

# Introduction

---

CS463/ECE424

University of Illinois



Security Mindset  
Threat Model  
Case Studies

---



# Goal of this Lecture

---

- Define security
- Introduce (revisit) security mindset
  - Begin to think like an attacker
  - Begin to think like a defender
  - Learn to reason about threats, risks
  - Learn to balance security costs and benefits

# What is Computer Security?

---

- A collection of **properties** that hold in a **system** in the presence of an **adversary** under a set of **constraints**

# What is Computer Security?

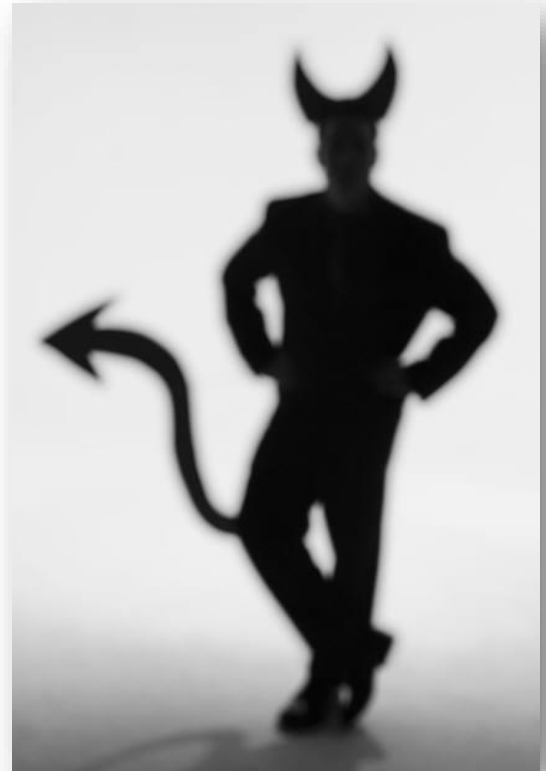
---

- A collection of **properties** that hold in a **system** in the presence of an **adversary** under a set of **constraints**
- Desktop, phones, web servers, data centers, network, ..., IoT devices, smart home, cars, ...
- Hardware, software, data

# Meet the Adversary

---

- Computer security studies how systems behave in the presence of an adversary



# Meet the Adversary

---

- Computer security studies how systems behave in the presence of an **adversary**
  - a.k.a. the attacker
  - a.k.a. the bad guy

\* An intelligence that actively tries to cause the system to misbehave.



# Think like an Attacker

---

- Think outside the box: Not constrained by system designer's worldview & assumptions.





# Think like an Attacker

---

- Think outside the box: Not constrained by system designer's worldview & assumptions.
- Look for weakest links – easiest to attack.



# Think like an Attacker

---

- Think outside the box: Not constrained by system designer's worldview & assumptions.
- Look for weakest links – easiest to attack.
- **Practice thinking like an attacker:** *For every system you interact with, think about what it means for it to be secure, and how it could be broken by an attacker.*

# Think as a Defender

---

- Security policy (goals)
  - What properties are we trying to enforce?
- Threat model (constraints)
  - Who are the attackers? Capabilities? Motivations?
  - What attacks to consider vs. ignore?
- Countermeasures

# Security Properties: CIA / AAA

---

- What properties are we trying to enforce?
  - **C**onfidentiality (privacy)
    - Prevent unauthorized parties from accessing certain data/system
  - **I**ntegrity
    - Prevent unauthorized parties from tampering with certain data/system
  - **A**vailability
    - Make sure certain data/system is available to users
  - ...

# Security Properties: CIA / AAA

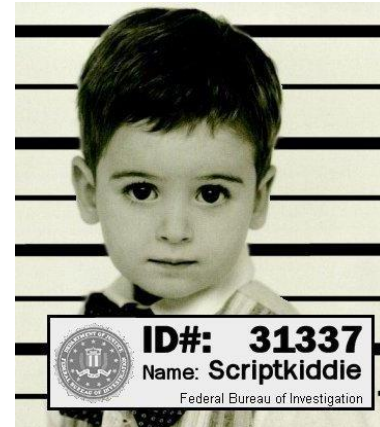
---

- What **properties** are we trying to enforce?
  - **Authenticity**
    - Proof of true identity/origin
  - **Anonymity**
    - Cannot be distinguished from others
  - **Accountability**
    - The ability to identify the responsible party
  - ...

# Threat Models

---

- Who are the attackers? Motives? Capabilities? Degree of access? Knowledge?  
(Know your enemy!)



# Threat Models

---

- Who are the attackers? Motives? Capabilities? Degree of access? Knowledge?  
(Know your enemy!)
- What kinds of attacks do we need to prevent?
- What kinds of attacks should we ignore?

# Risk Assessment

---

- What would security breaches cost us?
  - Direct costs: Money, property, safety, ...
  - Indirect costs: Reputation, future business, ...
  
- How likely are the breaches?
  - Probability of attacks?
  - Probability of attack success?



# Rational Paranoia

---



**PARANOIA**

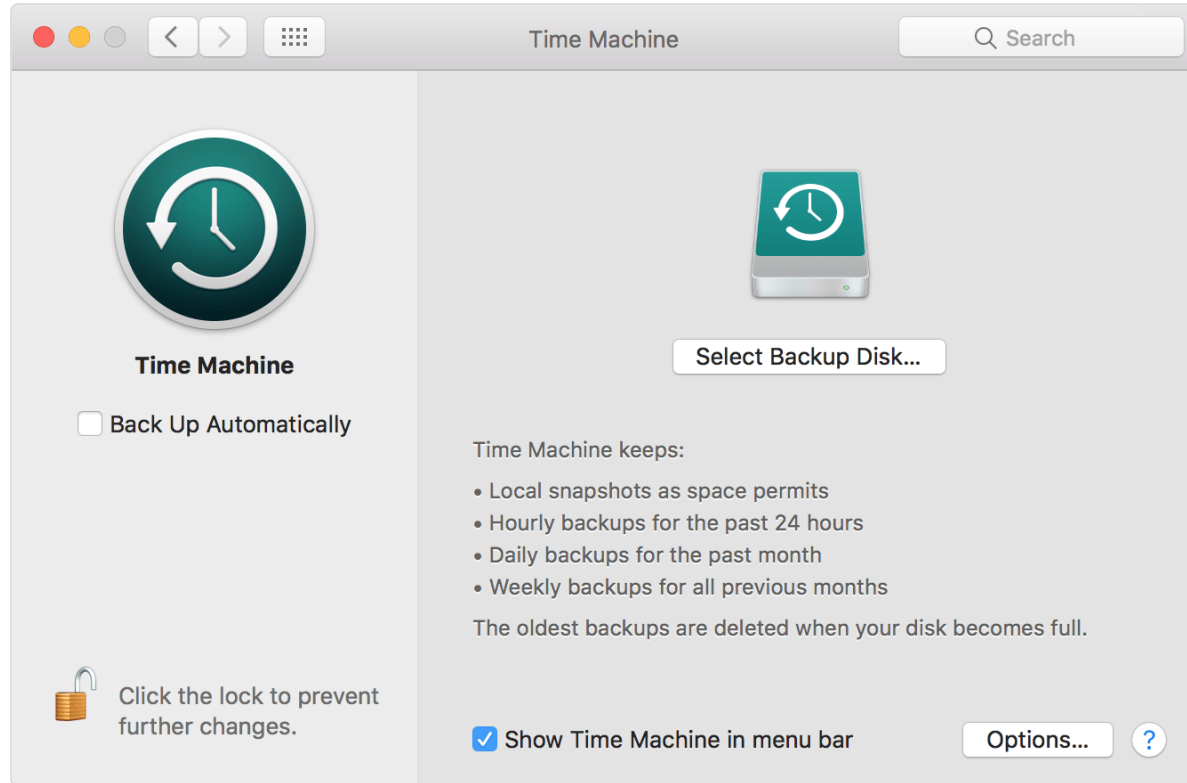
Yes. Tiny rodents with surveillance equipment **ARE** watching you.

# Countermeasures

---

- No security mechanism is free
  - Direct costs: Design, implementation, performance, ...
  - Indirect costs: Lost productivity/convenience, added complexity, ...
- No system is ever completely secure. Challenge is to rationally weigh costs vs. risks
  - Human psychology makes reasoning about high cost/low probability events hard

# Defense: Backups



# Defense: Automatic Updates



The App Store keeps OS X and apps from the App Store up to date.

- Automatically check for updates
    - Download newly available updates in the background  
You will be notified when the updates are ready to be installed
    - Install app updates
    - Install OS X updates
    - Install system data files and security updates
  - Automatically download apps purchased on other Macs  
Can't determine if automatic downloads are enabled due to a network problem
- 

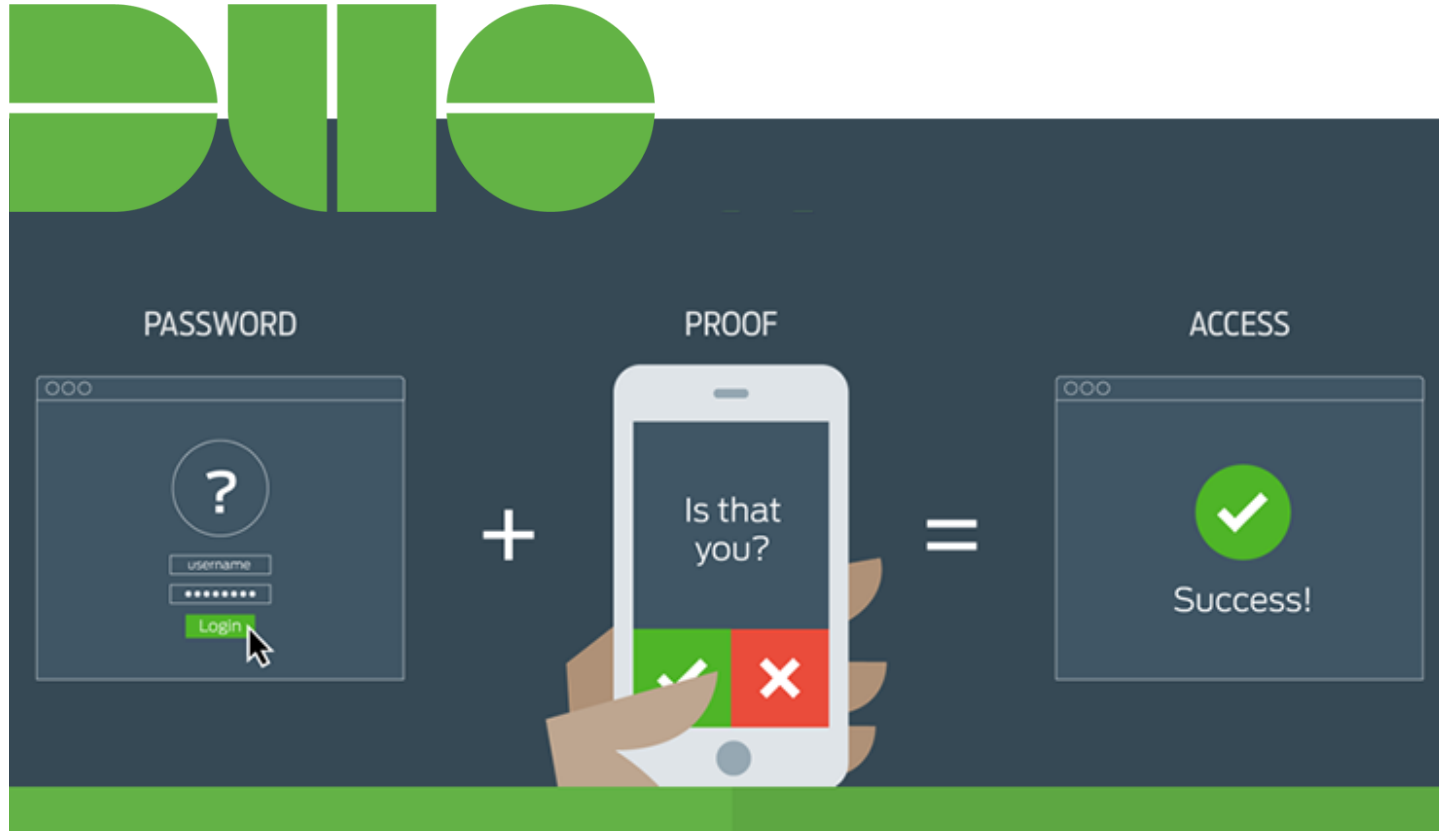
Last check was Thursday, December 1, 2016

Check Now





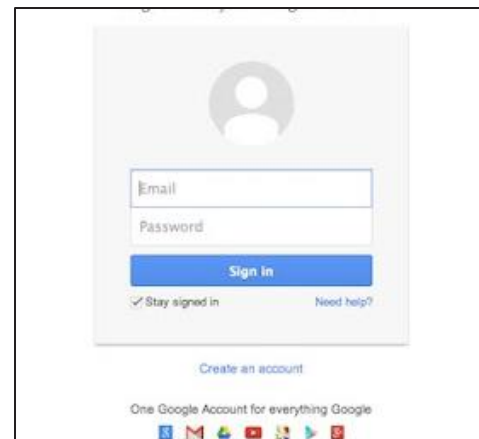
# Defense: Two Factor Authentication



# Extended Case Study: User Authentication

---

Why is “password” often insufficient to secure your account?



';--have i been pwned?

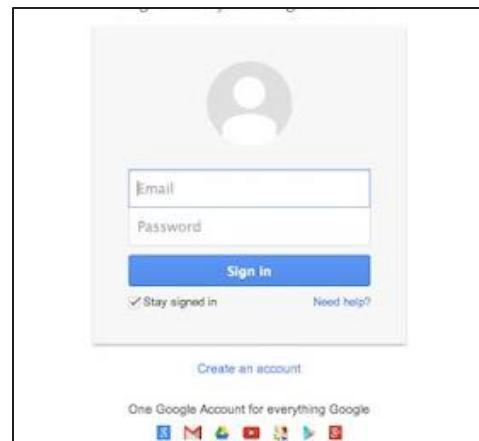
Check if your email or phone is in a data breach

# Extended Case Study: User Authentication

Why is “password” often insufficient to secure your account?

Data breaches expose user passwords

- Users often reuse passwords!
- A study (based on 62 million leaked passwords from 29 million users) shows:
  - 38% users have once reused the same password in two different services
  - 21% users once slightly modified an existing password to sign up for a new service [1]



'--have i been pwned?

Check if your email or phone is in a data breach

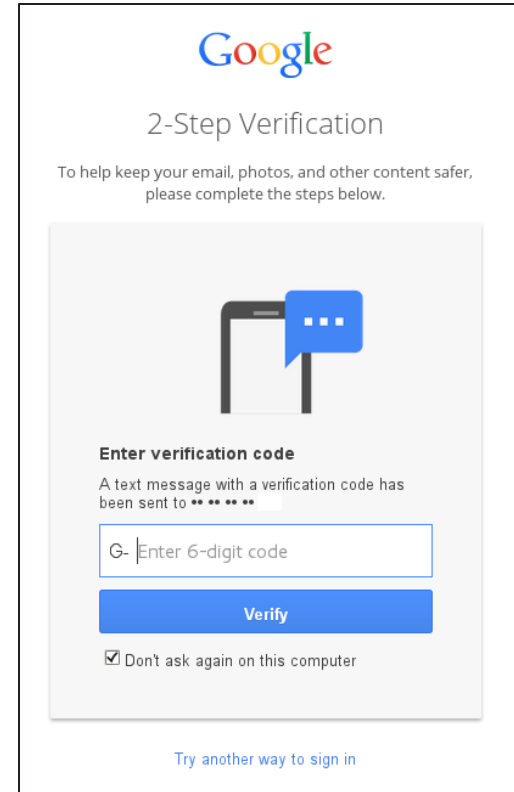
[1] The Next Domino To Fall: Empirical Analysis of User Passwords across Online Services, CODASPY, 2018.

<https://gangw.cs.illinois.edu/pass.pdf>



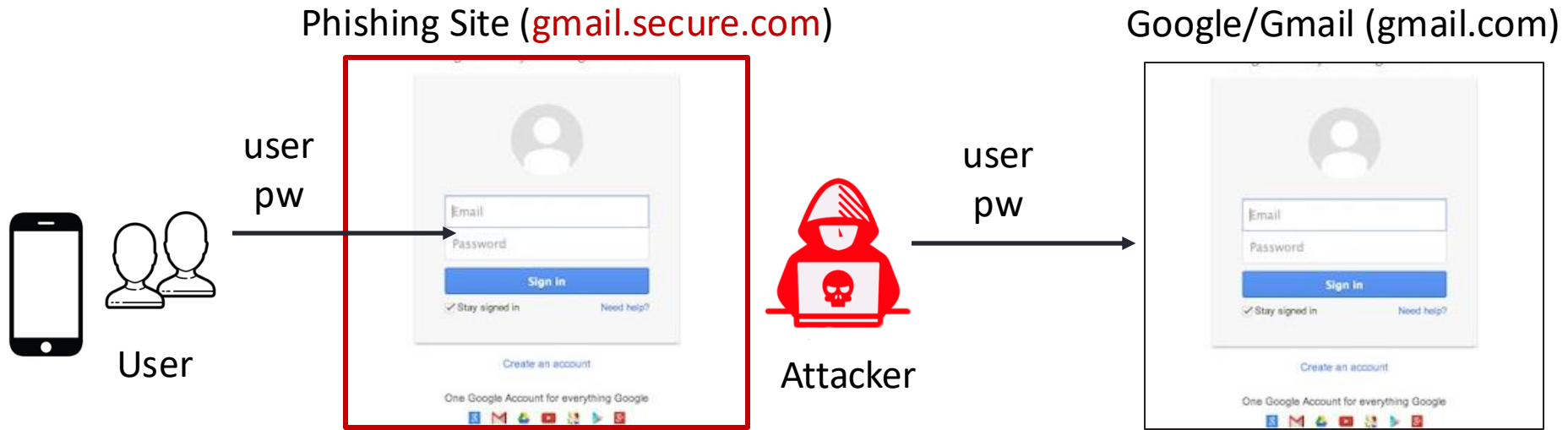
# Case Study: User Authentication at End-Point

- How about two-factor authentication (2FA)?
  - Idea: an additional factor to verify who you are
  - SMS, DuoMobile, etc.
- Is 2FA secure enough?



The screenshot shows the Google 2-Step Verification process. At the top is the Google logo, followed by the text "2-Step Verification". Below this is a message: "To help keep your email, photos, and other content safer, please complete the steps below." The main content area features an illustration of a smartphone with a blue speech bubble containing three dots. Below the illustration, the text reads "Enter verification code" and "A text message with a verification code has been sent to \* \* \* \* \*". There is a text input field with a "G-" icon and the placeholder text "Enter 6-digit code". A blue "Verify" button is positioned below the input field. At the bottom of the form, there is a checked checkbox with the text "Don't ask again on this computer". A link at the very bottom says "Try another way to sign in".

# Bypassing Standard 2FA via Real-Time Phishing



# Bypassing Standard 2FA via Real-Time Phishing

Phishing Site ([gmail.secure.com](http://gmail.secure.com))

Google/Gmail ([gmail.com](http://gmail.com))



User

user  
pw

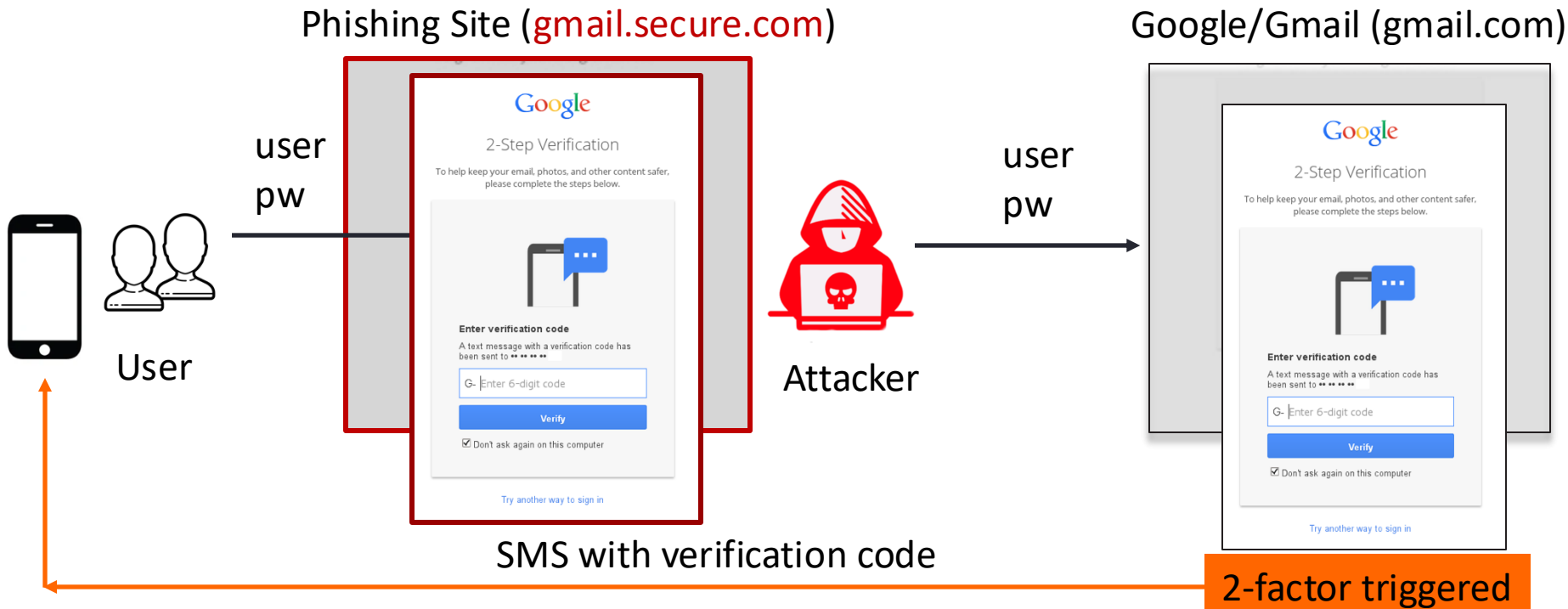


Attacker

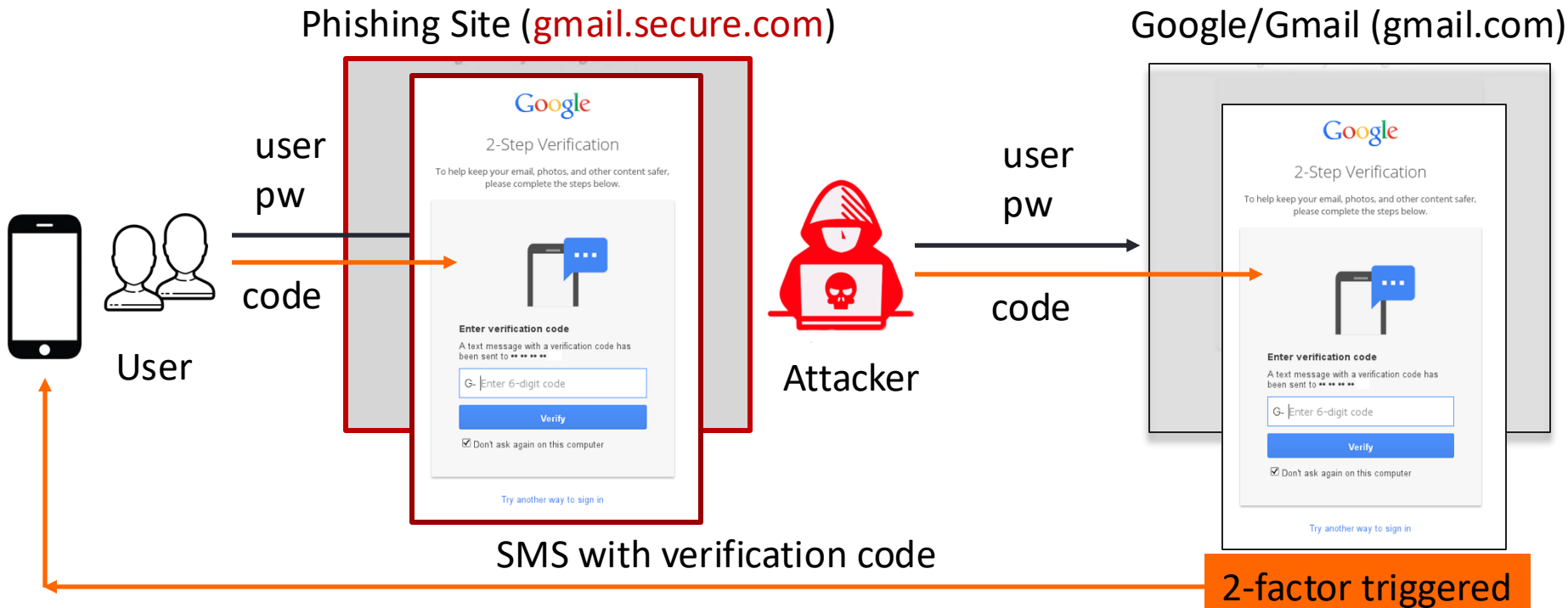
user  
pw

2-factor triggered

# Bypassing Standard 2FA via Real-Time Phishing



# Bypassing Standard 2FA via Real-Time Phishing

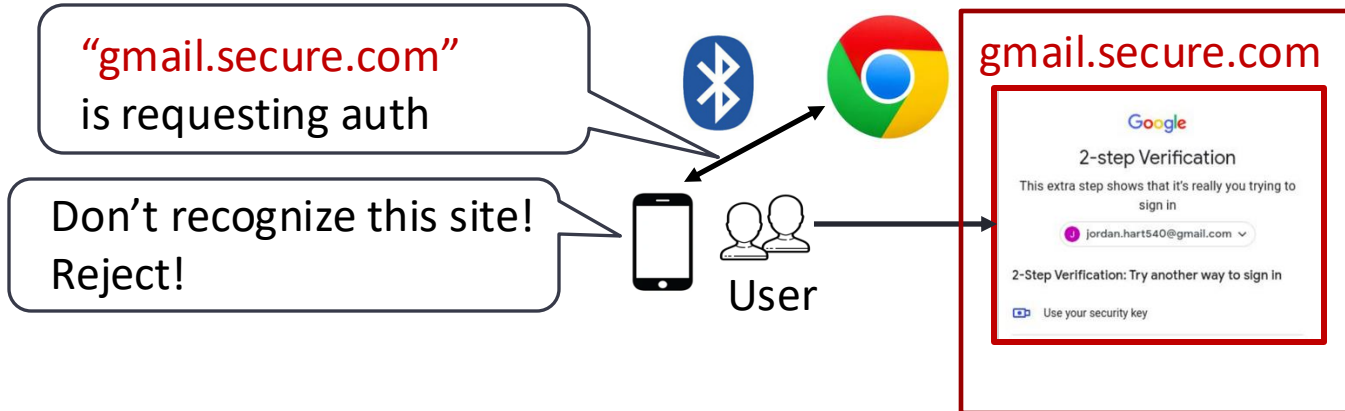


# Bypassing Standard 2FA via Real-Time Phishing

- Root cause: the phone (identity provider) cannot distinguish who sent the authentication request (real gmail vs. phishing), code not bonded to website

# Bypassing Standard 2FA via Real-Time Phishing

- Root cause: the phone (identity provider) cannot distinguish who sent the authentication request (real gmail vs. phishing), code not bonded to website
- One potential solution: FIDO Universal Second Factor (U2F)
  - The user's browser tells the authentication device (phone) which website is requesting;
  - A security token is unique for each website to avoid identity confusion



# References

---

- [1] Chun Wang, Steve T.K. Jan, Hang Hu, Douglas Bossart, and Gang Wang. “The Next Domino To Fall: Empirical Analysis of User Passwords across Online Services”. In Proceedings of The ACM Conference on Data and Applications Security and Privacy (CODASPY), 2018
- [2] Enis Ulqinaku, Hala Assal, AbdelRahman Abdou, Sonia Chiasson, and Srdjan Capkun. “Is Real-time Phishing Eliminated with FIDO? Social Engineering Downgrade Attacks against FIDO Protocols”, In Proceedings of USENIX Security, 2021.



# Discussion Question

---

- If Apple introduced Face ID today, what's your reaction?
  - Adversaries? Risk assessment?
  - Countermeasures? Costs/benefits?