Authentication & Authorization

Patch notes

Homework 1: Due tonight at midnight

- For folks running into issues:
  - FAQ on Slack
  - Different environments have caused issues:
    Submissions will be manually reviewed if necessary
- Feedback is always welcome:
  https://forms.gle/Xxi4JL25Vqg7U1pT8

Patch notes

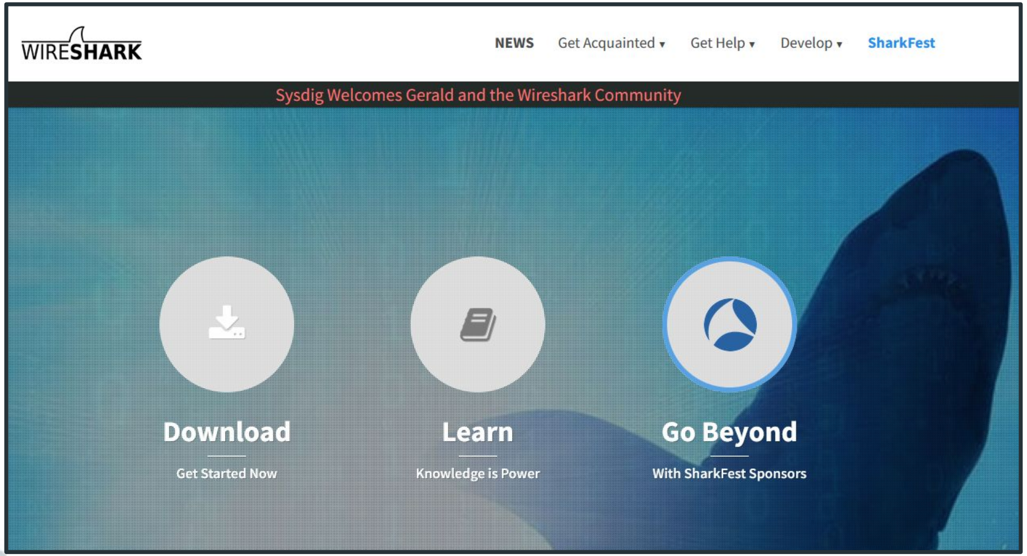
Deadline philosophy:

Deadlines are for your benefit, not mine. Doing something late is better than not doing it at all.

Patch notes

Download **Wireshark** in advance of recitation tomorrow:

https://www.wireshark.org/#download



AuthN & AuthZ

Authentication (AuthN): Proving *who* a party is

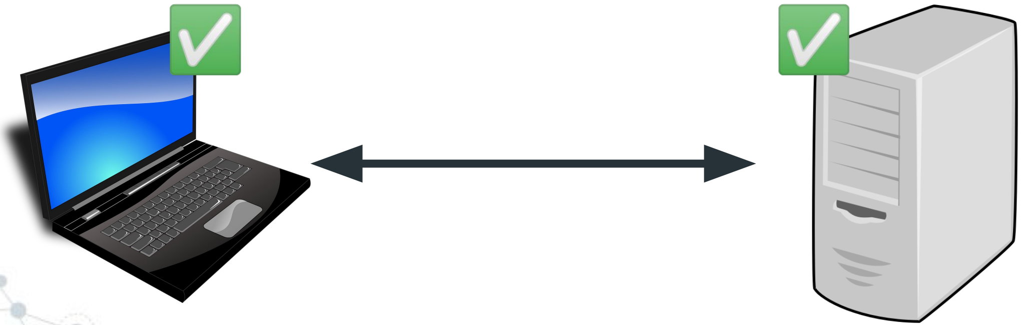
Authorization (AuthZ): Proving *what* a party is allowed to do

Auth: Umbrella term for both

Authentication (AuthN)

Authentication: Proves *who* both parties are

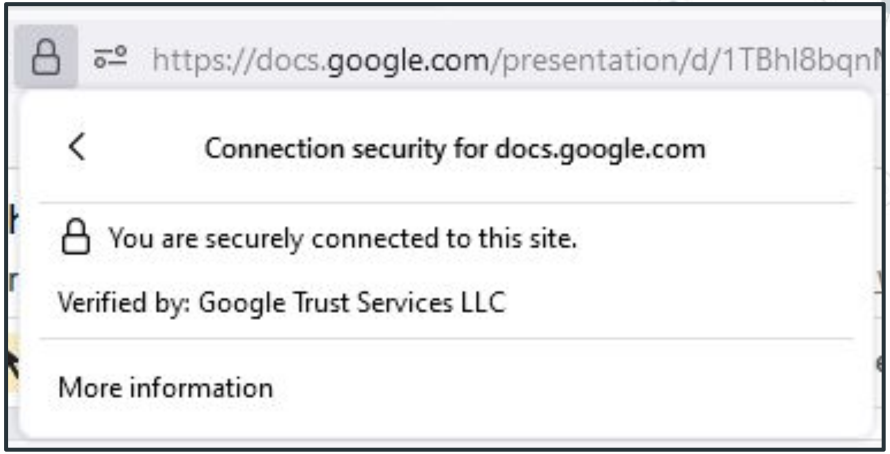
- Based on some kind of shared secret
- Common examples: Passwords, public keys



Authentication (AuthN)

Server authentication:

- Public Key Infrastructure



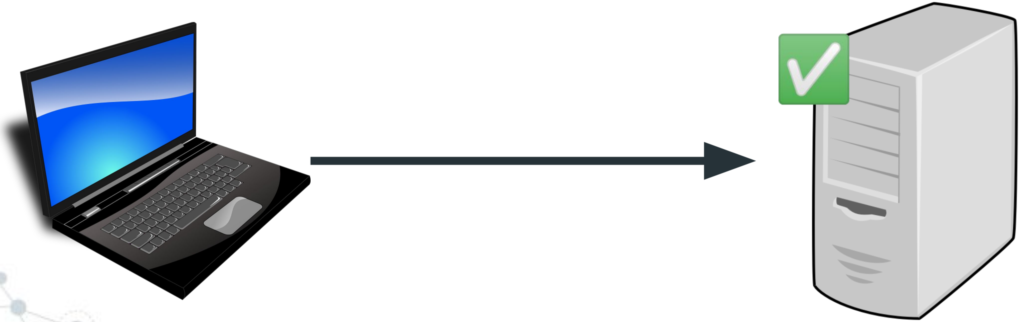
https://docs.google.com/presentation/d/1TBhl8bqn

Connection security for docs.google.com

You are securely connected to this site.

Verified by: Google Trust Services LLC

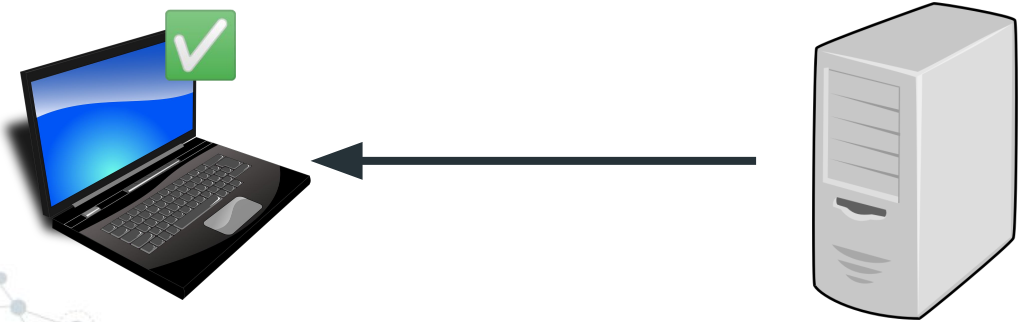
More information



Authentication (AuthN)

Client AuthN methods:

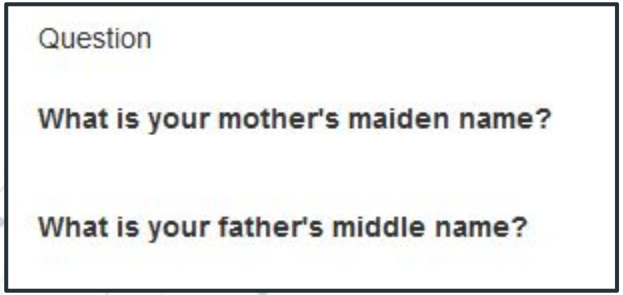
- Something only you *know*
- Something only you *have*
- Something only you *are*



Authentication (AuthN)

Something you *know*

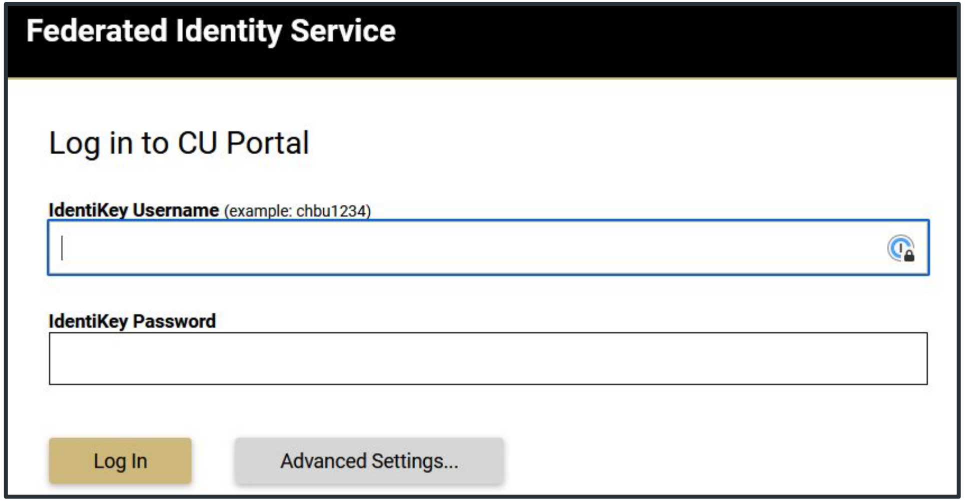
- Password
- Security question
- Birthday
- SSN



Question

What is your mother's maiden name?

What is your father's middle name?



Federated Identity Service

Log in to CU Portal

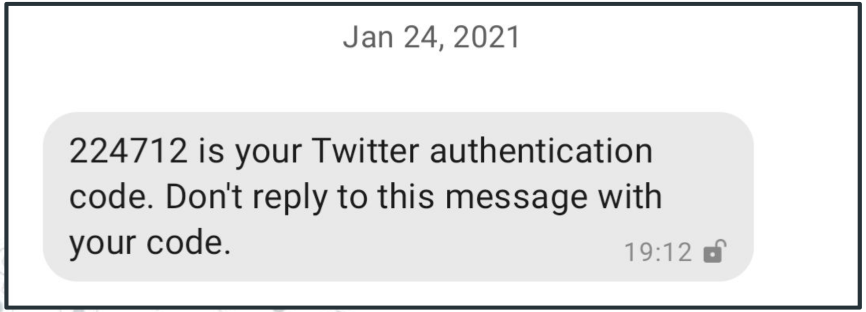
IdentiKey Username (example: chbu1234)

IdentiKey Password

Authentication (AuthN)

Something you *have*

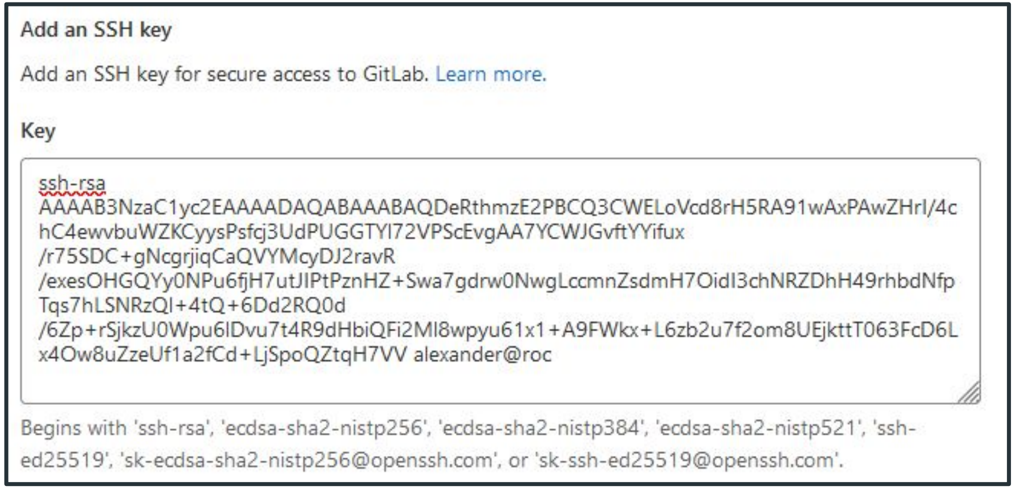
- Phone number
- Email access
- Private key



Jan 24, 2021

224712 is your Twitter authentication code. Don't reply to this message with your code.

19:12



Add an SSH key

Add an SSH key for secure access to GitLab. Learn more.

Key

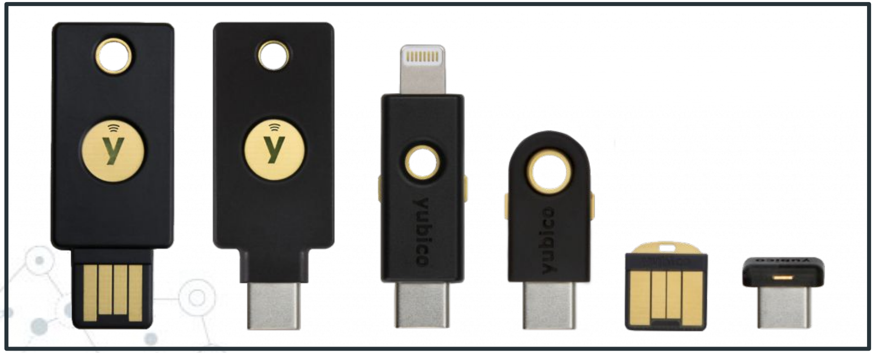
```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDeRthmzE2PBCQ3CWELoVcd8rH5RA91wAxPAwZHrl/4c
hC4ewvbuWZKCyysPsfcj3UdPUGGTYl72VPScEvgAA7YCWJGvftYYifux
/r75SDC+gNcgrjiqCaQVYMcyDJ2ravR
/exesOHGQYy0NPu6fjH7utJIPtPznHZ+Swa7gdrw0NwgLccmnZsdmH7OidI3chNRZDhH49rhbdNfp
Tqs7hLSNRzQl+4tQ+6Dd2RQ0d
/6Zp+rSjkzU0Wpu6lDvu7t4R9dHbiQFi2Ml8wpyu61x1+A9FWkx+L6zb2u7f2om8UEjktT063FcD6L
x4Ow8uZzeUf1a2fCd+LjSpoQZtqH7VV alexander@roc
```

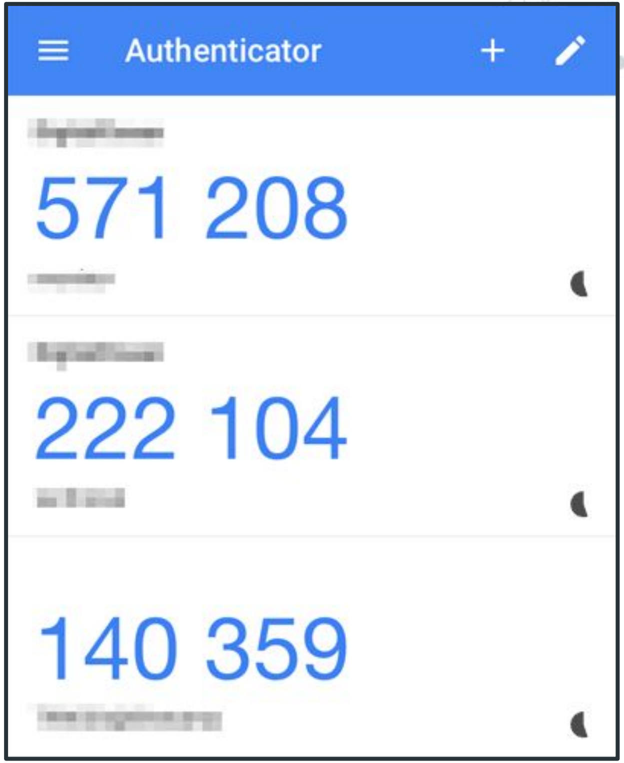
Begins with 'ssh-rsa', 'ecdsa-sha2-nistp256', 'ecdsa-sha2-nistp384', 'ecdsa-sha2-nistp521', 'ssh-ed25519', 'sk-ecdsa-sha2-nistp256@openssh.com', or 'sk-ssh-ed25519@openssh.com'.

Authentication (AuthN)

Private key storage mechanisms:

- Authenticator Apps
- YubiKeys
- Some phones





Authenticator

[redacted]

571 208

[redacted]

[redacted]

222 104

[redacted]

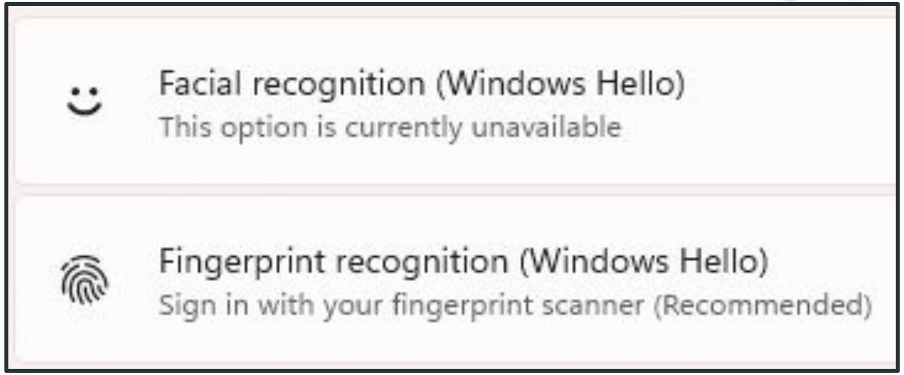
140 359

[redacted]

Authentication (AuthN)

Something you *are*

- Fingerprint
- Face recognition



Facial recognition (Windows Hello)
This option is currently unavailable

Fingerprint recognition (Windows Hello)
Sign in with your fingerprint scanner (Recommended)

Authentication (AuthN)

Different methods have different threat models!

Examples:

- **Passwords**: Brute-forcing
- **YubiKey**: Physical theft
- **Facial recognition**: Finding photos online

Authentication (AuthN)

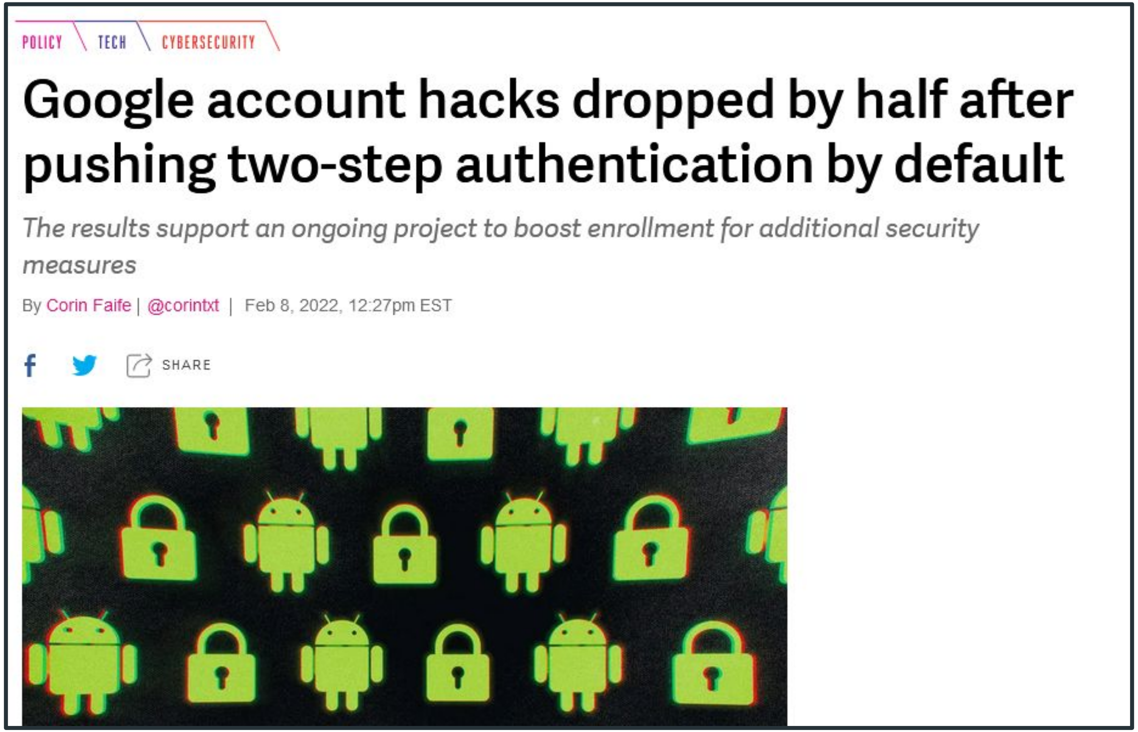
Multi-factor Authentication (MFA): Using more than one authentication method

(Also referred to as Two-factor Authentication, or 2FA)

+ Strictly improves security

− Increases risk of availability loss

Authentication (AuthN)



Google account hacks dropped by half after pushing two-step authentication by default

The results support an ongoing project to boost enrollment for additional security measures

By Corin Faife | @corintxt | Feb 8, 2022, 12:27pm EST

https://www.theverge.com/2022/2/8/22923618/google-account-hacks-dropped-half-two-step-authentication

Authentication (AuthN)

Authentication methods should be different types!

✅Password + Phone code
❌Password + Security Question
❌Phone code + email code

Authentication (AuthN)

Recovery Methods: Allows a user to login using multiple AuthN methods

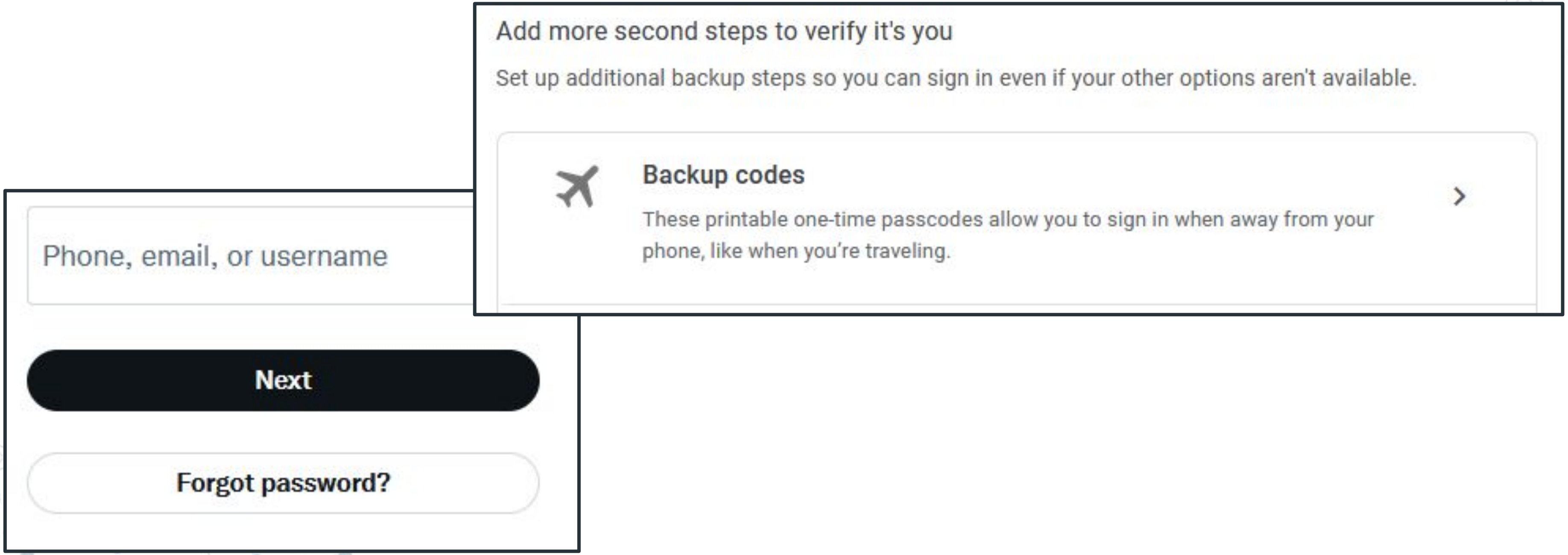
– Strictly decreases security

+ Reduces risk of availability loss

AuthN becomes as strong as the weakest method!

Authentication (AuthN)

Intended uses of recovery codes:



Add more second steps to verify it's you

Set up additional backup steps so you can sign in even if your other options aren't available.

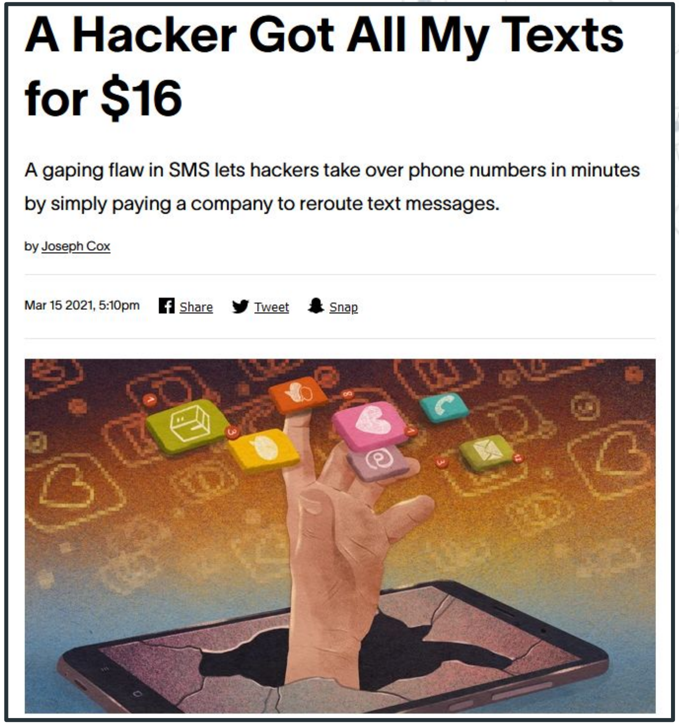
Backup codes

These printable one-time passcodes allow you to sign in when away from your phone, like when you're traveling.

Authentication (AuthN)

SMS spoofing: Intercepting SMS-based auth codes

- Ordering new SIM cards (SIM Swapping)
- Bribing telecom providers
- Bugs in text-based middleware



A Hacker Got All My Texts for $16

A gaping flaw in SMS lets hackers take over phone numbers in minutes by simply paying a company to reroute text messages.

by Joseph Cox

Mar 15 2021, 5:10pm

https://www.vice.com/amp/en/article/y3g8wb/hacker-got-my-texts-16-dollars-sakari-netnumber

Authentication (AuthN)

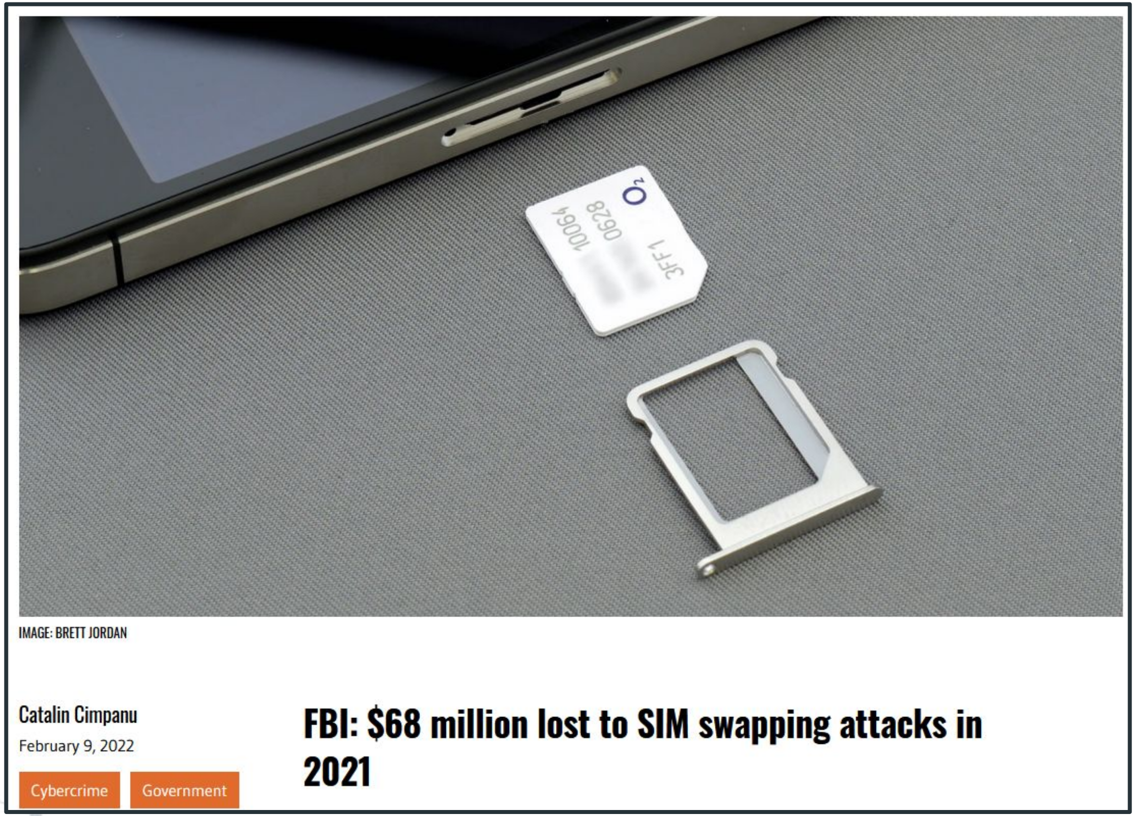


IMAGE: BRETT JORDAN

Catalin Cimpanu

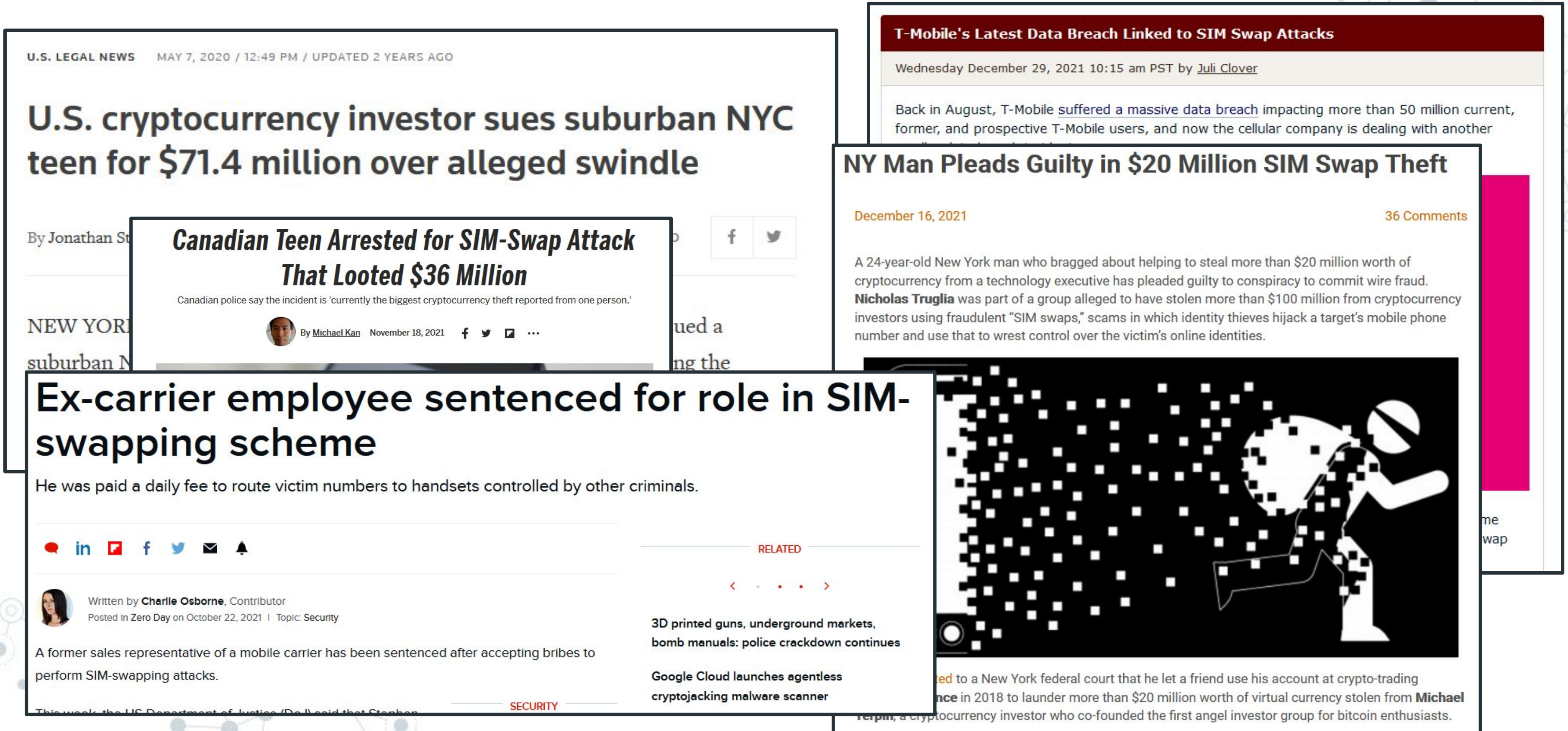
February 9, 2022

Cybercrime Government

FBI: $68 million lost to SIM swapping attacks in 2021

https://therecord.media/fbi-68-million-lost-to-sim-swapping-attacks-in-2021/

Authentication (AuthN)



U.S. LEGAL NEWS MAY 7, 2020 / 12:49 PM / UPDATED 2 YEARS AGO

U.S. cryptocurrency investor sues suburban NYC teen for $71.4 million over alleged swindle

By Jonathan St

NEW YORK ued a

suburban N ng the

Canadian Teen Arrested for SIM-Swap Attack That Looted $36 Million

Canadian police say the incident is 'currently the biggest cryptocurrency theft reported from one person.'

By Michael Kan November 18, 2021

Ex-carrier employee sentenced for role in SIM-swapping scheme

He was paid a daily fee to route victim numbers to handsets controlled by other criminals.

Written by **Charlie Osborne**, Contributor

Posted in Zero Day on October 22, 2021 | Topic: Security

A former sales representative of a mobile carrier has been sentenced after accepting bribes to perform SIM-swapping attacks.

SECURITY

This week, the US Department of Justice (DoJ) said that Stephen

RELATED

3D printed guns, underground markets, bomb manuals: police crackdown continues

Google Cloud launches agentless cryptojacking malware scanner

T-Mobile's Latest Data Breach Linked to SIM Swap Attacks

Wednesday December 29, 2021 10:15 am PST by Juli Clover

Back in August, T-Mobile suffered a massive data breach impacting more than 50 million current, former, and prospective T-Mobile users, and now the cellular company is dealing with another

me

wap

NY Man Pleads Guilty in $20 Million SIM Swap Theft

December 16, 2021 36 Comments

A 24-year-old New York man who bragged about helping to steal more than $20 million worth of cryptocurrency from a technology executive has pleaded guilty to conspiracy to commit wire fraud. **Nicholas Truglia** was part of a group alleged to have stolen more than $100 million from cryptocurrency investors using fraudulent "SIM swaps," scams in which identity thieves hijack a target's mobile phone number and use that to wrest control over the victim's online identities.

ted to a New York federal court that he let a friend use his account at crypto-trading **nce** in 2018 to launder more than $20 million worth of virtual currency stolen from **Michael Terpin**, a cryptocurrency investor who co-founded the first angel investor group for bitcoin enthusiasts.

Authentication (AuthN)

General advice*:

- Use **good passwords** with a **physical 2FA option**
- Use **backup** 2FA options to avoid getting locked out

- Avoid SMS auth methods if possible
- Avoid guessable security questions

***Will vary person to person**

Recap

Authentication (AuthN): Proves identity

- Things only you *know*
- Things only you *have*
- Things only you *are*

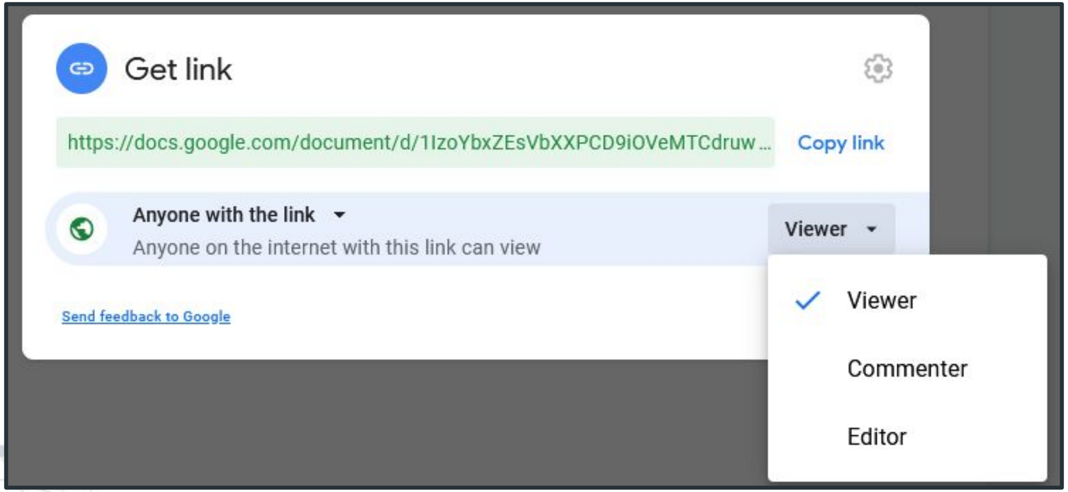
Multi-factor Authentication (MFA): Requiring multiple AuthN factors to log in

Recovery methods: Allowing one AuthN to bypass another

Authorization (AuthZ)

Authorization: Determining *what* a party is allowed to do

- Requires authentication
- Very implementation-specific



Get link

https://docs.google.com/document/d/1IzoYbxZEsVbXXPCD9iOVeMTCdruw...

Anyone with the link

Anyone on the internet with this link can view

Viewer

Authorization (AuthZ)

Common example: Linux file permissions

- Each file has an *owner* and a *group*
- Each file has read, write, and execute permissions for the *owner*, *group*, and *all*.

	Read	**Write**	**Execute**
Owner	✅	✅	✅
Group	✅	❌	✅
All	✅	❌	❌

Authorization (AuthZ)

Often represented like this:

```
$ ls -al
-rwxr-xr-- 1 alex alex 32 Jan 24 00:32 foo.txt
```

	Read	Write	Execute
Owner	✅	✅	✅
Group	✅	❌	✅
All	✅	❌	❌

Authorization (AuthZ)

Try it yourself:

```
$ echo 'Testing' > test.txt
$ cat test.txt
$ chmod goa-r test.txt # Remove read access
$ cat test.txt
```

Authorization (AuthZ)

Access Control Lists (ACLs): Lists that map users to the permissions they have

	View	Edit	Delete
Bob	✅	✅	✅
Alice	✅	❌	❌
Carol	✅	✅	✅
Eve	❌	❌	❌

Authorization (AuthZ)

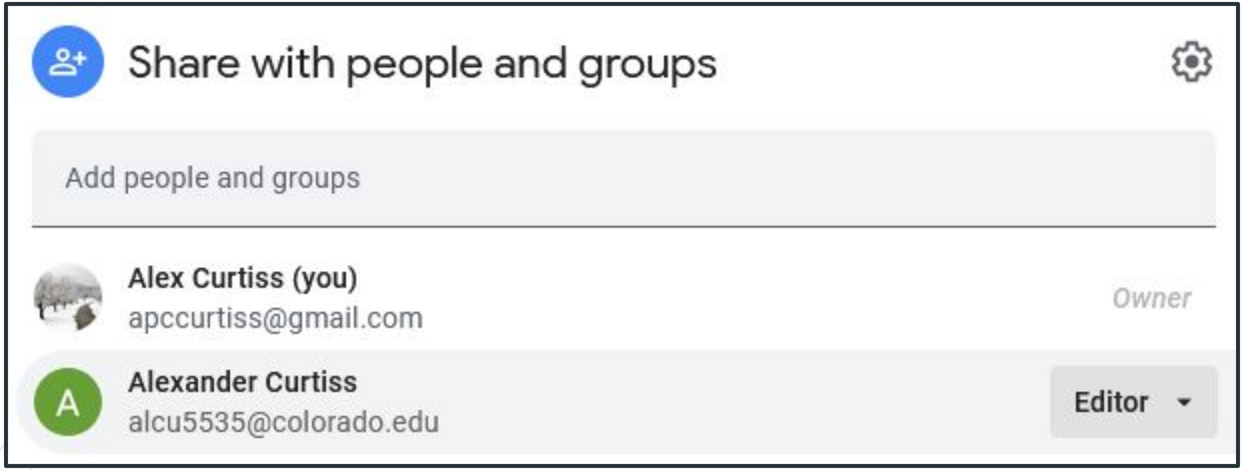
Access Control Lists (ACLs): Lists that map users to the permissions they have

- Problem: Does not scale well with 1000s of users

	View	Edit	Delete
Bob	✅	✅	✅
Alice	✅	❌	❌
Carol	✅	✅	✅
Eve	❌	❌	❌

Authorization (AuthZ)

ACL example



Share with people and groups

Add people and groups

Alex Curtiss (you)
apccurtiss@gmail.com
Owner

Alexander Curtiss
alcu5535@colorado.edu
Editor

Authorization (AuthZ)

Role-based Access Control (RBAC): Lists that map groups of users to the permissions they have

	Roles
Bob	[Admin]
Alice	[Mod]
Carol	[Mod, Editor]
Eve	[Guest]

	View	Edit	Delete
Admin	✅	✅	✅
Mod	✅	❌	✅
Editor	✅	✅	❌
Guest	✅	❌	❌

Authorization (AuthZ)

Role-based Access Control (RBAC): Lists that map groups of users to the permissions they have

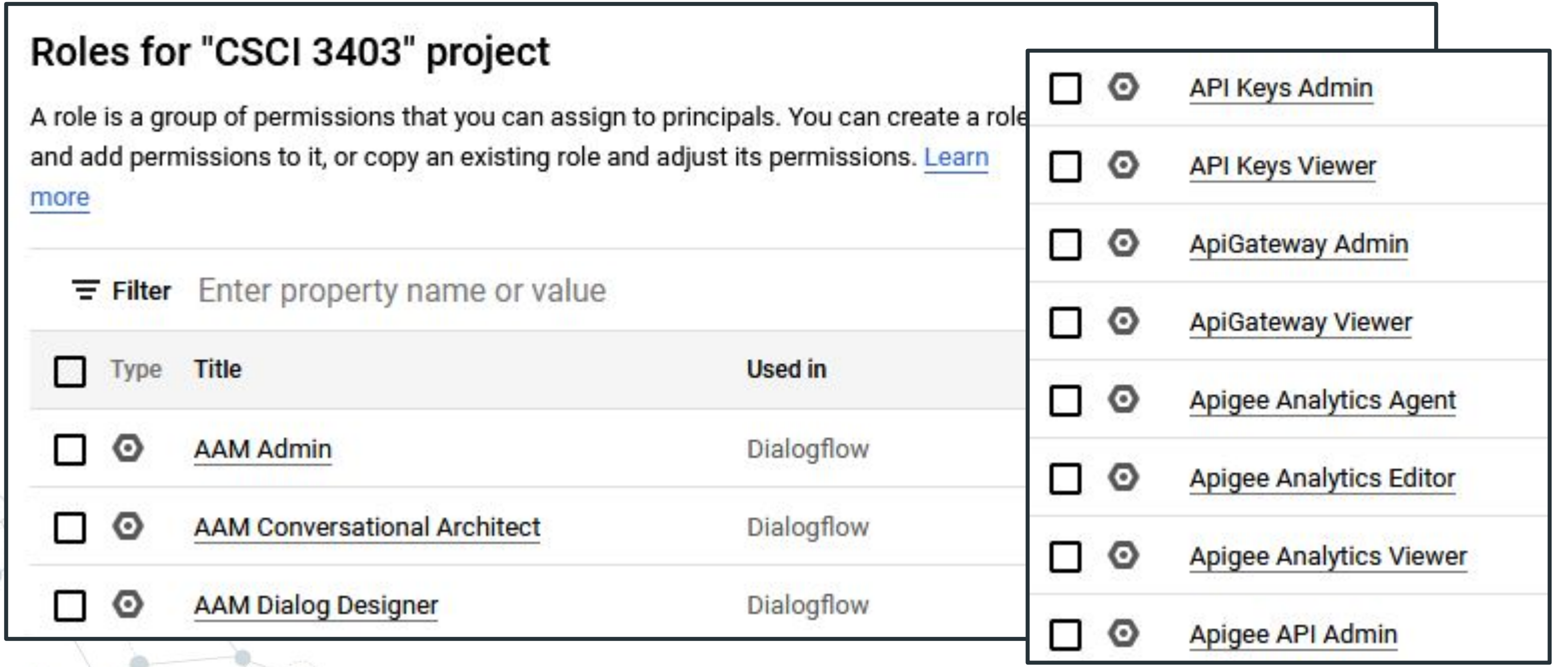
- Scales better, although scaling is still an issue

	Roles
Bob	[Admin]
Alice	[Mod]
Carol	[Mod, Editor]
Eve	[Guest]

	View	Edit	Delete
Admin	✅	✅	✅
Mod	✅	❌	✅
Editor	✅	✅	❌
Guest	✅	❌	❌

Authorization (AuthZ)

RBAC example:



Roles for "CSCI 3403" project

A role is a group of permissions that you can assign to principals. You can create a role and add permissions to it, or copy an existing role and adjust its permissions. Learn more

Filter Enter property name or value

□	Type	Title	Used in
□	⊙	AAM Admin	Dialogflow
□	⊙	AAM Conversational Architect	Dialogflow
□	⊙	AAM Dialog Designer	Dialogflow

□	⊙	API Keys Admin
□	⊙	API Keys Viewer
□	⊙	ApiGateway Admin
□	⊙	ApiGateway Viewer
□	⊙	Apigee Analytics Agent
□	⊙	Apigee Analytics Editor
□	⊙	Apigee Analytics Viewer
□	⊙	Apigee API Admin

Recap

Vocab:

Authorization: Whether or not a user has permission to perform an action

Access Control List (ACL): Maps users to permissions.

Role-based Access Control (RBAC): Maps user roles to permissions. Requires a map of users to roles.

AuthZ: Day 2

Patch Notes

- Homework #2 (Network Lab) will be released some time this weekend

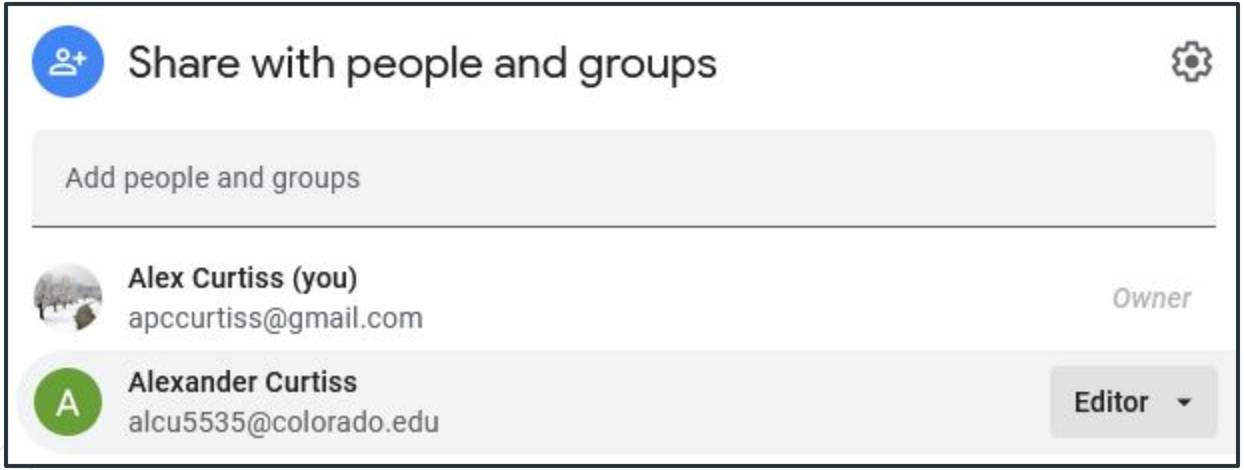
Patch Notes

Clearer late policy guidelines:

- Late work will still be accepted for full credit
- We will not spend time on overdue assignments (unless you reached out in advance)
- This policy can change at any time

Recap

Authorization: Whether or not a user has permission to perform an action



Share with people and groups

Add people and groups

Alex Curtiss (you)
apccurtiss@gmail.com
Owner

Alexander Curtiss
alcu5535@colorado.edu
Editor

Authorization (AuthZ)

Access Control Lists (ACLs): Lists that map users to the permissions they have

- Problem: Does not scale well with 1000s of users

	View	Edit	Delete
Bob	✅	✅	✅
Alice	✅	❌	❌
Carol	✅	✅	✅
Eve	❌	❌	❌

Authorization (AuthZ)

Role-based Access Control (RBAC): Lists that map groups of users to the permissions they have

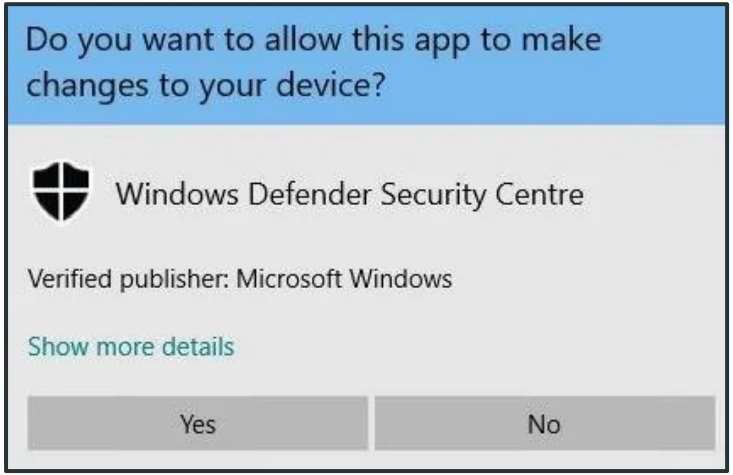
- Scales better, although scaling is still an issue

	Roles
Bob	[Admin]
Alice	[Mod]
Carol	[Mod, Editor]
Eve	[Guest]

	View	Edit	Delete
Admin	✅	✅	✅
Mod	✅	❌	✅
Editor	✅	✅	❌
Guest	✅	❌	❌

Authorization (AuthZ)

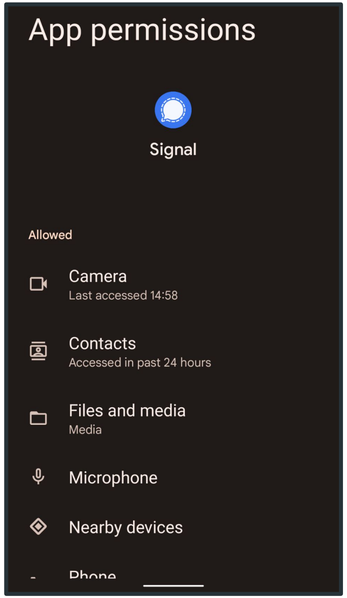
Problem 1: Permission controls can have different levels of detail.



Do you want to allow this app to make changes to your device?

Windows Defender Security Centre

Verified publisher: Microsoft Windows



App permissions

Signal

Allowed

Camera
Last accessed 14:58

Contacts
Accessed in past 24 hours

Files and media
Media

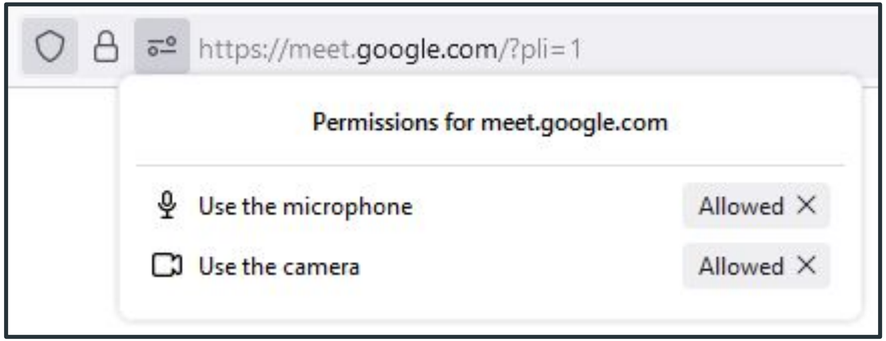
Microphone

Nearby devices

Phone

Authorization (AuthZ)

Good levels of detail: Phones, browsers, etc.

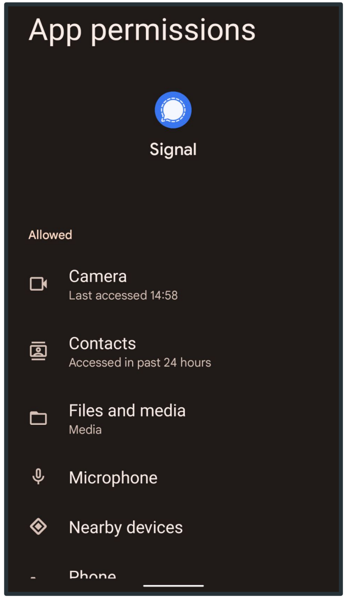


https://meet.google.com/?pli=1

Permissions for meet.google.com

Use the microphone — Allowed ✕

Use the camera — Allowed ✕



App permissions

Signal

Allowed

Camera
Last accessed 14:58

Contacts
Accessed in past 24 hours

Files and media
Media

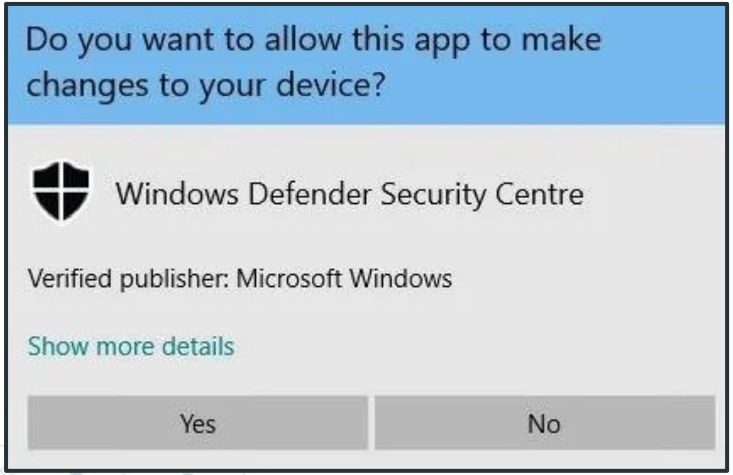
Microphone

Nearby devices

Phone

Authorization (AuthZ)

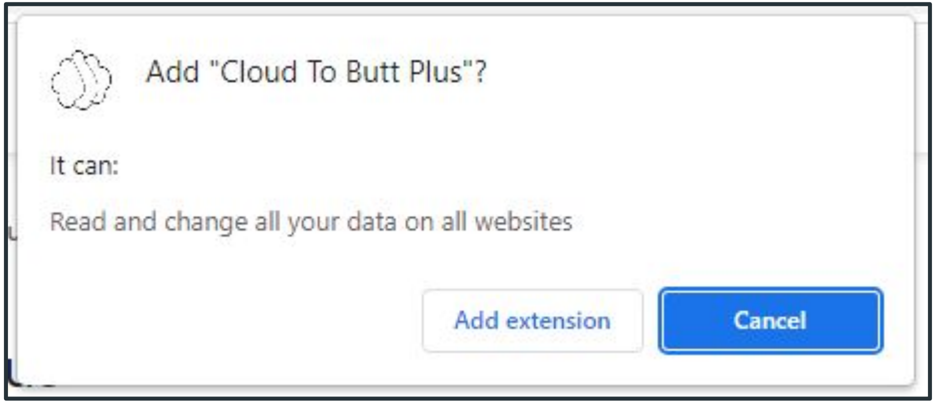
Not detailed enough: Broad permissions can be abused in unexpected ways



Do you want to allow this app to make changes to your device?

Windows Defender Security Centre

Verified publisher: Microsoft Windows



Add "Cloud To Butt Plus"?

It can:

Read and change all your data on all websites

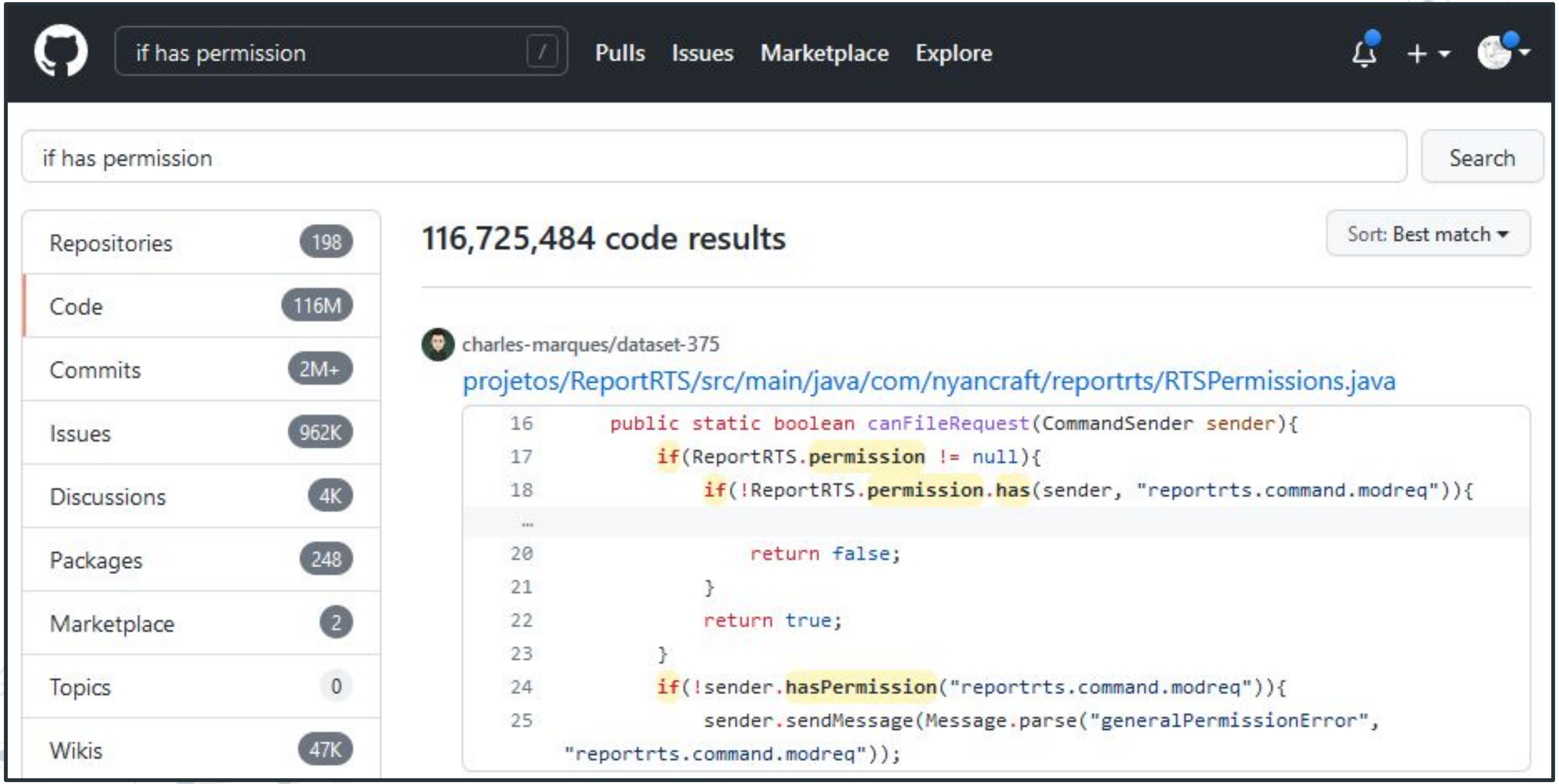
Authorization (AuthZ)

Problem 2: There is no standard tool for these.

Most boil down to a conditional somewhere, and code is always broken.

```
if action == 'edit' and not edit_permitted:
    raise Forbidden('You do not have edit permission.')
```

Authorization (AuthZ)



if has permission

Repositories	198
Code	116M
Commits	2M+
Issues	962K
Discussions	4K
Packages	248
Marketplace	2
Topics	0
Wikis	47K

116,725,484 code results

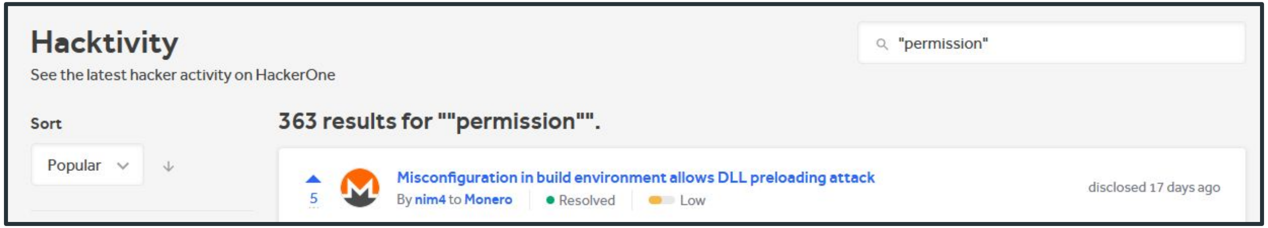
charles-marques/dataset-375

projetos/ReportRTS/src/main/java/com/nyancraft/reportrts/RTSPermissions.java

```
    public static boolean canFileRequest(CommandSender sender){
        if(ReportRTS.permission != null){
            if(!ReportRTS.permission.has(sender, "reportrts.command.modreq")){
…
                return false;
            }
            return true;
        }
        if(!sender.hasPermission("reportrts.command.modreq")){
            sender.sendMessage(Message.parse("generalPermissionError",
"reportrts.command.modreq"));
```

Authorization (AuthZ)

https://hackerone.com/hacktivity?querystring="permission"



Hacktivity

See the latest hacker activity on HackerOne

"permission"

Sort

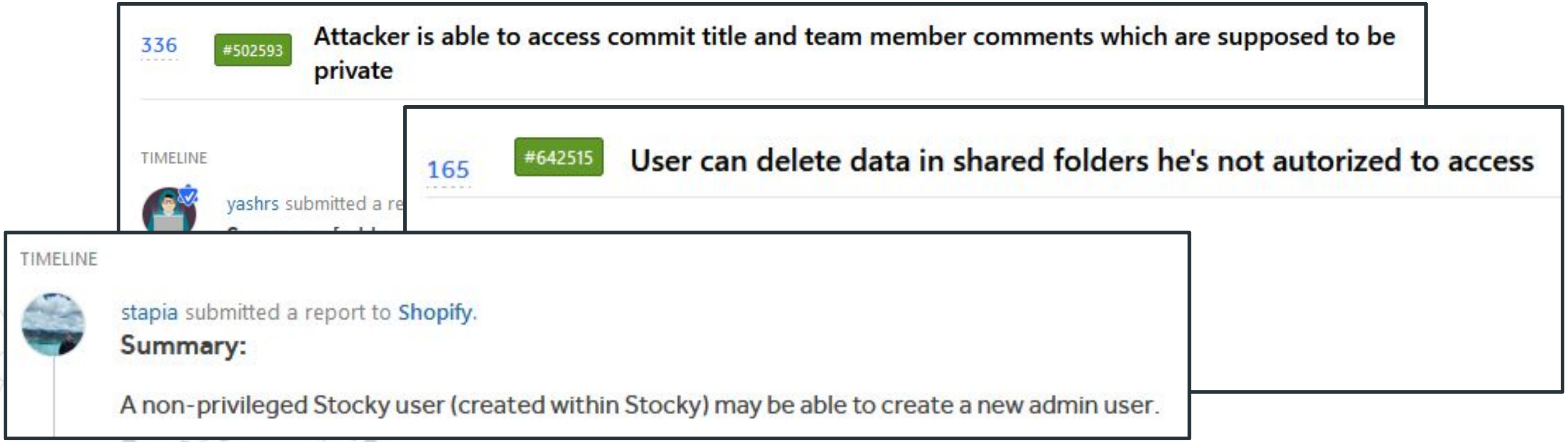
Popular

363 results for ""permission"".

5 Misconfiguration in build environment allows DLL preloading attack

By nim4 to Monero ● Resolved Low

disclosed 17 days ago



336 #502593 Attacker is able to access commit title and team member comments which are supposed to be private

TIMELINE

yashrs submitted a re

165 #642515 User can delete data in shared folders he's not autorized to access

TIMELINE

stapia submitted a report to Shopify.

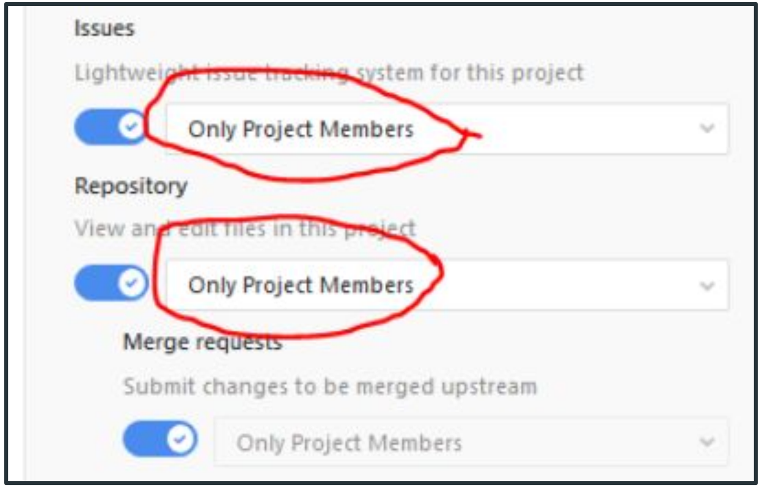
Summary:

A non-privileged Stocky user (created within Stocky) may be able to create a new admin user.

Authorization (AuthZ)

Deep dive: https://hackerone.com/reports/502593

Expected: Commit messages and discussion should only be visible to project members



Issues

Lightweight issue tracking system for this project

Only Project Members

Repository

View and edit files in this project

Only Project Members

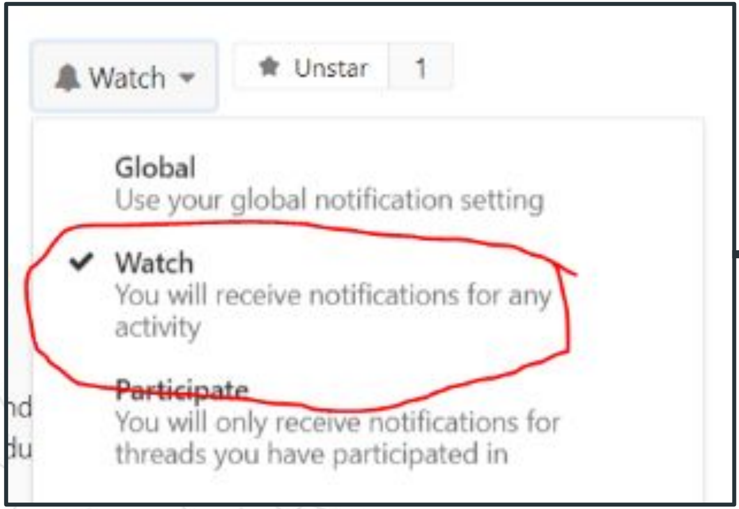
Merge requests

Submit changes to be merged upstream

Only Project Members

Authorization (AuthZ)

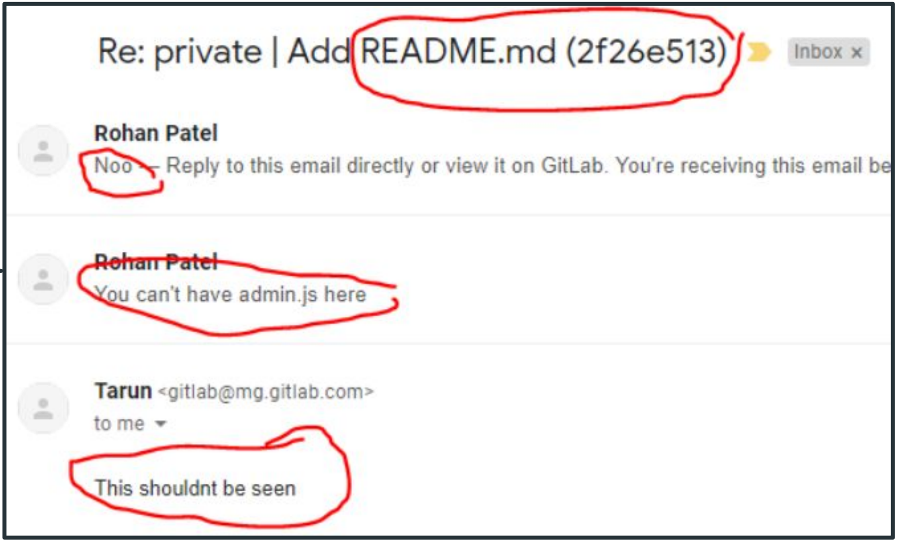
Actual: Control affects the UI, but not email notifications!



Global
Use your global notification setting

✓ Watch
You will receive notifications for any activity

Participate
You will only receive notifications for threads you have participated in


Re: private | Add README.md (2f26e513)

Rohan Patel
Noo -- Reply to this email directly or view it on GitLab. You're receiving this email be

Rohan Patel
You can't have admin.js here

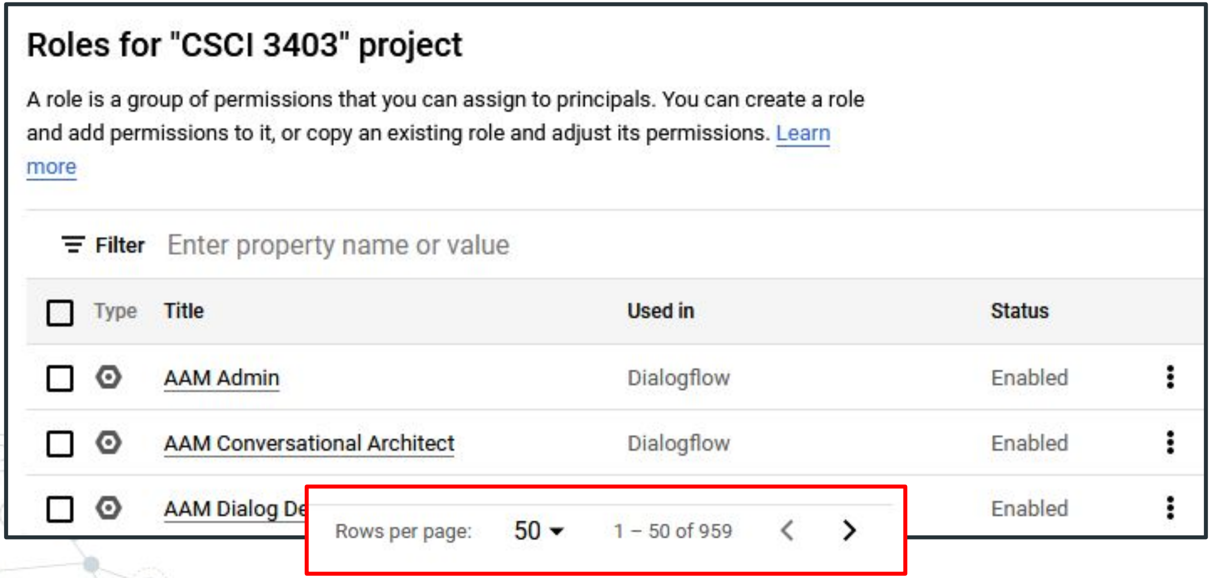
Tarun <gitlab@mg.gitlab.com>
to me ▾

This shouldnt be seen

Authorization (AuthZ)

Problem 3: Keeping lists updated is a lot of work!

- One misplaced control or file is all it takes!



Roles for "CSCI 3403" project

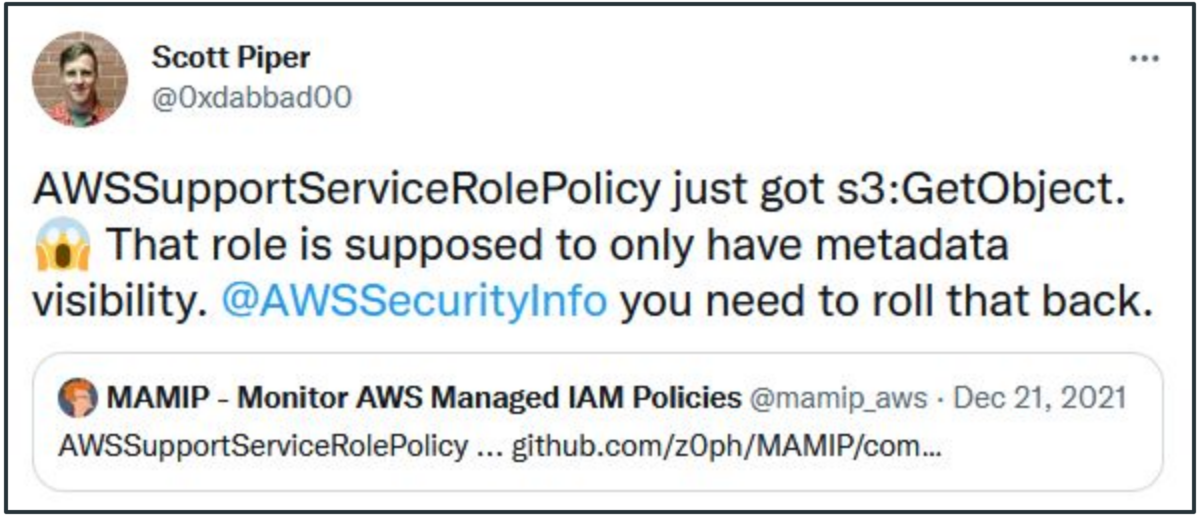
A role is a group of permissions that you can assign to principals. You can create a role and add permissions to it, or copy an existing role and adjust its permissions. Learn more

Filter Enter property name or value

□	Type	Title	Used in	Status	
□	⚙	AAM Admin	Dialogflow	Enabled	⋮
□	⚙	AAM Conversational Architect	Dialogflow	Enabled	⋮
□	⚙	AAM Dialog De		Enabled	⋮

Rows per page: 50 ▾ 1 – 50 of 959 ‹ ›

Authorization (AuthZ)



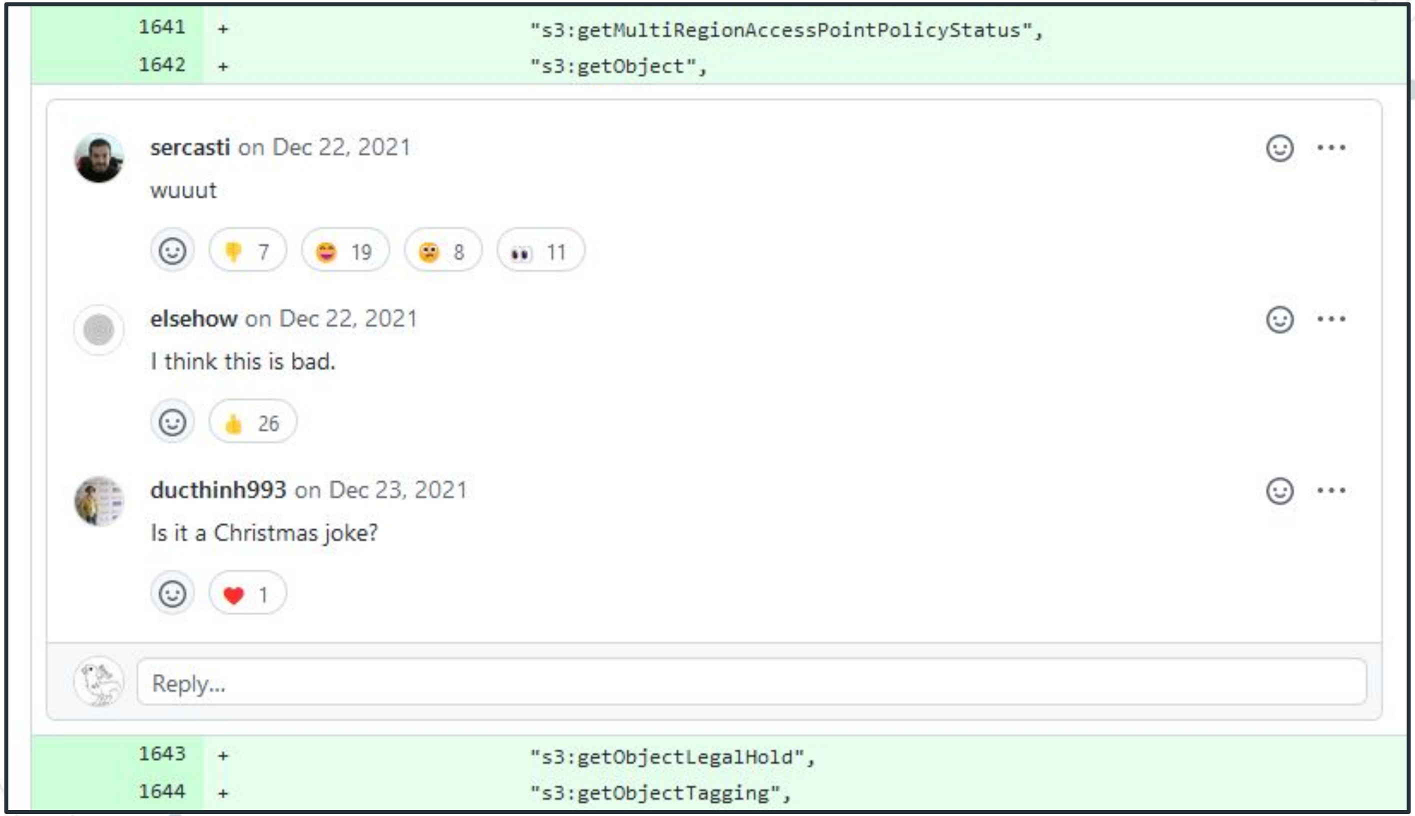
Scott Piper
@0xdabbad00

AWSSupportServiceRolePolicy just got s3:GetObject. 😱 That role is supposed to only have metadata visibility. @AWSSecurityInfo you need to roll that back.

MAMIP - Monitor AWS Managed IAM Policies @mamip_aws · Dec 21, 2021
AWSSupportServiceRolePolicy ... github.com/z0ph/MAMIP/com...

https://twitter.com/0xdabbad00/status/1473448889948598275?t=4JjT7z0XCe_dR00hH-vasw&s=19

Authorization (AuthZ)



```
+                "s3:getMultiRegionAccessPointPolicyStatus",
+                "s3:getObject",
```

sercasti on Dec 22, 2021

wuuut

👎 7 😄 19 😕 8 👀 11

elsehow on Dec 22, 2021

I think this is bad.

👍 26

ducthinh993 on Dec 23, 2021

Is it a Christmas joke?

❤️ 1

```
+                "s3:getObjectLegalHold",
+                "s3:getObjectTagging",
```

https://github.com/z0ph/MAMIP/commit/9d72709

Authorization (AuthZ)

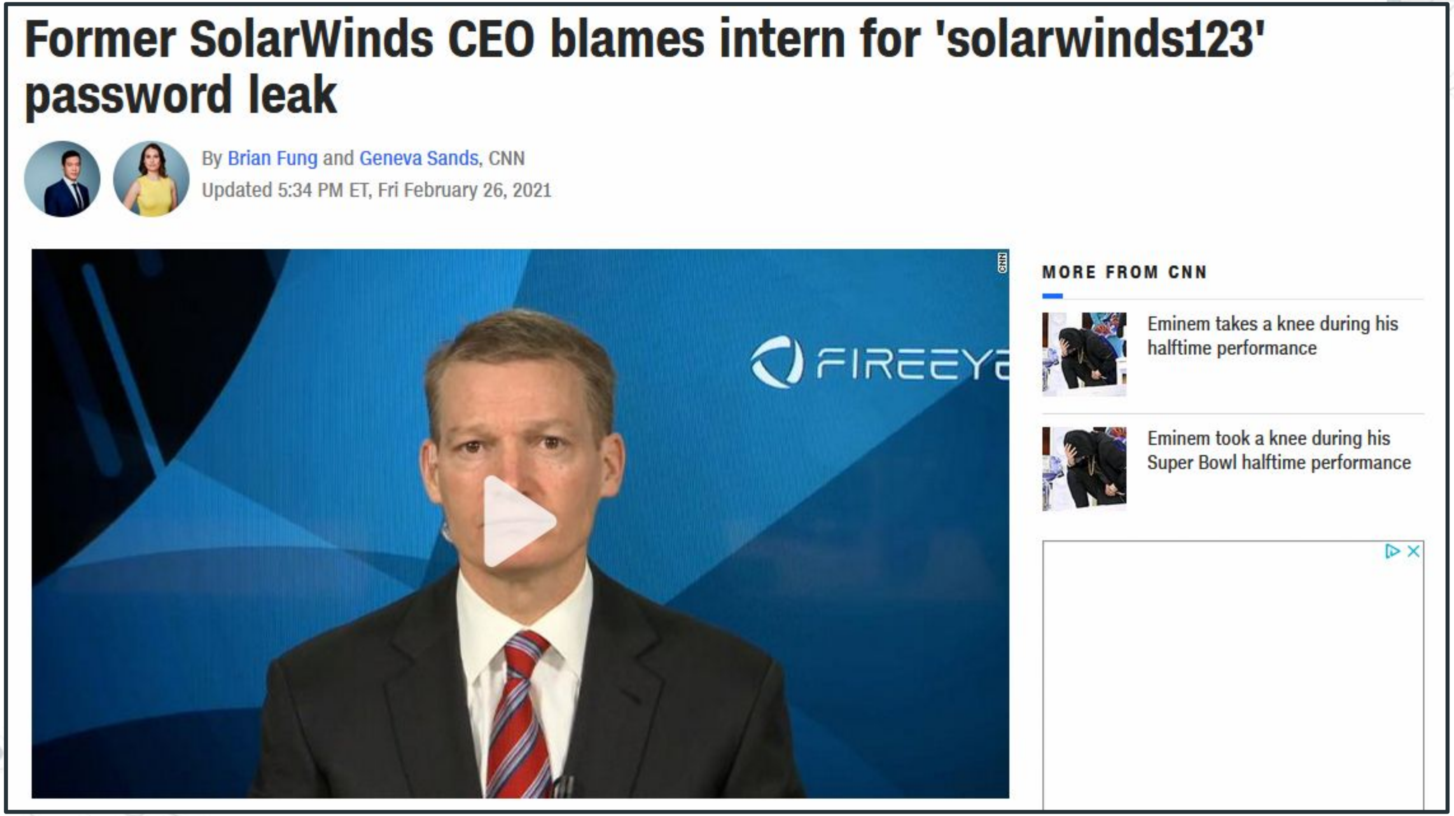
Principle of Least Privilege: A user should be given the least access needed for their role

Separation of Duties: No one person has complete access to a system

+ Improves security

− Causes friction as roles expand

Authorization (AuthZ)



Former SolarWinds CEO blames intern for 'solarwinds123' password leak

By Brian Fung and Geneva Sands, CNN
Updated 5:34 PM ET, Fri February 26, 2021

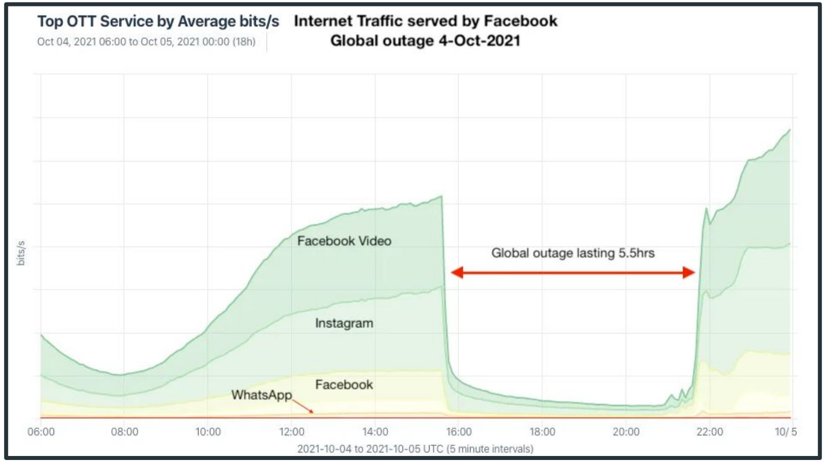
MORE FROM CNN

Eminem takes a knee during his halftime performance

Eminem took a knee during his Super Bowl halftime performance

https://www.cnn.com/2021/02/26/politics/solarwinds123-password-intern/index.html

“During maintenance [...] a command accidentally disconnected all of Facebook's data centers”



https://en.wikipedia.org/wiki/2021_Facebook_outage

Authorization (AuthZ)

Takeaway: Access control suffers from *systemic* problems:

- Poor interface and design
- Bugs
- Lack of maintenance

Solutions:

- Principle of Least Privilege
- Separation of Duties

Questions?