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 ...
Logistics

• Lab 2 is due next week
  • Remember we have a lot of resources/recordings on lab2 stuff!
• Lab 3 will go out shortly(?) after Lab 2 is due
Surprise not-quiz time

XSS again
Reflected XSS

1. visit web site
2. receive malicious page
3. click on link
4. echo user input
5. send valuable data

User victim

Attack server

Server victim

5/10/2023
Stored XSS

1. Inject malicious script
2. Request content
3. Receive malicious script
4. Steal valuable data
XSRF (aka CSRF)

1. Establish session
2. Visit server
3. Receive malicious page
4. Send forged request

User victim

Attack server

Server victim
Authentication
Default Passwords

• Examples from Mitnick’s “Art of Intrusion”
  • U.S. District Courthouse server: “public” / “public”
  • NY Times employee database: pwd = last 4 SSN digits

• Mirai IoT botnet
  • Weak and default passwords on routers and other devices
Weak Passwords

• RockYou hack
  • “Social gaming” company
  • Database with 32 million user passwords from partner social networks
  • Passwords stored in the clear
  • December 2009: entire database hacked using an SQL injection attack and posted on the Internet
  • One of many such examples!
Weak Passwords

- **RockYou hack**
  - ““
  - D
  - P
  - D
  - P

<table>
<thead>
<tr>
<th>Rank</th>
<th>Password</th>
<th>Number of Users with Password (absolute)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>123456</td>
<td>290731</td>
</tr>
<tr>
<td>2</td>
<td>12345</td>
<td>79078</td>
</tr>
<tr>
<td>3</td>
<td>123456789</td>
<td>76790</td>
</tr>
<tr>
<td>4</td>
<td>Password</td>
<td>61958</td>
</tr>
<tr>
<td>5</td>
<td>iloveyou</td>
<td>51622</td>
</tr>
<tr>
<td>6</td>
<td>princess</td>
<td>35231</td>
</tr>
<tr>
<td>7</td>
<td>rockyou</td>
<td>22588</td>
</tr>
<tr>
<td>8</td>
<td>1234567</td>
<td>21726</td>
</tr>
<tr>
<td>9</td>
<td>12345678</td>
<td>20553</td>
</tr>
<tr>
<td>10</td>
<td>abc123</td>
<td>17542</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Rank</th>
<th>Password</th>
<th>Number of Users with Password (absolute)</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>Nicole</td>
<td>17168</td>
</tr>
<tr>
<td>12</td>
<td>Daniel</td>
<td>16409</td>
</tr>
<tr>
<td>13</td>
<td>babygirl</td>
<td>16094</td>
</tr>
<tr>
<td>14</td>
<td>monkey</td>
<td>15294</td>
</tr>
<tr>
<td>15</td>
<td>Jessica</td>
<td>15162</td>
</tr>
<tr>
<td>16</td>
<td>Lovely</td>
<td>14950</td>
</tr>
<tr>
<td>17</td>
<td>michael</td>
<td>14898</td>
</tr>
<tr>
<td>18</td>
<td>Ashley</td>
<td>14329</td>
</tr>
<tr>
<td>19</td>
<td>654321</td>
<td>13984</td>
</tr>
<tr>
<td>20</td>
<td>Qwerty</td>
<td>13856</td>
</tr>
</tbody>
</table>
Password Policies

• Old recommendation:
  • 7 or 8 characters, at least 3 out of {digits, upper-case, lower-case, non-alphanumeric}, no dictionary words, change every 4 months, password may not be similar to previous 12 passwords…

[Inglesant and Sasse, “The True Cost of Unusable Password Policies”]
Password Policies

• Old recommendation:
  • 7 or 8 characters, at least 3 out of {digits, upper-case, lower-case, non-alphanumeric}, no dictionary words, change every 4 months, password may not be similar to previous 12 passwords...

• But ... results in frustrated users and less security
  • Burdens of devising, learning, forgetting passwords
  • Users construct passwords insecurely, write them down
    • Can’t use their favorite password construction techniques (small changes to old passwords, etc.)
  • Heavy password re-use across systems
  • (Password managers can help)

[Inglesant and Sasse, “The True Cost of Unusable Password Policies”]
“New” (2017) NIST Guidelines 😊

• Remove requirement to periodically change passwords
• Screen for commonly used passwords
• Allow copy-paste into password fields
  • But concern: what apps have access to clipboard?
• Allow but don’t require arbitrary special characters
• Etc.

“This summer, hackers destroyed my entire digital life in the span of an hour. My Apple, Twitter, and Gmail passwords were all robust—seven, 10, and 19 characters, respectively, all alphanumeric, some with symbols thrown in as well—but the three accounts were linked, so once the hackers had conned their way into one, they had them all. They really just wanted my Twitter handle: @mat.”
Improving(?) Passwords

• Add biometrics
  • For example, keystroke dynamics or voiceprint

• Graphical passwords
  • Goal: easier to remember? no need to write down?

• Password managers
  • Examples: LastPass, KeePass, built into browsers
  • Can have security vulnerabilities...

• Two-factor authentication
  • Leverage phone (or other device) for authentication
Password managers

• Generation
  • Secure generation of random passwords

• Management
  • Allows for password-per-account

• Safety?
  • Single point of failure
  • Vulnerability?
  • Phishing?
Multi-Factor Authentication
Questions:

Do you use 2-factor auth?
Do you use a password manager?
Why or why not?

How to compromise account protected with hardware second factor?
Secondary Factors Do Help!

Account takeover prevention rates, by challenge type

Device-based challenges
- On-device prompt: 90%, 99%
- SMS code: 76%, 96%
- Security key: 100%, 100%

Knowledge-based challenges
- Secondary email address: 73%, 63%
- Phone number: 26%, 100%
- Last sign-in location: 10%

Both device- and knowledge-based challenges help thwart automated bots, while device-based challenges help thwart phishing and even targeted attacks.
Why does 2FA (sometimes) work?

• Stops phishing, when it is hardware token

• Doesn’t when it is SMS 😞
  • (Curious for an example? Attend Ariana’s lecture in 1.5 weeks!)
Hardware 2FA tokens (U2F/FIDO)
Graphical Passwords

- Many variants... one example: Passfaces
  - Assumption: easy to recall faces
Graphical Passwords

• Another variant: draw on the image (Windows 8)

• Problem: users choose predictable points/lines
Unlock Patterns

• Problems:
  • Predictable patterns (familiar pattern by now)
  • Smear patterns
  • Side channels: apps can use accelerometer and gyroscope to extract pattern!
What About Biometrics?

• Authentication: **What you are**

• Unique identifying characteristics to authenticate user or create credentials
  
  • Biological and physiological: Fingerprints, iris scan
  • Behaviors characteristics - how perform actions: Handwriting, typing, gait

• Advantages:
  
  • Nothing to remember
  • Passive
  • Can’t share (generally)
  • With perfect accuracy, could be fairly unique
What are reasons to use/not use biometrics?

• Canvas
Issues with Biometrics

• Private, but not secret
  • Maybe encoded on the back of an ID card?
  • Maybe encoded on your glass, door handle, ...
  • Sharing between multiple systems?

• Revocation is difficult (impossible?)
  • Sorry, your iris has been compromised, please create a new one...

• Physically identifying
  • Soda machine to cross-reference fingerprint with DMV?

• Birthday paradox
  • With false accept rate of 1 in a million, probability of false match is above 50% with only 1609 samples
Attacking Biometrics

• An adversary might try to steal biometric info
  • Malicious fingerprint reader
    • Consider when biometric is used to derive a cryptographic key
  • Residual fingerprint on a glass
Passkeys (2023)

• An actual, deployed, genuine *password replacement*
  • *Also a 2fa replacement!*
  • *And a username replacement!*

• Basic goals:
  • Store some sort of key on user end-devices
  • Use that key to login to Stuff
  • Don’t allow losing the key
  • Somehow make the key moving between devices Easy
Privacy and web tracking
A topic in flux

• Tracking via cookies

• Tracking via other methods

• Fingerprinting
Ads That Follow You

Advertisers (and others) track your browsing behaviors for the purposes of targeted ads, website analytics, and personalized content.
Third-Party Web Tracking

These ads allow criteo.com to link your visits between sites, even if you never click on the ads.

Browsing profile for user 123:
- cnn.com
- theonion.com
- adult-site.com
- political-site.com
6,521% growth 2011 to 2022

24% growth 2020 to 2022

Concerns About Privacy

The New York Times
‘Do Not Track’ Privacy Bill Appears in Congress
By TANZINA VEGA

And the privacy legislation just keeps on coming.

On Friday, two bills were introduced in Washington in support of a Do Not Track mechanism that would give users control over how much of their data was collected by advertisers and other online companies.

By JENNIFER VALENTINO-DEVRIES, JEREMY SINGER-VINE and ASHKAN SOLTANI
December 24, 2012
First and Third Parties

- **First-party cookie**: belongs to top-level domain.
- **Third-party cookie**: belongs to domain of embedded content (such as image, iframe).
Anonymous Tracking

Trackers included in other sites use third-party cookies containing unique identifiers to create browsing profiles.
Basic Tracking Mechanisms

- Tracking requires:
  1. re-identifying a user.
  2. communicating id + visited site back to tracker.

```markdown
Hypertext Transfer Protocol
GET /pixel/p-3aud4J6uA4Z6Y.gif?labels=InvisibleBox&busty=2710 HTTP/1.1\r\nHost: pixel.quantserve.com\r\nConnection: keep-alive\r\nAccept: image/webp, */*; q=0.8\r\nUser-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_2) AppleWebKit/537.36\nReferer: http://www.thelonion.com/\r\nAccept-Encoding: gzip, deflate, sdch\r\nAccept-Language: en-US, en; q=0.8\r\nCookie: mc=52a65386-f1de1-00ade-0b26e; d=ENkBRqGH4GYEA35MMIL74MKiyDsIA2MQI1Q
```
Tracking Technologies

- HTTP Cookies
- HTTP Auth
- HTTP Etags
- Content cache
- IE userData
- HTML5 protocol and content handlers
- HTML5 storage
- Flash cookies
- Silverlight storage
- TLS session ID & resume
- Browsing history
- window.name
- HTTP STS
- DNS cache
- “Zombie” cookies that respawn (http://samy.pl/evercookie)
Other Trackers?

“Personal” Trackers
Personal Tracking

• Tracking is **not anonymous** (linked to accounts).
• Users **directly visit tracker’s site** → evades some defenses.
How prevalent is tracking? (2011)

524 unique trackers on Alexa top 500 websites (homepages)

457 domains (91%) embed at least one tracker. (97% of those include at least one cross-site tracker.)

50% of domains embed between 4 and 5 trackers.

One domain includes 43 trackers.
Who/what are the top trackers? (2011)
How has this changed over time?

• The web has existed for a while now...
  - What about tracking before 2011?
  - What about tracking before 2009?

• Solution: time travel!
The Wayback Machine to the Rescue

Time travel for web tracking: http://trackingexcavator.cs.washington.edu
1996-2016: More & More Tracking

• More trackers of more types, more per site, more coverage
Defenses to Reduce Tracking

• Do Not Track?

Send a ‘Do Not Track’ request with your browsing traffic

Do Not Track is not a technical defense: trackers must honor the request.
Defenses to Reduce Tracking

- Do Not Track proposal?
- Private browsing mode?

Private browsing mode doesn’t protect against network attackers fully.

You’ve gone incognito
Now you can browse privately, and other people who use this device won’t see your activity. However, downloads and bookmarks will be saved. Learn more

Chrome won’t save the following information:
- Your browsing history
- Cookies and site data
- Information entered in forms

Your activity might still be visible to:
- Websites you visit
- Your employer or school
- Your internet service provider
Defenses to Reduce Tracking

• Do Not Track proposal?
• Private browsing mode?
• Third-party cookie blocking?
3\textsuperscript{rd} party cookies

• Safari and FF (mostly) now block 3\textsuperscript{rd} party cookies
  
  • https://webkit.org/blog/10218/full-third-party-cookie-blocking-and-more/
  

• Chrome...

  “By undermining the business model of many ad-supported websites, blunt approaches to cookies encourage the use of opaque techniques such as fingerprinting (an invasive workaround to replace cookies), which can actually reduce user privacy and control. We believe that we as a community can, and must, do better.”

Aug 2022: Remove 3\textsuperscript{rd} party cookies by 2024