HPC & Data Science Summer Institute

Security

Tuesday, August 6, 2024

10:15 am – 11:-00 am (Pacific Time)

SDSC
SAN DIEGO SUPERCOMPUTER CENTER

UC San Diego

Thank You!

What to Expect

- What This Isn't
  - "How-To" Guidance
  - "All You Need to Know"

- Generalization
  - Awareness
  - Tools
  - Mindset

StyleGAN2 (Karras et al.)

Coming Up…

- J is a PI who followed some advice from a forum.
- Here’s what happened to his lab.

Security Folklore

Potions

Just use this and nothing bad will happen.

- A one-size-fits-all product or practice.
  - All you need to do to be secure.
  - Red Flag: “Won’t impact your work.”
- Examples:
  - “Just install <security software>, it’s the best!”
  - “Just run a firewall, it will keep the hackers out.“
  - “Just install a VPN, it will keep the hackers from attacking your laptop.”

Potions: cont.

What's the problem?

- Different use-cases have their own security needs.
- Different use-cases have their own tolerance for disruptions.
- “How do they know my use-case is applicable?”
- Some potions are useful, none are sufficient.

Invisibility Cloaks

Nothing to see here!

- Inaction by arguing they're not a potential victim.

- Examples:
  - "My research is public."
  - "I don't have any sensitive data."
  - "I have nothing to hide."
  - "I'm just some random person."

Invisibility Cloaks: cont.

What's the problem?

- Attackers don't know that there's nothing interesting until they break in.
- You don't know what the attacker is looking for.
- Not all harm is caused by an attacker.
  - Other researchers make mistakes.
  - Technical issues.

Tin-Foil Hats

Everything is out to get me.

- Inaction because no action is sufficient or it's overwhelming.
- Examples:
  - "It's going to happen anyway, why bother?"
  - "I don't have time for this."
  - "Security is YOUR problem, not mine."

Do Research
Be Secure
JAKE-CLARK.TUMBLR
imgflip.com

Tin-Foil Hats: cont.

What's the problem?

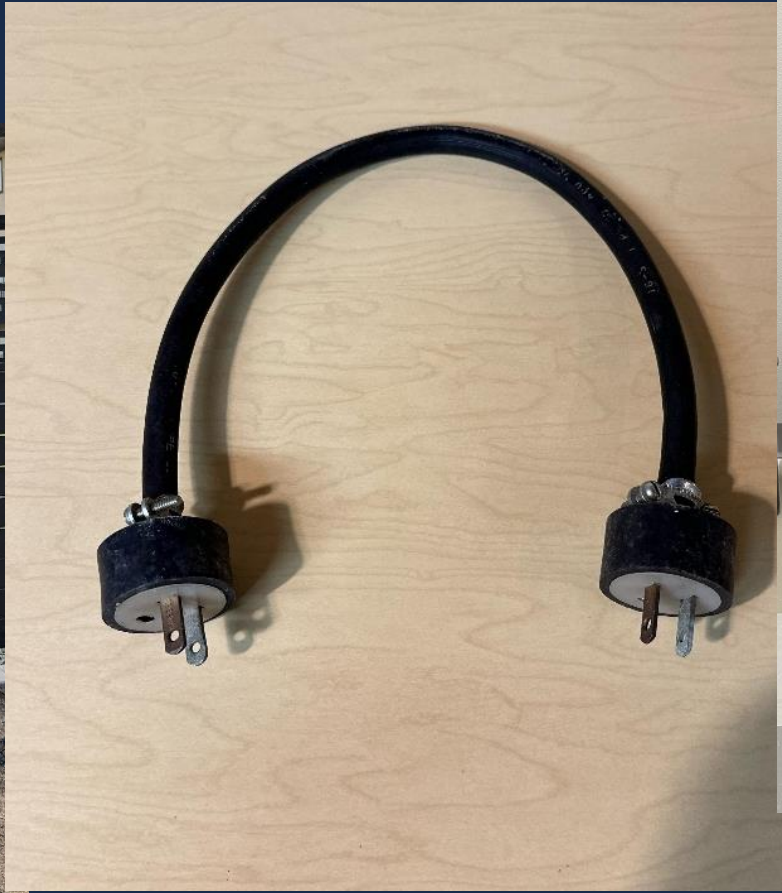
- You have a lot of control.
  - Make attacks more likely to fail.
  - Make successful attacks less impactful.
- Promotes a false dichotomy.

An Approach to Security

- Spot danger.
- Reduce the danger.

- Have a contingency plan.

Let's Get Dangerous!



Case Study

SSHut Down

StyleGAN2 (Karras et al.)

SSHut Down

- J’s researchers found their accounts disabled at several institutions.
- All the computers in the lab needed to be analyzed and cleaned-up.
- Almost two weeks of disruption.

SSHut Down

But Wait, There's More!

- Security Analysts at multiple HPC operators involved.
- Hundreds of person-hours spent.

- … But at least the lab's data wasn't controlled or encumbered.
  - So, there's that!

SSHut Down

A Little Background: One Person, Multiple Sites

account @ *Site 2*

account @ *Site 1*

account @ *Site n*

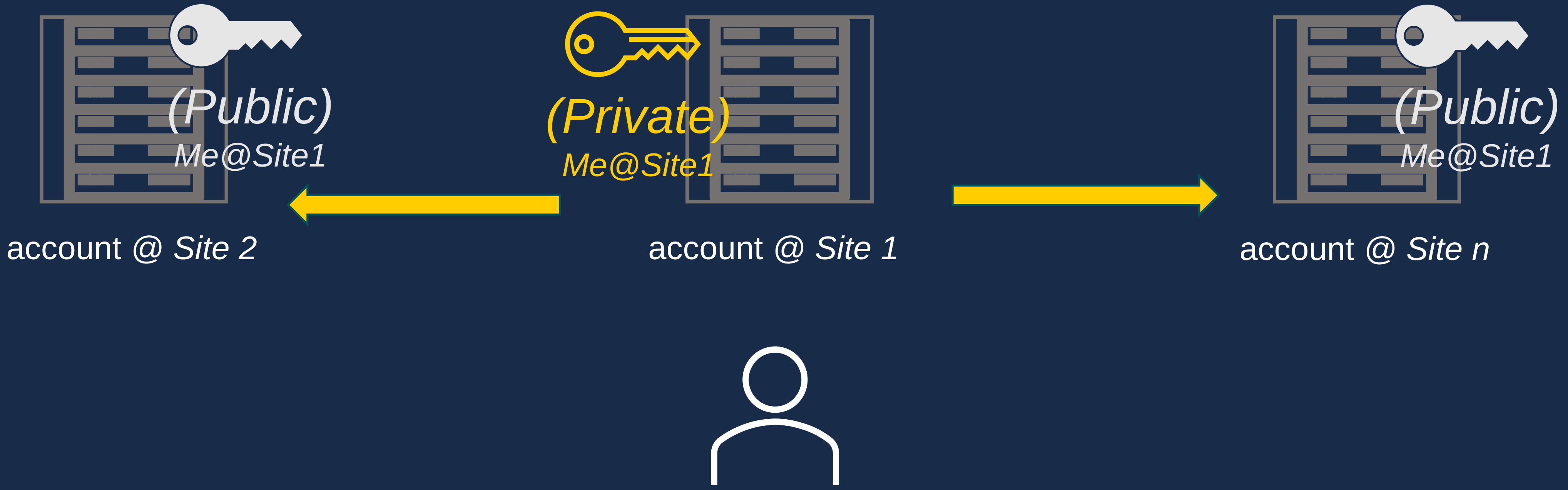
SSHut Down

When Not-A-Password Is A Password

- Need to log in from one CI environment to another quickly.
- Can script something, however that needs a password.
- Knew password in a text file is bad.
- SSH Keys?

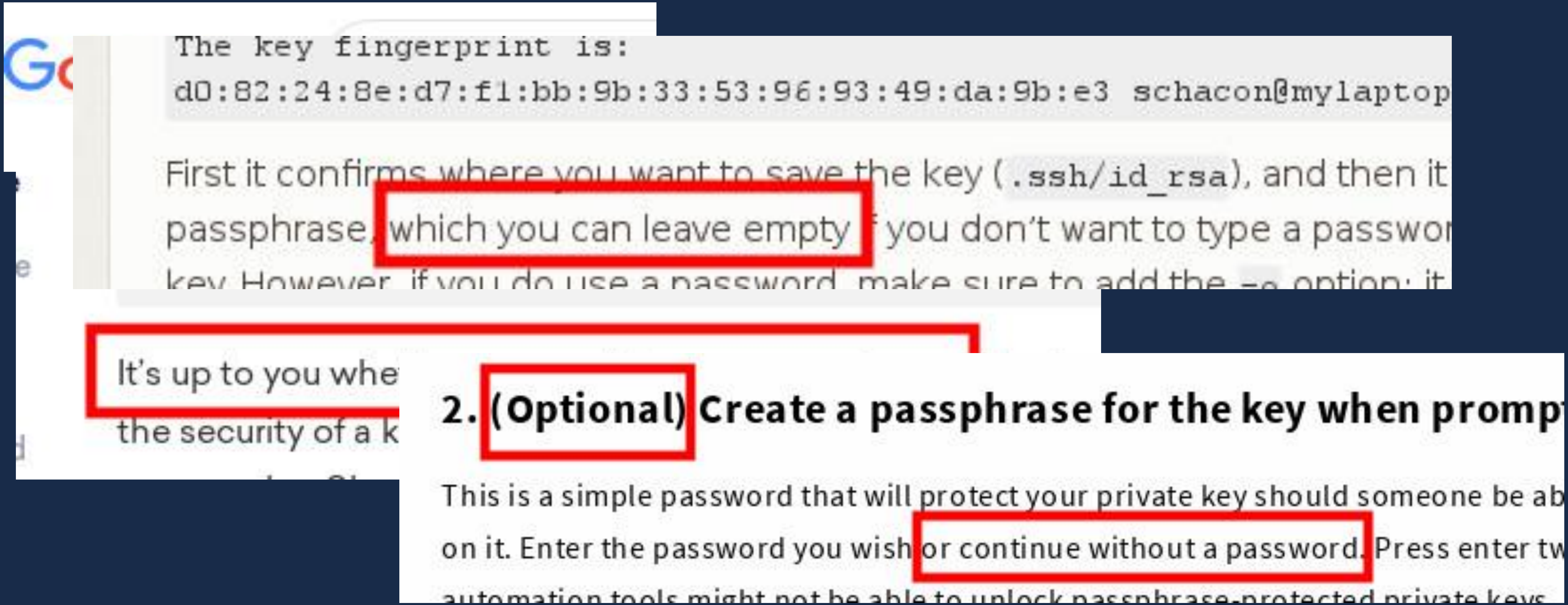
SSHut Down

Background: SSH Keys



SSHut Down

When Not-A-Password Is A Password



```
The key fingerprint is:
d0:82:24:8e:d7:f1:bb:9b:33:53:96:93:49:da:9b:e3 schacon@mylaptop
```

First it confirms where you want to save the key (`.ssh/id_rsa`), and then it passphrase, which you can leave empty f you don't want to type a passwor key. However, if you do use a password, make sure to add the `-o` option; it

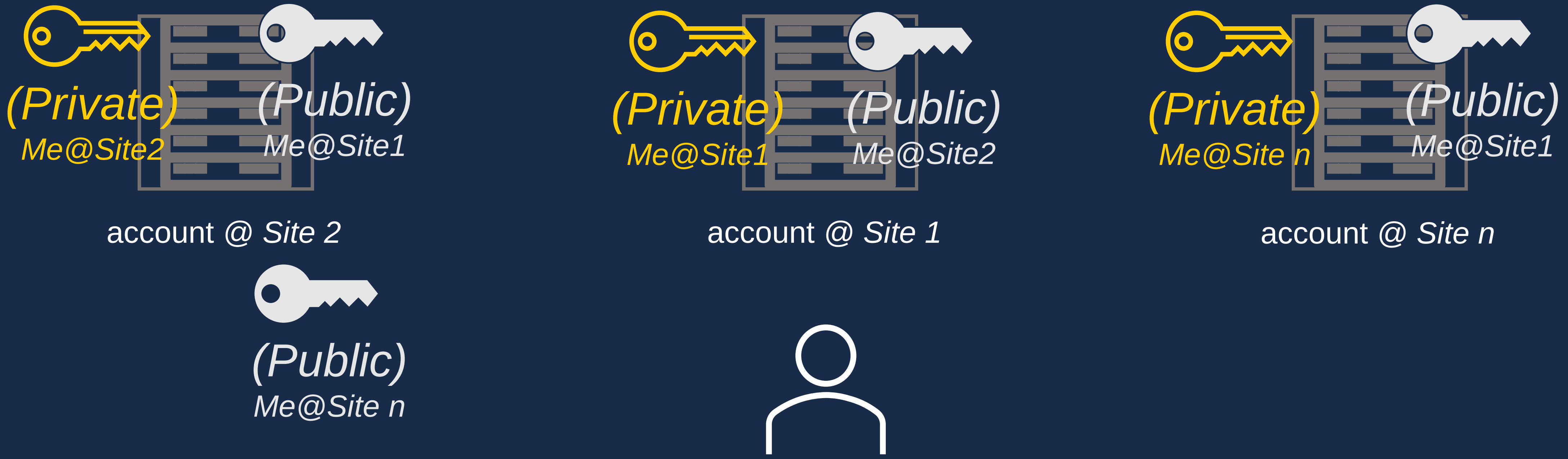
It's up to you whe the security of a k

2. (Optional) Create a passphrase for the key when promp

This is a simple password that will protect your private key should someone be ab on it. Enter the password you wish or continue without a password. Press enter tw automation tools might not be able to unlock passphrase-protected private keys.

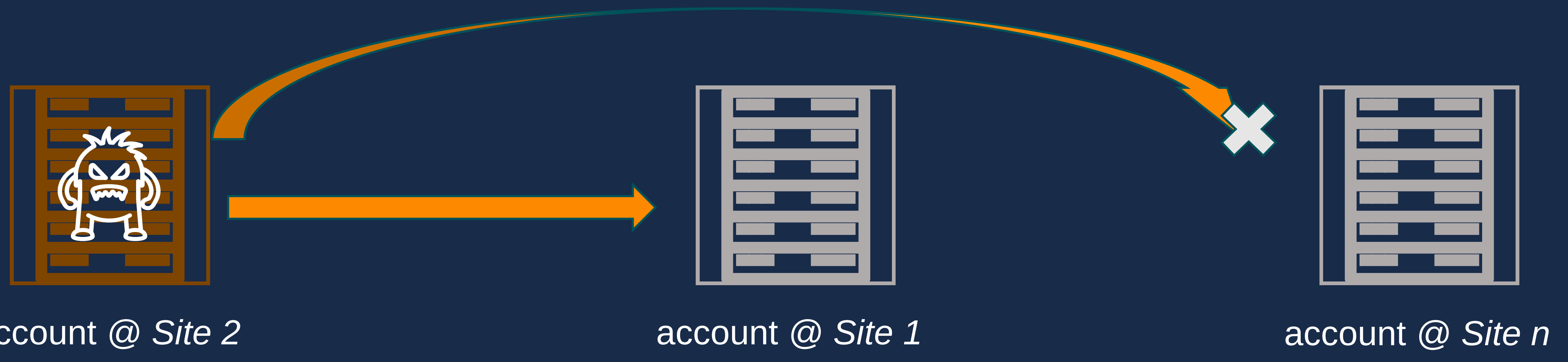
SSHut Down

Building A Web of Mistrust



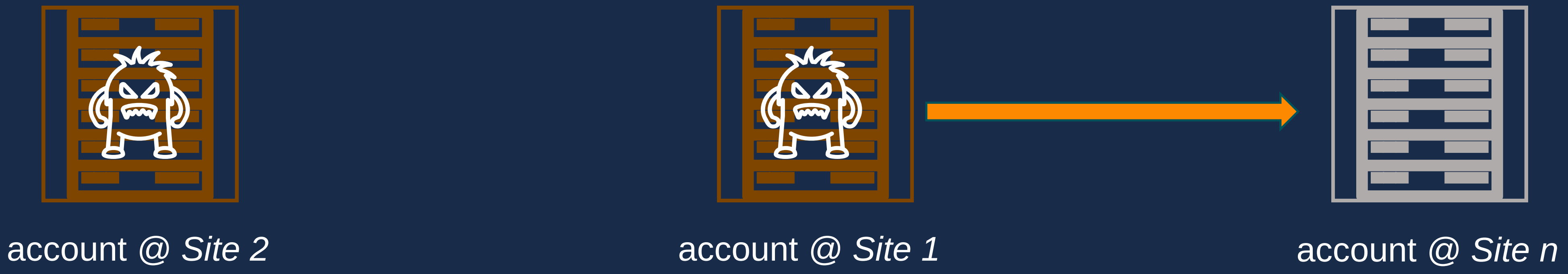
SSHut Down

One Intrusion, Multiple Sites



SSHut Down

One Intrusion, Multiple Sites (part 2)



account @ *Site 2*

account @ *Site 1*

account @ *Site n*

SSHut Down

One Intrusion, Multiple Sites (part 3)

account @ *Site 2*

account @ *Site 1*

account @ *Site n*

SSHut Down

That's Not All, Folks!

- Lab researchers did the same with their own accounts.
- Some individuals added their coworkers' public keys to their account.
- At least one lab machine allowed one of the private keys to log in to the *root* account. Attacker could become anyone in lab.

- $O(n^2)$ relationships!

SSHut Down

Spot the Danger!

- SSH Keys let an SSH Client in possession of a particular *private key* log in to an SSH Server authorizing the corresponding *public key*.
  - What happens if someone else gets a copy of the private key?
  - Isn’t the private key like a password?
  - Isn’t storing a password on-disk *dangerous*?
- Some individuals added their coworkers’ public keys to their account.
  - Isn’t this like giving the coworker their password?
  - Isn’t that against policy?

SSHut Down

Reduce the Danger!

- SSH Keys let an SSH Client in possession of a particular *private key* log in to an SSH Server authorizing the corresponding *public key*.
  - Protect the *private key* with a *long* passphrase.
  - Minimize the number and copies of *private keys*.
  - Use *ssh-agent* instead of storing *private keys* on remote machines.
  - Use *sk-* or *FIDO2-bound* or *hardware-bound* SSH Keys.

- Some individuals added their coworkers' public keys to their account.
  - <u>Don't do this.</u>
  - Do consult with the CI's User Support to solve your access challenges.

StyleGAN2 (Karras et al.)

Coming Up…

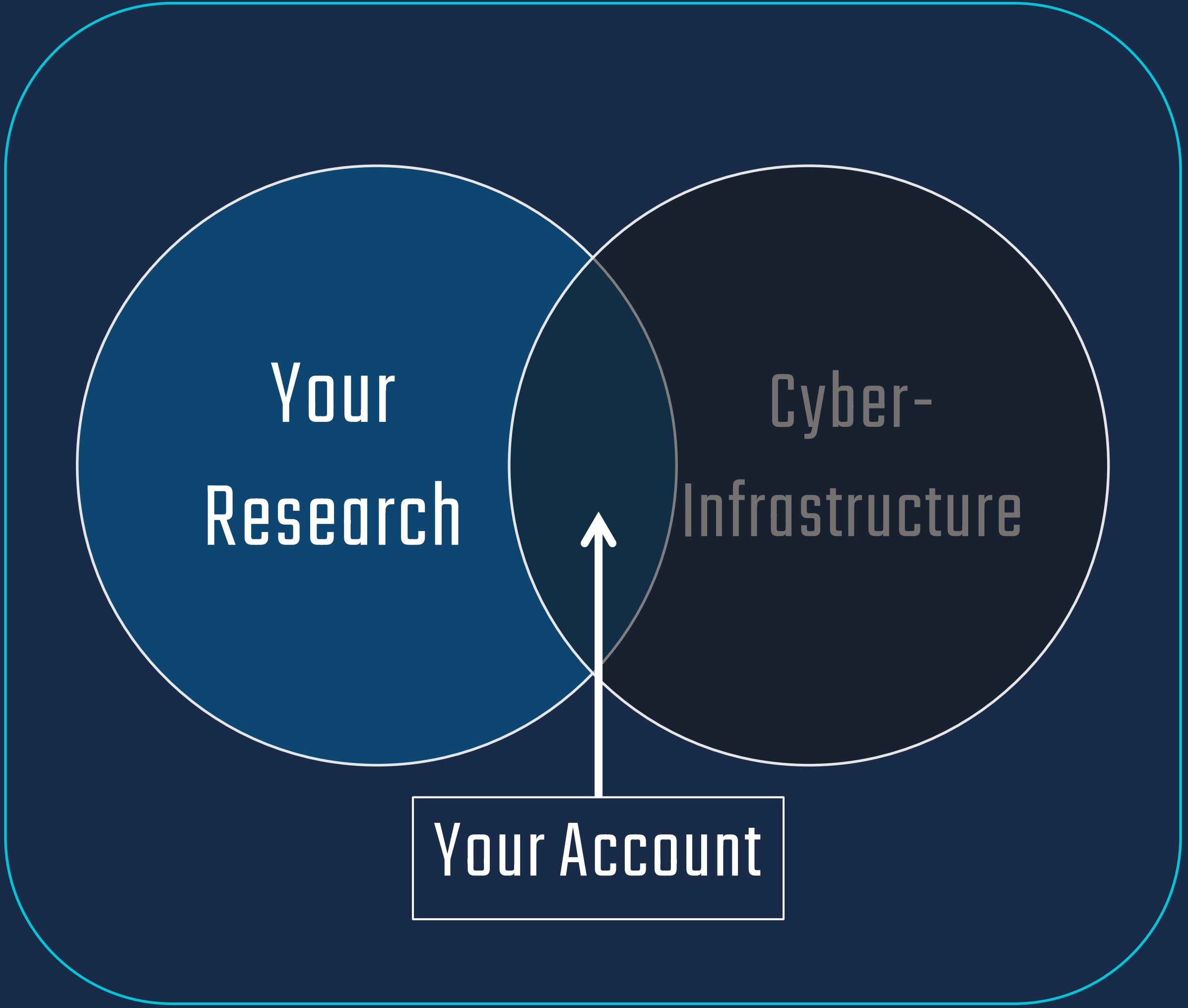
- M is a senior staff member working on a grant proposal.
- She logged in to edit the document.
- Here’s what happened to her account.

Looking Out For Danger

A Critical Component of Security: You

- "What are we protecting?"
- "What are we protecting it from?"

- CI Operators address most of the dangers to the CI.
- But what about your research and your account?



Your Likely Areas of Concern

Where Do I Start?

Let's start at the very ~~beginning~~ end

- Think *Dangerously!*
- Forget about “Will it happen?” for a moment.
- *Imagine* Danger: “What if a danger manifests?”
  - Does it even matter?
  - If it does, how am I affected?
- Who knows the consequences to a particular danger?
- You’re in the best position to know
  - It’s your research
  - It’s your code
  - It’s your data

Dangers to Your Account

- The CI Operator wants only you to have access to your account.
  - Imagine danger: Someone else gets access to your account.
  - Likely consequences: Your account is locked, your research is destroyed…
- “Can <this> help someone else access my account?”

- Some areas of focus:
  - Does it facilitate credential theft?
    - On-disk storage without encryption: Passwords, private keys, API keys…
  - Does it contain or help install malware?
    - Untrusted code, supply-chain, cut-and-paste commands…
  - Does it let you bypass the CI Operator’s log-in process?
    - Jupyter, Globus Connect Personal, VSCode…

Dangers to Your Account: cont.

Tools for addressing general dangers to your account

- Multi-factor authentication
  - (…or at least minimize password-only authentication)
- CI-provided tools for common tasks.
  - (Globus Managed Endpoint, *satellite* reverse-proxy, Science Gateways, *modules*, *singularity* images)
- Minimize dependencies / Favor codes with fewer dependencies.
  - (Leverage CI-provided libraries if feasible)
- Obtain code and data from trustworthy sources.
- Avoid storing passwords and password-equivalents on shared CI.

Dangers to Your Research

Can be framed in C-I-A triad.

- **Confidentiality**: The research is or contains components that must be kept secret.
- **Integrity**: The research is or contains components that must be authentic and free from corruption.
- **Availability**: The research is or contains components that must be available for use.

Requires knowledge of the use-case or workflow. (You!)

Dangers to Your Research: cont.

Some areas of focus

- What if someone else can view/change/delete my data/programs?
- What if my data/program is altered/corrupted?
  - How would I know if it was?
- What if my research is lost or corrupted?
- Is the data or software covered by a DUA, legal statute, or institutional policy? What does it say?

Dangers to Your Research: cont.

Tools for General C-I-A challenges

- Confidentiality: Encryption. (and minimalization!)
  - (GnuPG, gocryptfs, application-dependent)
- Integrity: Cryptographic Digest (“hashing”) / Signing / Checksums.
  - (sha256sum, GnuPG, S/MIME)
- Availability: Backups, redundant services, multiple copies.
  - (rsync, Globus Connect, git, AWS S3)

Case Study

Gone Phishin’

StyleGAN2 (Karras et al.)

Gone Phishin'

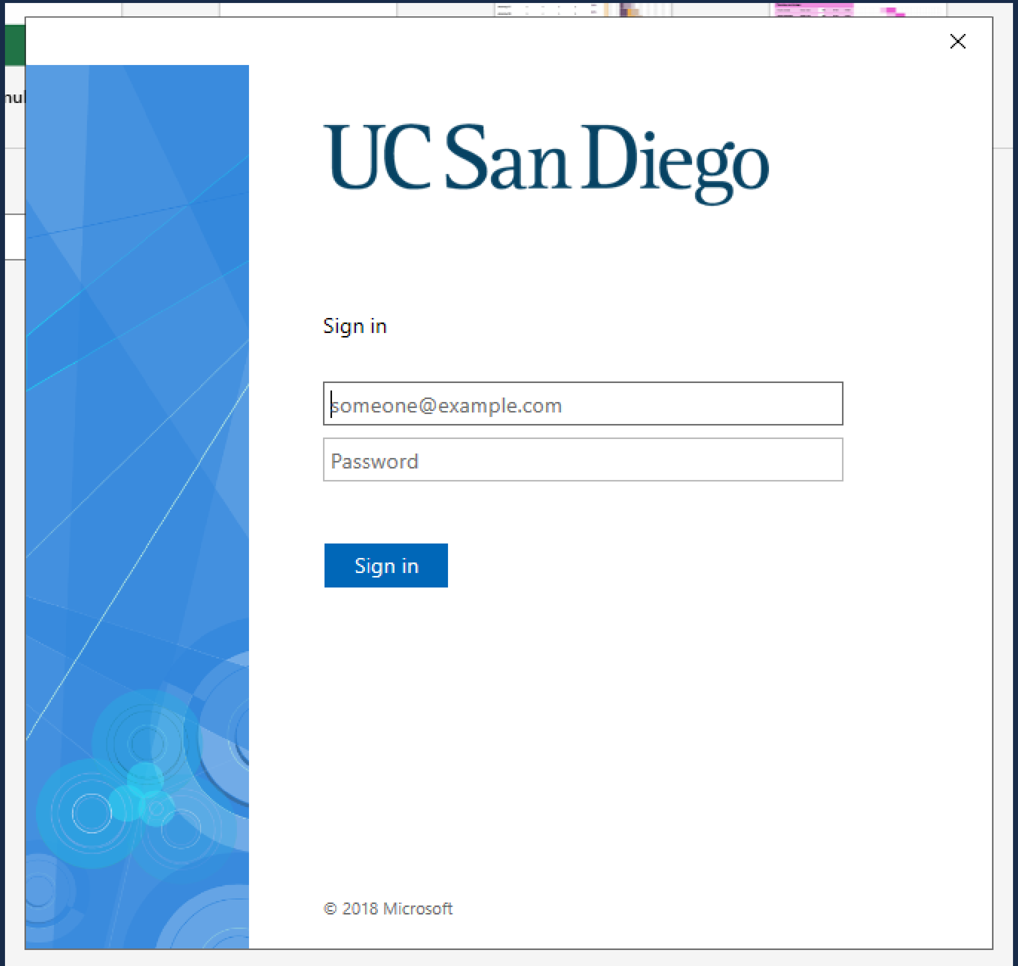
- Account locked!
- Unable to check email.
- Unable to work on proposal.

- Lost two days due to initial incident-response and clean-up.
- Spent much of the week changing passwords out of caution.

Advanced Phishing

Looks Normal Even If It's Not

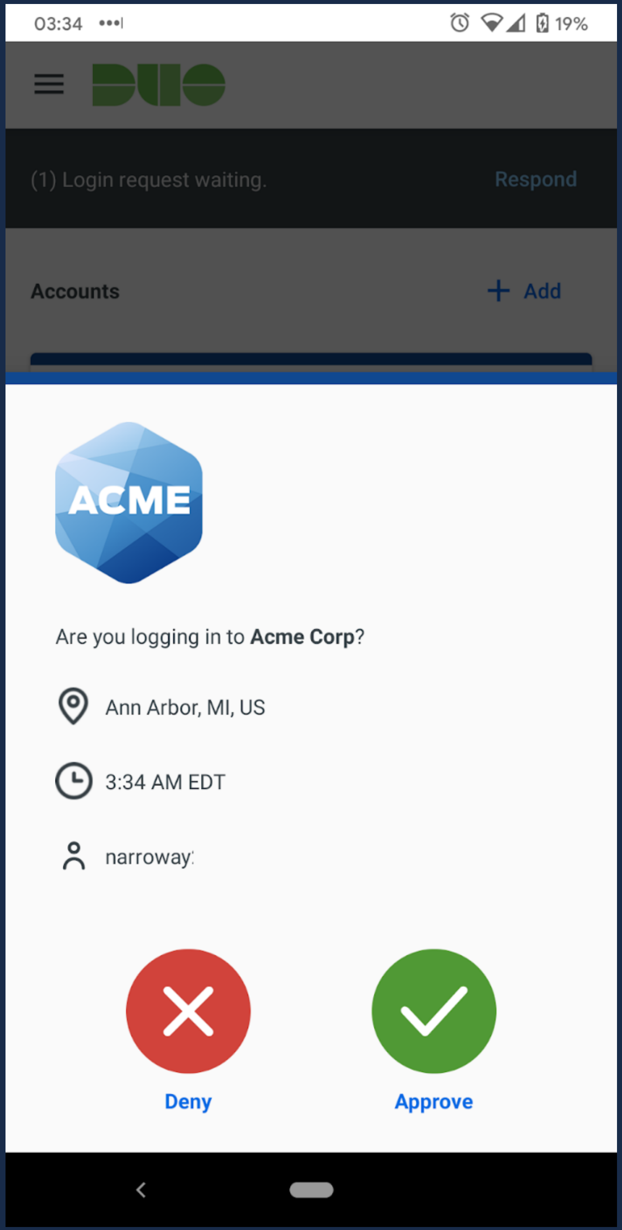
- Prompted to log in.
- Entered username and password.



Advanced Phishing

DUO to the Rescue?

- Got a DUO Push



(1) Login request waiting.

Are you logging in to **Acme Corp**?

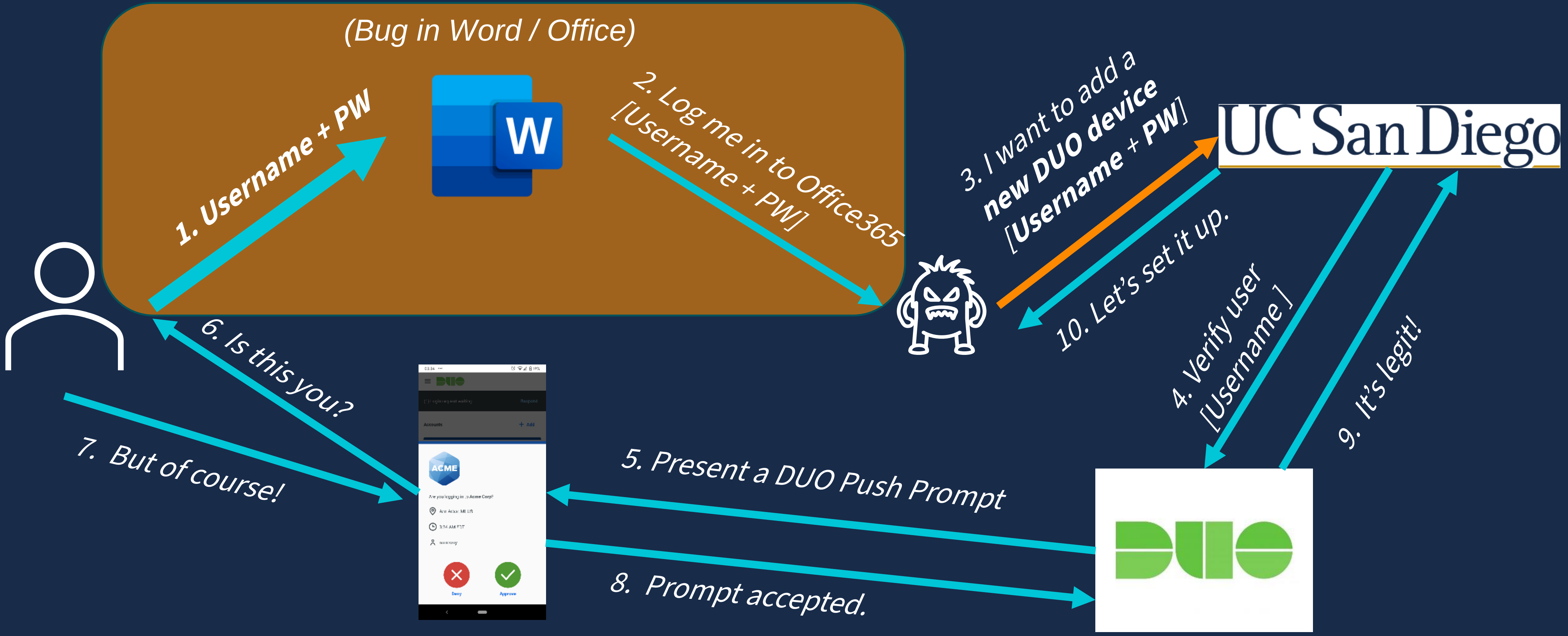
Ann Arbor, MI, US

3:34 AM EDT

narroway:

Advanced Phishing

How Could This Be?



(Bug in Word / Office)

1. Username + PW

2. Log me in to Office365 [Username + PW]

3. I want to add a **new DUO device** **[Username** + PW]

4. Verify user [Username]

5. Present a DUO Push Prompt

6. Is this you?

7. But of course!

8. Prompt accepted.

9. It's legit!

10. Let's set it up.

Advanced Phishing

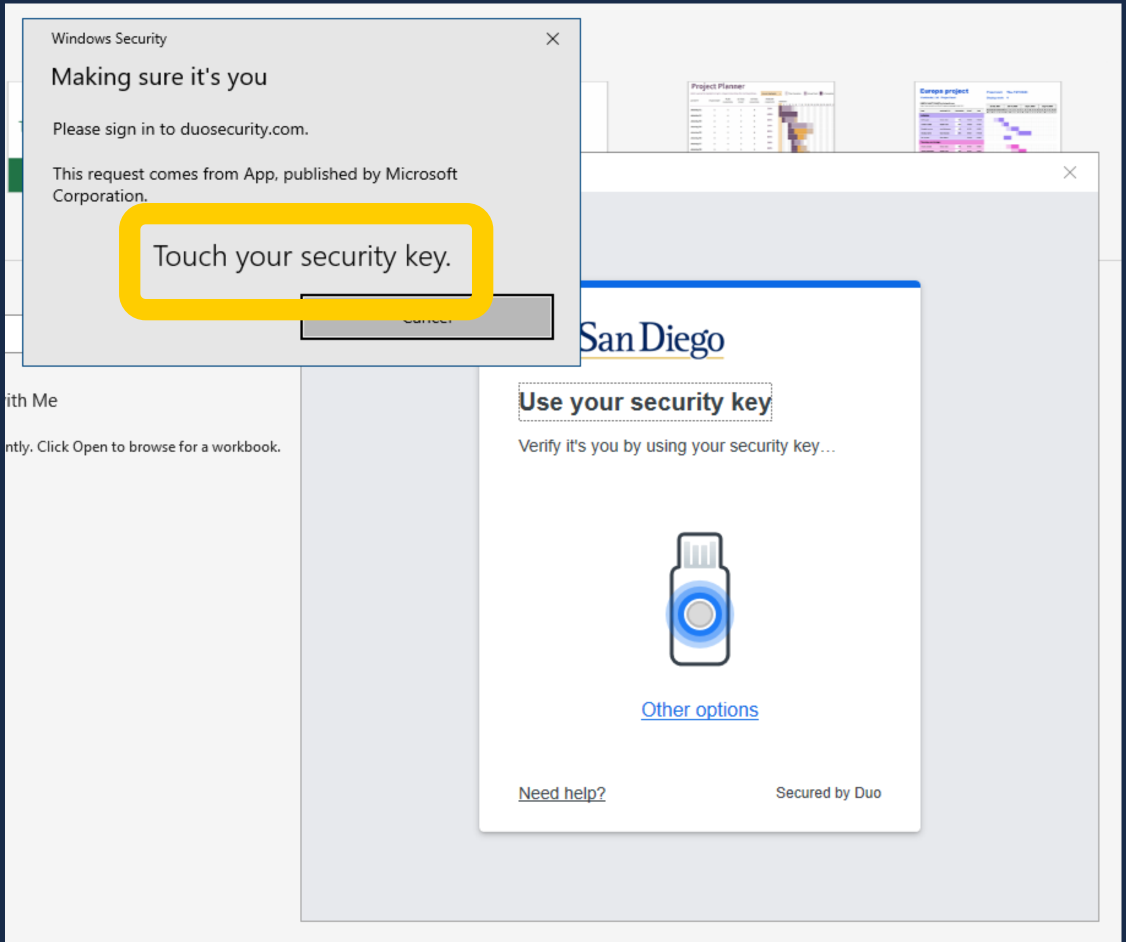
The Take-away

- **You can do everything right and still suffer.**
- Don’t blame yourself!
  - Expect to be treated respectfully by IT and security personnel.
- **Nothing is bullet-proof.**

- A contingency plan is important.
  - Sometimes all you can do is scream into a pillow.

Shameless Plug

FIDO2 the Rescue!



Windows Security

Making sure it's you

Please sign in to duosecurity.com.

This request comes from App, published by Microsoft Corporation.

Touch your security key.

Use your security key

Verify it's you by using your security key…

- Hardened hardware device.
  - Inexpensive (~20 USD).
  - Designed to prevent cloning.
- Phishing resistant.
  - A unique key for each URL.
  - M's login attempt would have failed, preventing the attack.
- Works with SSH.
  - (Newer client and server required)
- Also works with
  - DUO, Amazon, Google, Github…

Thank You!

Questions?

Scott Sakai <ssakai@sdsc.edu>