[tl;dr sec] #102 - Why AuthZ is Hard, Vendor Security 2.0, TruffleHog Chrome Extension

Detailed breakdown of why authorization is hard, how we should approach vendor security going forward, a Chrome extension to find secrets.

8 minute read

Hey there,

I hope you've been doing well!

Whisper Me Sweet Crypto Nothings

> *Shall I compare thee to a summer's day?*
> *Thou art more lovely and more temperate.*
> *...*
> *So long as men can breathe, or eyes can see,*
> *So long lives this, and this gives life to thee.*

Shakespeare may have set a high bar, but I don't think we've collectively lost our ability to woo romantically.

The world has just changed a bit.

There are new forms of art and ways to express (https://memes.com/blog/non-fungible-token-memes-that-help-us-understand-and-laugh-at-nfts) that you'll be a loving partner and provider. Like:

Webinar Next Week! (https://stackhawk.zoom.us/webinar/register/7616313099586/WN_WkpX2v4iROm-MFeEEnvUqg)

Next Thursday, Sept 30, I'll be joining StackHawk CSO Scott Gerlach (https://twitter.com/sgerlach) to discuss What's New with SAST + DAST (https://stackhawk.zoom.us/webinar/register/7616313099586/WN_WkpX2v4iROm-MFeEEnvUqg). Hope to see you there!

This must mean I've `#madeit`, as my friend Daghan (https://twitter.com/DaghanAltas) shared with me:

(https://twitter.com/andrew__reed/status/1437814085182050304?s=21)

🗒 In this newsletter...

- **AppSec**: TruffleHog the Chrome extension, BSidesSF CFP is open
- **Mobile Security**: Android automatically removes permissions from unused apps
- **Web Security**: Web security roadmap, add payload position support to Turbo Intruder, React security slides
- **Cloud Security**: Use GitHub Actions without long lived AWS creds, OMIGOD Azure bugs, permissions reference for AWS IAM
- **Machine Learning**: Applying OpenAI in cyber tooling, GitHub Copilot generated insecure code 40% of the time
- **Container Security**: Anonymous and ephemeral Docker image registry, critical review of NSA's k8s guidance
- **It's Time for Vendor Security 2.0**: Vendor Security Questionnaires are ineffective, what to do instead
- **Red Team**: Reverse engineering and binary exploitation challenges
- **Politics / Privacy**: America should fight back against ransomware, Facebook plans to use News Feed for its own PR, five-part WSJ Facebook investigation, how US police use Google to track you
- **Misc**: Remember Norm Macdonald, time travel debugging web apps
- **Why Authorization is Hard**: Real world challenges, trade-offs, and different approaches in building authorization in real companies

AppSec

TruffleHog The Chrome Extension (https://trufflesecurity.com/blog/trufflehog-the-chrome-extension)
Truffle Security's Dylan Ayrey (https://twitter.com/InsecureNature) has released a Chrome extension (https://github.com/trufflesecurity/Trufflehog-Chrome-Extension) for finding secrets that have made their way into JavaScript, as well as exposed `.git` and `.env` files. This happens more often then you'd think. See Dylan's Hacktivity talk (https://www.youtube.com/watch?v=i9b5Yij_HV4) for more details.

BSidesSF CFP Open until October 11 (https://bsidessf.org/cfp)
BSidesSF is one of my favorite cons- great talks and excellent hallwaycon. Highly recommend!

Mobile Security

Google will extend Permission Auto-Reset feature to older Android versions (https://therecord.media/google-will-extend-permission-auto-reset-feature-to-older-android-versions/)
Apparently Android has a Permission Auto-Reset feature that automatically removes user permissions from apps that haven't been opened and used for a few months. Neat!

Web Security

Web Security Roadmap (https://securityflow.io/roadmap/)
Detailed guide by HolyBugx (https://twitter.com/HolyBugx) on how to become a web security researcher, broken down by levels, topics, and resources.

defparam/haptyc (https://github.com/defparam/haptyc)
A Python library which was built to add payload position support and Sniper/Clusterbomb/Batteringram/Pitchfork attack types into Turbo Intruder, by Evan Custodio (https://twitter.com/defparam).

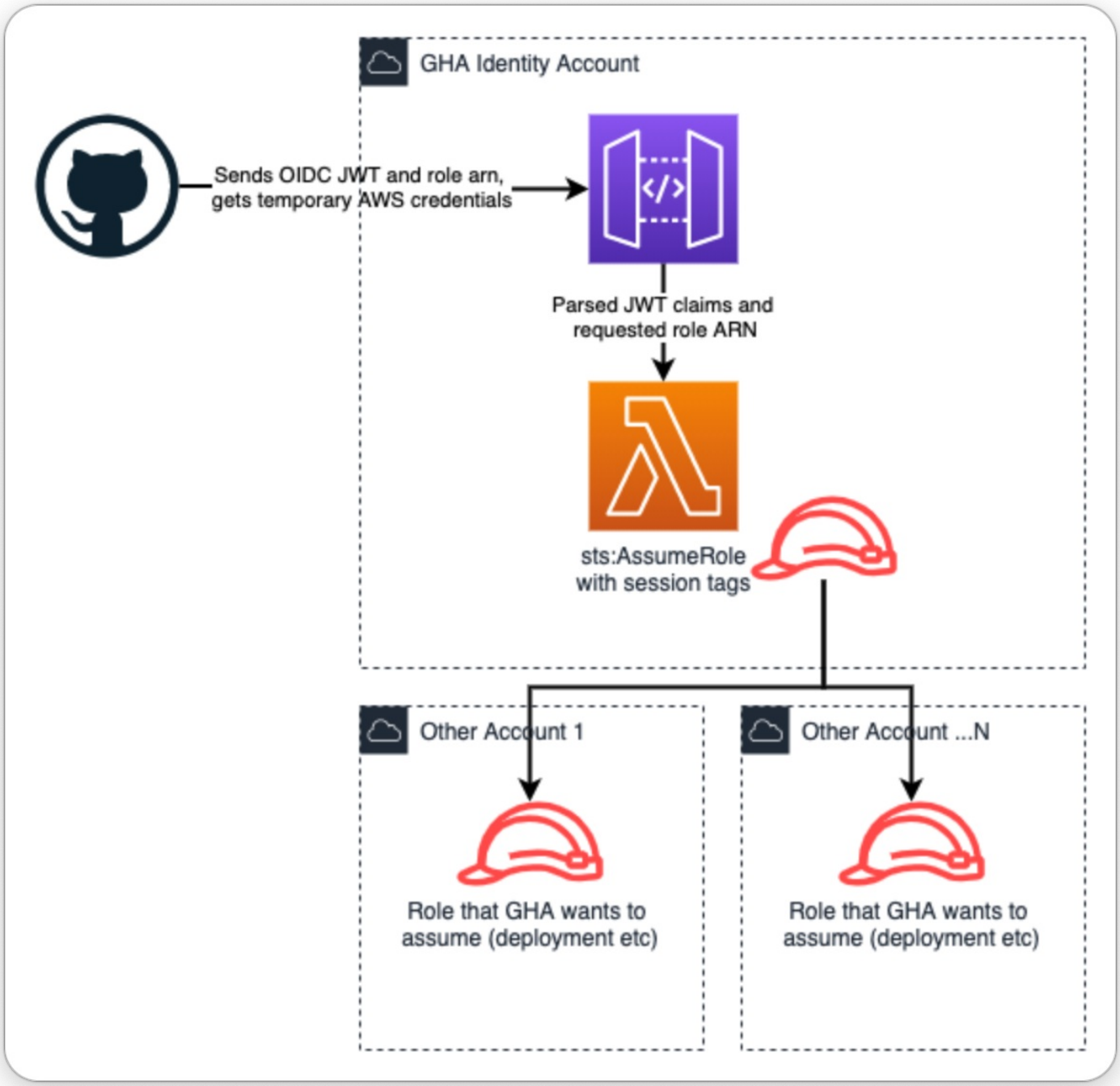
Better Security Through Code Hygiene (https://pragmaticwebsecurity.com/files/talks/securitycodehygiene.pdf)
React security slides by Philippe De Ryck (https://twitter.com/PhilippeDeRyck), including using DOMPurify to sanitize user input if you have to use `dangerouslySetInnerHTML`, and using Semgrep to flag insecure code. H/T Rami (https://twitter.com/ramimacisabird) for the link. Big +1 on Philippe's conclusions:

> - *Developers should focus on development, not on fine-grained security rules*
> - *Encapsulate dangerous features in secure components*
> - *Use code analysis techniques to flag direct use of dangerous features*

Cloud Security

AWS federation comes to GitHub Actions (https://awsteele.com/blog/2021/09/15/aws-federation-comes-to-github-actions.html)

AWS federation comes to GitHub Actions (https://awsteele.com/blog/2021/09/15/aws-federation-comes-to-github-actions.html)
By Aidan Steele (https://twitter.com/__steele): GitHub Actions has new functionality that can vend OpenID Connect credentials to jobs running on the platform. Meaning: CI/CD jobs no longer need **any** long-term secrets to be stored in GitHub! PoC (https://github.com/glassechidna/ghaoidc):

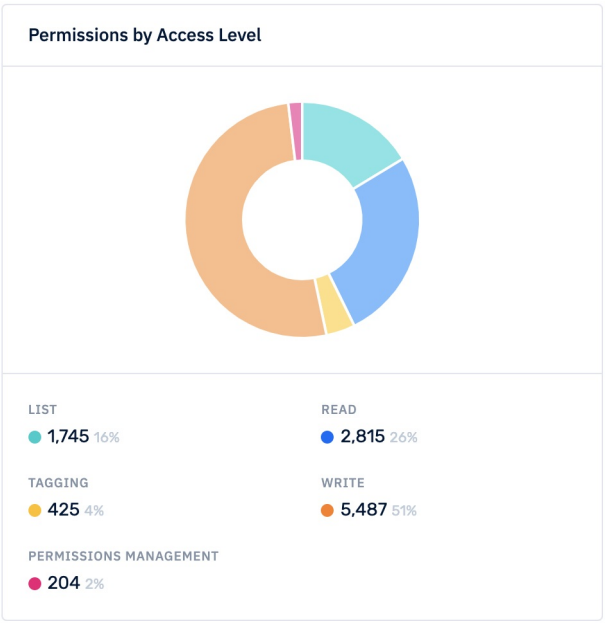


"Secret" Agent Exposes Azure Customers To Unauthorized Code Execution (https://www.wiz.io/blog/secret-agent-exposes-azure-customers-to-unauthorized-code-execution)
Great research by Wiz (https://twitter.com/wiz_io): Microsoft Azure silently install management agents on your Linux VMs, which now have RCE and local privilege escalation vulnerabilities. Mostly requires manual updates. Great play-by-play thread from Kevin Beaumont (https://twitter.com/GossiTheDog/status/1437896101756030982), and to quote Ami Luttwak (https://twitter.com/amiluttwak/status/1437898746747097090):

> *The RCE is the simplest RCE you can ever imagine. Simply remove the auth header and you are root. remotely. on all machines. Is this really 2021?*

If you want to play around with it, there's this BugHuntr.io (https://bughuntr.io/login?next=/scenario/bugs/CVE-2021-38647) lab, this nuclei template (https://github.com/projectdiscovery/nuclei-templates/blob/master/cves/2021/CVE-2021-38647.yaml), this Python PoC (https://github.com/horizon3ai/CVE-2021-38647), or watch IppSec's video (https://www.youtube.com/watch?v=TXqi1BKtcyM).

permissions.cloud: Permissions Reference for AWS IAM (https://permissions.cloud/)
Super cool work by Ian Mckay (https://twitter.com/iann0036): the IAM dataset (https://github.com/iann0036/iam-dataset) maps SDK calls to IAM actions, which are then displayed nicely on this site. Also, iamfast-js (https://github.com/iann0036/iamfast-js) and related repos aim to generate IAM policies based on analyzing your source code. Baller.



Machine Learning

Down the Rabbit Hole: Unusual Applications of OpenAI in Cybersecurity Tooling (https://spaceraccoon.dev/down-the-rabbit-hole-unusual-applications-of-openai-in-cybersecurity-tooling)
Eugene Lim (https://twitter.com/spaceraccoonsec) discusses his experiments with using OpenAI not just for human-based attacks like phishing and misinformation, specifically: reverse engineering assembly, analyzing Metasploit payloads, code reviews (e.g finding XSS), etc.

GitHub Copilot Generated Insecure Code In 40% Of Circumstances During Experiment (https://www.theinsaneapp.com/2021/09/github-copilot-generated-40-percent-insecure-code.html)
Out of 1,692 programs generated in 89 different code-completion scenarios.

Container Security

ttl.sh (https://ttl.sh/)
An anonymous & ephemeral (and free) Docker image registry, by Replicated (https://twitter.com/replicatedhq).

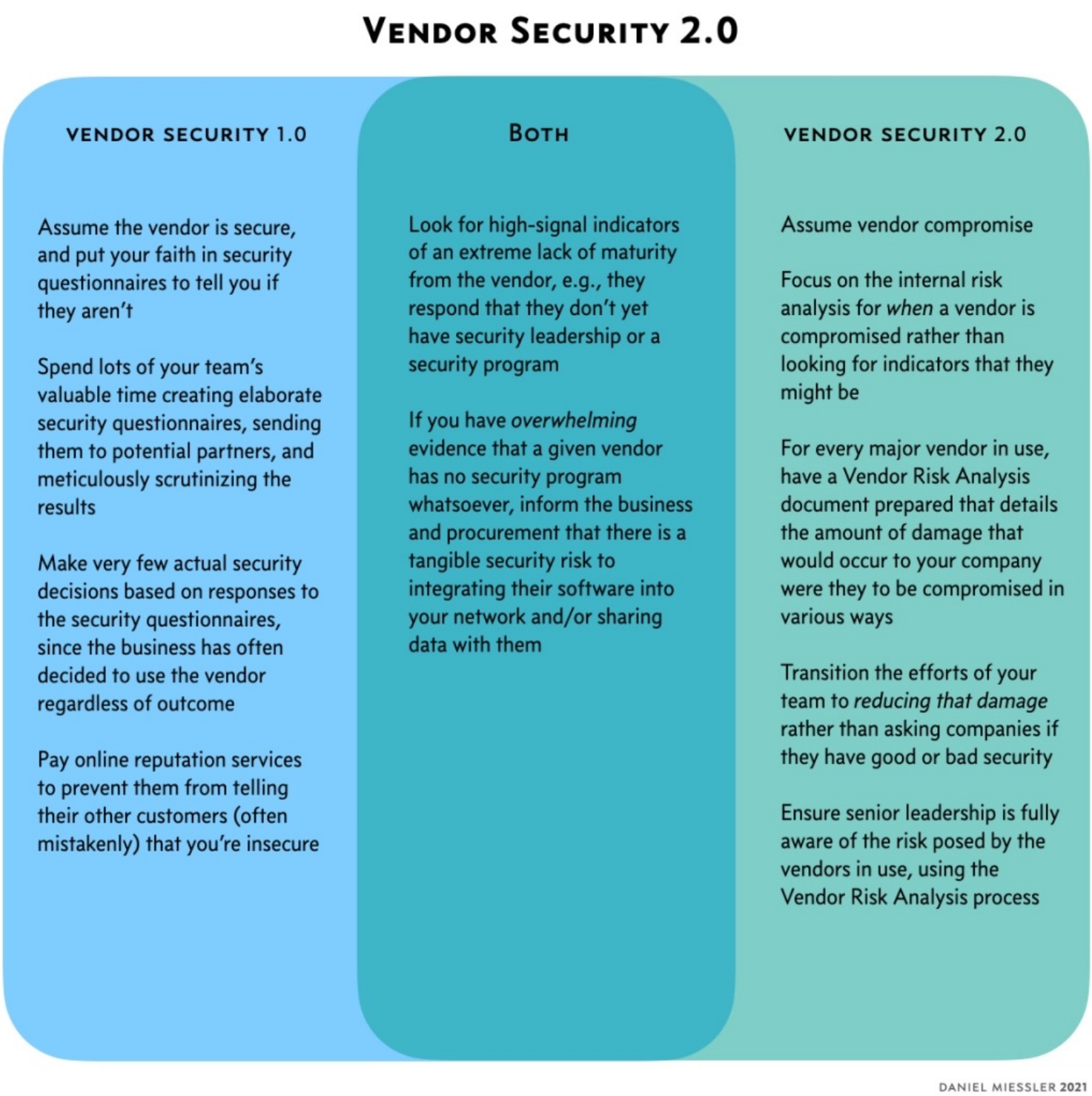
NSA & CISA Kubernetes Security Guidance – A Critical Review (https://research.nccgroup.com/2021/09/09/nsa-cisa-kubernetes-security-guidance-a-critical-review/)
NCC Group's Iain Smart (https://twitter.com/smarticu5) provides on feedback on what he views the NSA and CISA guidance doc outlined well, as well as some parts he views as misleading or incorrect.

It's Time for Vendor Security 2.0 (https://danielmiessler.com/blog/its-time-for-vendor-security-2-

0/)

Strong agree from me on this useful and snarky article by Daniel Miessler (https://twitter.com/DanielMiessler). Vendor Security Questionnaires seem ineffective at determining security posture and business needs often trump security recommendations.

Understanding a vendor's risk to your business if compromised and working to limit it - this is the way.



A few people had comments I liked on Twitter.

Thomas Ptacek (https://twitter.com/tqbf/status/1440721886409723905):

> *SOC2 exerts the same forcing pressure to organize security; of course, SOC2 is just the Boss Fight version of a dumb security questionnaire.*

And Dino Dai Zovi (https://twitter.com/dinodaizovi/status/1440722987133505541):

> *tl;dr: assume breach of every thing across a trust boundary and that includes vendors whether you give them money or not.*

> *Start with identifying data sent and/or held by that vendor and how much ability you have to reduce data risk while preserving value of using that vendor.*

> *Identify security maturity of vendor relative to sensitivity and volume of data sent/stored with them.*

> *Measure that downside of data at risk against the upside value of using that vendor. If upside > downside, continue using them. If downside > upside, don't use that vendor.*
>
> *Most of vendor security IMHO is matching data at risk to security maturity of the vendor.*

Red Team

Deus X64: A Pwning Campaign (https://deusx64.ai/)
A series of increasingly difficult computer security challenges pertaining to reverse-engineering and binary exploitation, by RET2 Systems (https://twitter.com/ret2systems).

Politics / Privacy

Opinion | America Is Being Held for Ransom. It Needs to Fight Back. (https://www.nytimes.com/2021/09/20/opinion/ransomware-biden-russia.html)
Crowdstrike co-founder Dmitri Alperovitch (https://twitter.com/dalperovitch) argues that sanctions and defense alone will not be sufficient against ransomware, as it's unrealistic to expect that every American hospital, school, fire department and small business to defend itself against highly sophisticated criminals. Instead, like with ISIS, the U.S. should pursue an aggressive campaign targeting the foundation of ransomware criminals' operations: their personnel, infrastructure and money.

Inside Facebook's Push to Defend Its Image (https://www.nytimes.com/2021/09/21/technology/zuckerberg-facebook-project-amplify.html)
Facebook has kicked off a new internal project to use the News Feed, its most important digital real estate, to promote articles about how Facebook is about ~~political polarization~~ ~~making you sad~~ ~~invading your privacy~~ ~~promoting vaccine skepticism~~ bringing us all closer together ❤. Cutting off external parties from analyzing engagement data? Don't worry about it 😵

The Facebook Files (https://www.wsj.com/articles/the-facebook-files-11631713039)
Oh boy, what a drop by the WSJ, a five-part investigation covering:

1. Facebook has a secret VIP list for whom standard policy enforcements do not apply.
2. An internal investigation found Instagram usage increased anxiety and depression, especially in teenage girls. more (https://www.bbc.com/news/technology-58570353)
3. Facebook's algorithm changes increased engagement, but made users angrier. The Zuck resisted proposed fixes because he was worried they would lead people to interact with Facebook less.
4. Facebook employees flag drug cartels and human traffickers leveraging the platform, but the company's response is often inadequate or nothing at all.
5. Company documents show antivaccine activists undermined Zuckerberg's ambition to support the rollout by flooding the site and using Facebook's own tools to sow doubt about the Covid-19 vaccine.

The new warrant: how US police mine Google for your location and search history (https://www.theguardian.com/us-news/2021/sep/16/geofence-warrants-reverse-search-warrants-police-google)
Article from The Guardian on geofence and keyword warrants. The fundamental challenge is that companies that depend on ad revenue slurp up user data for targeting purposes, but then they have a rich set of data that police can

depend on ad revenue slurp up user data for targeting purposes, but then they have a rich set of data that police can subpoena.

Misc

From Norm Macdonald's memori: Based on a True Story (https://twitter.com/seanoneal/status/1437854956934029315)
Right in the feels. Also, here's Norm on SNL's Celebrity Jeopardy (https://www.youtube.com/watch?v=bEghu90QJH4).

> *It can be difficult to define yourself by something that happened so long ago and is gone forever. It's like a fellow at the end of the bar telling no one in particular about the silver medal he won in high school track, the one he still wears around his neck.*

> *The only thing an old man can tell a young man is that it goes fast, real fast, and if you're not careful it's too late. Of course, the young man will never understand this truth.*

The Time Travel Debugger for Web Development (https://www.replay.io/)
Replay.io (https://twitter.com/replayio) is building a new tool that enables you to record web app execution flow and go backwards and forwards. Sounds awesome for tracking down tricky bugs. Time travel debugging (https://en.wikipedia.org/wiki/Time_travel_debugging) is one of the coolest concepts I wished I saw more of. Python, Java, and Ruby support coming.

Why Authorization is Hard (https://www.osohq.com/post/why-authorization-is-hard)

As a security consultant at NCC Group, I saw how a number of companies implemented authorization in their monolith or across their fleet of microservices.

Nearly universally, they had made some decisions early that ended up making things painful several years later.

This detailed post by Oso's Sam Scott (https://twitter.com/samososos) may be one of the best I've read on covering the real world challenges, trade-offs, and different approaches in building authorization in real companies.

The post also links to blog posts other companies have written about their authorization approach: Carta (https://medium.com/building-carta/authz-cartas-highly-scalable-permissions-system-782a7f2c840f), Slack (https://slack.engineering/role-management-at-slack/), Airbnb (https://medium.com/airbnb-engineering/himeji-a-scalable-centralized-system-for-authorization-at-airbnb-341664924574), Intuit (https://medium.com/intuit-engineering/authz-intuits-unified-dynamic-authorization-system-bea554d18f91).

Oso has also put together an even more lengthy write-up in their Authorization Academy (https://www.osohq.com/developers/authorization-academy). Nice!

Finally, check out the HN thread (https://news.ycombinator.com/item?id=28543457) on this post for various people weighing in, and posts by a number of other authorization-focused start-ups, including Authzed (https://play.authzed.com/schema) (YC W21), Cerbos (https://cerbos.dev/), Aserto (https://www.aserto.com/), and Warrant (https://warrant.dev/) (YC S21). Open source libraries referenced: Casbin (https://casbin.org/), and ory/keto (https://github.com/ory/keto), an implementation of Google's Zanzibar.

✉ Wrapping Up

Have questions, comments, or feedback? Just reply directly, I'd love to hear from you.

If you find this newsletter useful and know other people who would too, I'd really appreciate if you'd forward it to them

Thanks for reading!

Cheers,
Clint
@clintgibler (https://twitter.com/clintgibler) @tldrsec (https://twitter.com/tldrsec)

Tags: tldr_sec

Updated: September 22, 2021