CSE 484: Computer Security and Privacy

Authentication

Spring 2021

Tadayoshi Kohno

Thanks to Franzi Roesner, Dan Boneh, Dieter Gollmann, Dan Halperin, David Kohlbrenner, Yoshi Kohno, John Manferdelli, John Mitchell, Vitaly Shmatikov, Bennet Yee, and many others for sample slides and materials ...
Administrivia

• Lab 2 due May 25
• Final Project Checkpoint due May 26
• Lab 3 has become extra credit
Basic Problem

How do you prove to someone that you are who you claim to be?

Any system with access control must solve this problem.
Many Ways to Prove Who You Are

• What you know
  • Passwords
  • Answers to questions that only you know

• Where you are
  • IP address, geolocation

• What you are
  • Biometrics

• What you have
  • Secure tokens, mobile devices
A slightly more fundamental question

• What are we trying to prove?
Passwords and Computer Security

• In 2012, 76% of network intrusions exploited weak or stolen credentials (username/password)
  • Source: Verizon Data Breach Investigations Report

• In Mitnick’s “Art of Intrusion” 8 out of 9 exploits involve password stealing and/or cracking

• First step after any successful intrusion: install sniffer or keylogger to steal more passwords

• Second step: run cracking tools on password files
  • Cracking needed because modern systems usually do not store passwords in the clear
UNIX-Style Passwords

• How should we store passwords on a server?
  • In cleartext?
  • Encrypted?
  • Hashed?
Password Hashing

• Instead of user password, store \( H(\text{password}) \)
• When user enters password, compute its hash and compare with entry in password file
  • System does not store actual passwords!
  • System itself can’t easily go from hash to password
    • Which would be possible if the passwords were encrypted

• Hash function \( H \) must have some properties
  • One-way: given \( H(\text{password}) \), hard to find password
    • No known algorithm better than trial and error
  • “Slow” to compute
UNIX Password System

• Approach: Hash passwords
• Problem: passwords are not truly random
  • With 52 upper- and lower-case letters, 10 digits and 32 punctuation symbols, there are $94^8 = 6$ quadrillion possible 8-character passwords ($\approx 2^{52}$)
  • **BUT:** Humans like to use dictionary words, human and pet names $= 1$ million common passwords
Dictionary Attack

• Dictionary attack is possible because many passwords come from a small dictionary
  • Attacker can pre-compute $H(\text{word})$ for every word in the dictionary – this only needs to be done once!
    • This is an offline attack
    • Once password file is obtained, cracking is instantaneous
  • Sophisticated password guessing tools are available
    • Take into account freq. of letters, password patterns, etc.
Salt

franzi:fURxfg.4hLBX:14510:30:Franzi:/u/franzi:/bin/csh

salt
(chosen randomly when password is first set)

/ etc / passwd entry

Password

hash(salt,pwd)

• Users with the same password have different entries in the password file
• Offline dictionary attack becomes much harder
Advantages of Salting

• Without salt, attacker can pre-compute hashes of all dictionary words once for all password entries
  • Same hash function on all UNIX machines
  • Identical passwords hash to identical values; one table of hash values can be used for all password files

• With salt, attacker must compute hashes of all dictionary words once for each password entry
  • With 12-bit random salt, same password can hash to $2^{12}$ different hash values
  • Attacker must try all dictionary words for each salt value in the password file

• Pepper: Secret salt (not stored in password file)
Shadow Password

username:x:14510:30:User Name:/u/username:/bin/csh

Hashed password is no longer stored in a world-readable file

Hashed passwords are stored in /etc/shadow file which is only readable by system administrator (root)
Other Password Security Risks

• Keystroke loggers
  • Hardware
  • Software (spyware)

• Shoulder surfing

• Same password at multiple sites

• Broken implementations
  • Recall TENEX timing attack

• Social engineering
Other Issues

• Usability
  • Hard-to-remember passwords?
  • Carry a physical object all the time?

• Denial of service
  • Attacker tries to authenticate as you, account locked after three failures
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
  
  • “RockYou hack
  
  • 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

<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”]
Image from http://www.interactivetools.com/staff/dave/damons_office/
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.

Recovering Passwords

Palin E-Mail Hacker Says It Was Easy
By Kim Zetter | September 18, 2008 | 10:05 am | Categories: Elections, Hacks and Cracks

After the password recovery was reenabled, it took seriously 45 mins on wikipedia and google to find the info, Birthday? 15 seconds on wikipedia, zip code? well she had always been from Wasilla, and it only has 2 zip codes (thanks online postal service!)

The second was somewhat harder, the question was “where did you meet your spouse?” did some research, and apparently she had eloped with mister palin after college, if you'll look on some of the screenshots that I took and other fellow anon have so graciously put on photobucket you will see the google search for “palin eloped” or some such in one of the tabs.

I found out later though more research that they met at high school, so I did variations of that, high, high school, eventually hit on “Wasilla high” I promptly changed the password to popcorn and took a cold shower...
“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
Multi-Factor Authentication
FIDO + Hardware Two Factors
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?
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: Fingerprint, 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
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
Malaysia car thieves steal finger

By Jonathan Kent
BBC News, Kuala Lumpur

Police in Malaysia are hunting for members of a violent gang who chopped off a car owner's finger to get round the vehicle's hi-tech security system.

The car, a Mercedes S-class, was protected by a fingerprint recognition system.

Accountant K Kumaran's ordeal began when he was run down by four men in a small car as he was about to get into his Mercedes in a Kuala Lumpur suburb.
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
Attacking Biometrics

[Starbug -- http://istouchidhackedyet.com/]
Attacking Biometrics

[Starbug -- http://istouchidhackedyet.com/]
Attacking Biometrics

Making dummy print from wood glue

[Starbug -- http://istouchidhackedyet.com/]
Attacking Biometrics

Using dummy print

[Starbug -- http://istouchidhackedyet.com/]