specific* exploit strategy the exploit uses
• Break *similar* exploit strategies
  • Consider how XSS filtering worked in Lab 2!

• Minimize breaking explicit features of the program
• Minimize breaking *implicit* features of the program
Public bug finding - Terminology

• “Zero Days” – 0 days (aka “o-days”)
  • Refers to a bug that is made publicly known at the same time as the vendor is told
  • The vendor has had ‘0 days’ of lead time to fix it

• CVE Number
  • Common Vulnerabilities and Exposures
  • E.g. CVE-2022-4135

• CVSS
  • Common Vulnerability Scoring System
  • Very limited utility, scores barely correlated with impact

• CWE
  • Common Weakness Enumeration
  • Standardized list of bug types
Public bug finding - Disclosure

• At some point, the vendor finds out about the bug
  • Either publicly revealed by finder (an 0-day)
  • Internally found by code auditing
  • Found being used in-the-wild

• If you find the bug:
  • When do you disclose?
  • How do you disclose?
  • “Full-disclosure” vs “Coordinated disclosure” vs “Responsible disclosure”

• Bug bounty programs offer incentives to disclose
  • But at a cost: you usually have to sign NDAs
Anonymity (Tor)
Tor

• Second-generation onion routing network
  • http://tor.eff.org
  • Developed by Roger Dingledine, Nick Mathewson and Paul Syverson
  • Specifically designed for low-latency anonymous Internet communications

• Running since October 2003

• “Easy-to-use” client proxy
  • Freely available, can use it for anonymous browsing
Issues and Notes of Caution

• Passive traffic analysis
  • Infer from network traffic who is talking to whom
  • To hide your traffic, must carry other people’s traffic!

• Active traffic analysis
  • Inject packets or put a timing signature on packet flow

• Compromise of network nodes
  • Attacker may compromise some routers
    • Powerful adversaries may compromise “too many”
  • It is not obvious which nodes have been compromised
    • Attacker may be passively logging traffic
  • Better not to trust any individual router
    • Assume that some fraction of routers is good, don’t know which
Issues and Notes of Caution

• Tor isn’t completely effective by itself
  • Tracking cookies, fingerprinting, etc.
  • Exit nodes can see everything!
Issues and Notes of Caution

• The simple act of using Tor could make one a target for additional surveillance

• Hosting an exit node could result in illegal activity coming from your machine

• Tor not designed to protect against adversaries with the capabilities of a state (public statement by designers, at least in the past)
Usability and Security
Importance of Usability in Security

• Why is usability important?
  • People are the critical element of any computer system
    • People are the reason computers exist in the first place
  • Even if it is possible for a system to protect against an adversary, people may use the system in other, less secure ways
Usable Security Roadmap

• 2 case studies
  • HTTPS indicators + SSL warnings
  • Phishing

• Step back: root causes of usability problems, and how to address
Case Study #1: Browser HTTPS Indicators

• **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?
  • You discussed this in section a couple weeks ago
The Lock Icon

• 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
Will You Notice?

[Clever favicon inserted by network attacker]
Do These Indicators Help? (2007)

• “The Emperor’s New Security Indicators”
  • http://www.usablesecurity.org/emperor/emperor.pdf

<table>
<thead>
<tr>
<th>Score</th>
<th>First chose not to enter password...</th>
<th>Group</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>upon noticing HTTPS absent</td>
<td>0 0%</td>
</tr>
<tr>
<td>1</td>
<td>after site-authentication image removed</td>
<td>0 0%</td>
</tr>
<tr>
<td>2</td>
<td>after warning page</td>
<td>8 47%</td>
</tr>
<tr>
<td>3</td>
<td>never (always logged in)</td>
<td>10 53%</td>
</tr>
<tr>
<td></td>
<td><strong>Total</strong></td>
<td>18</td>
</tr>
</tbody>
</table>

Lesson:
Users don’t notice the absence of indicators!
Newer Versions of Chrome

c. 2017

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

2022

mail.google.com/mail/u/0/#inbox

Not secure http-password.badssl.com

Not secure https://self-signed.badssl.com

2023/2024

example.com

example.com

Connection is secure
Case Study #1: Browser HTTPS Indicators

• **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?
Challenge: Meaningful Warnings

See current designs for different conditions at https://badssl.com/.
Firefox vs. Chrome Warning

33% vs. 70% clickthrough rate
Experimenting w/ Warning Design

<table>
<thead>
<tr>
<th>#</th>
<th>Condition</th>
<th>CTR</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Control (default Chrome warning)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Chrome warning with policeman</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Chrome warning with criminal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Chrome warning with traffic light</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Mock Firefox</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Mock Firefox, no image</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Mock Firefox with corporate styling</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 1. Click-through rates and sample size for conditions.
# Experimenting w/ Warning Design

<table>
<thead>
<tr>
<th>#</th>
<th>Condition</th>
<th>CTR</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Control (default Chrome warning)</td>
<td>67.9%</td>
<td>17,479</td>
</tr>
<tr>
<td>2</td>
<td>Chrome warning with policeman</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Chrome warning with criminal</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Chrome warning with traffic light</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Mock Firefox</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Mock Firefox, no image</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Mock Firefox with corporate styling</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

![Figure 1. The default Chrome SSL warning (Condition 1).](image-url)
Experimenting w/ Warning Design

<table>
<thead>
<tr>
<th>#</th>
<th>Condition</th>
<th>CTR</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Control (default Chrome warning)</td>
<td>67.9%</td>
<td>17,479</td>
</tr>
<tr>
<td>2</td>
<td>Chrome warning with policeman</td>
<td>68.9%</td>
<td>17,977</td>
</tr>
<tr>
<td>3</td>
<td>Chrome warning with criminal</td>
<td>66.5%</td>
<td>18,049</td>
</tr>
<tr>
<td>4</td>
<td>Chrome warning with traffic light</td>
<td>68.8%</td>
<td>18,084</td>
</tr>
<tr>
<td>5</td>
<td>Mock Firefox</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Mock Firefox, no image</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Mock Firefox with corporate styling</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

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

Figure 4. The three images used in Conditions 2-4.

[Felt et al.]
Experimenting w/ Warning Design

<table>
<thead>
<tr>
<th>#</th>
<th>Condition</th>
<th>CTR</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Control (default Chrome warning)</td>
<td>67.9%</td>
<td>17,479</td>
</tr>
<tr>
<td>2</td>
<td>Chrome warning with policeman</td>
<td>68.9%</td>
<td>17,977</td>
</tr>
<tr>
<td>3</td>
<td>Chrome warning with criminal</td>
<td>66.5%</td>
<td>18,049</td>
</tr>
<tr>
<td>4</td>
<td>Chrome warning with traffic light</td>
<td>68.8%</td>
<td>18,084</td>
</tr>
<tr>
<td>5</td>
<td>Mock Firefox</td>
<td>56.1%</td>
<td>20,023</td>
</tr>
<tr>
<td>6</td>
<td>Mock Firefox, no image</td>
<td>55.9%</td>
<td>19,297</td>
</tr>
<tr>
<td>7</td>
<td>Mock Firefox with corporate styling</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

Figure 2. The mock Firefox SSL warning (Condition 5).
Experimenting w/ Warning Design

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

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

<table>
<thead>
<tr>
<th>Adherence</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>30.9%</td>
<td>4,551</td>
</tr>
</tbody>
</table>
Opinionated Design Helps!

<table>
<thead>
<tr>
<th>Adherence</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>30.9%</td>
<td>4,551</td>
</tr>
<tr>
<td>32.1%</td>
<td>4,075</td>
</tr>
<tr>
<td>58.3%</td>
<td>4,644</td>
</tr>
</tbody>
</table>

[Felt et al.]
Today’s warnings (2022)
Deprecated encryption schemes

This site can’t provide a secure connection

rc4.badssl.com uses an unsupported protocol.

Error code: SSL_ERROR_NO_CIPHER_OVERLAP

- The page you are trying to view cannot be shown because the authenticity of the received data could not be verified.
- Please contact the website owners to inform them of this problem.

Learn more...
Expired certificates

Warning: Potential Security Risk Ahead

Firefox detected an issue and did not continue to expired.badssl.com. The website is either misconfigured or your computer clock is set to the wrong time.

It's likely the website's certificate is expired, which prevents Firefox from connecting securely. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

What can you do about it?

Your computer clock is set to 12/7/2022. Make sure your computer is set to the correct date, time, and time zone in your system settings, and then refresh expired.badssl.com.

If your clock is already set to the right time, the website is likely misconfigured, and there is nothing you can do to resolve the issue. You can notify the website's administrator about the problem.

Learn more...
Self-signed certificates

Your connection is not private

Attckers might be trying to steal your information from self-signed.badssl.com (for example, passwords, messages, or credit cards). Learn more

NET:ERR_CERT_AUTHORITY_INVALID

Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to self-signed.badssl.com. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

Learn more...
Untrusted Root certificate

Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to untrusted-root.badssl.com. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

What can you do about it?

The issue is most likely with the website, and there is nothing you can do to resolve it.

If you are on a corporate network or using anti-virus software, you can reach out to the support teams for assistance. You can also notify the website's administrator about the problem.

Learn more...

To get Chrome's highest level of security, turn on enhanced protection

Advanced

Back to safety
Address Bar behaviors (2022)
Does anything stand out?

• Pollev
• What makes warnings hard, especially over time?
• Why do Firefox and Chrome make different warning designs?
Case Study #2: Phishing

• **Design question:** How do you help users avoid falling for phishing sites?
A Typical Phishing Page

Weird URL
http instead of https
Safe to Type Your Password?
Safe to Type Your Password?

Bank of the West

Gives me you pa55w0rds!

User name:

Password:

Login

Done
Safe to Type Your Password?
Safe to Type Your Password?

“Picture-in-picture attacks”
Trained users are more likely to fall victim to this!
Phishing Warnings (2008)
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

[Image: Screenshots of passive and active warnings in different browsers]
If you don’t recognize your personalized “SiteKey”, don’t enter your Passcode.
Modern anti-phishing

- Largely driven by Google Safe Browsing
  - Browser sends 32-bit prefix of hash(url)
  - API says: good or bad
Modern warnings

Deceptive site ahead

Attackers on testsafebrowsing.appspot.com may trick you into doing something dangerous like installing software or revealing your personal information (for example, passwords, phone numbers, or credit cards). Learn more
Deceptive site ahead

Firefox blocked this page because it may trick you into doing something dangerous like installing software or revealing personal information like passwords or credit cards.

Advisory provided by Google Safe Browsing.
The page ahead may try to charge you money

These charges could be one-time or recurring and may not be obvious.
The site ahead contains malware

Attackers currently on testsafebrowsing.appspot.com might attempt to install
dangerous programs on your computer that steal or delete your information (for example,
photos, passwords, messages, and credit cards) Learn more

Details

Back to safety
Which warning is ‘better’?

• For user security?
• For user agency?
• For user understanding?
• For... what?