DeFi Team OpSec: Security beyond the contracts

By: engn33r

Agenda

1. Why OpSec Matters
2. Attack Vectors
3. Defensive Measures
4. Emergency Planning
5. Spread Paranoid

Slides: engn33r.com

World’s Fastest Intro

I’m engn33r, I do security and coding

Currently dev @ Twyne
Formerly auditor @ electisec

yAudit

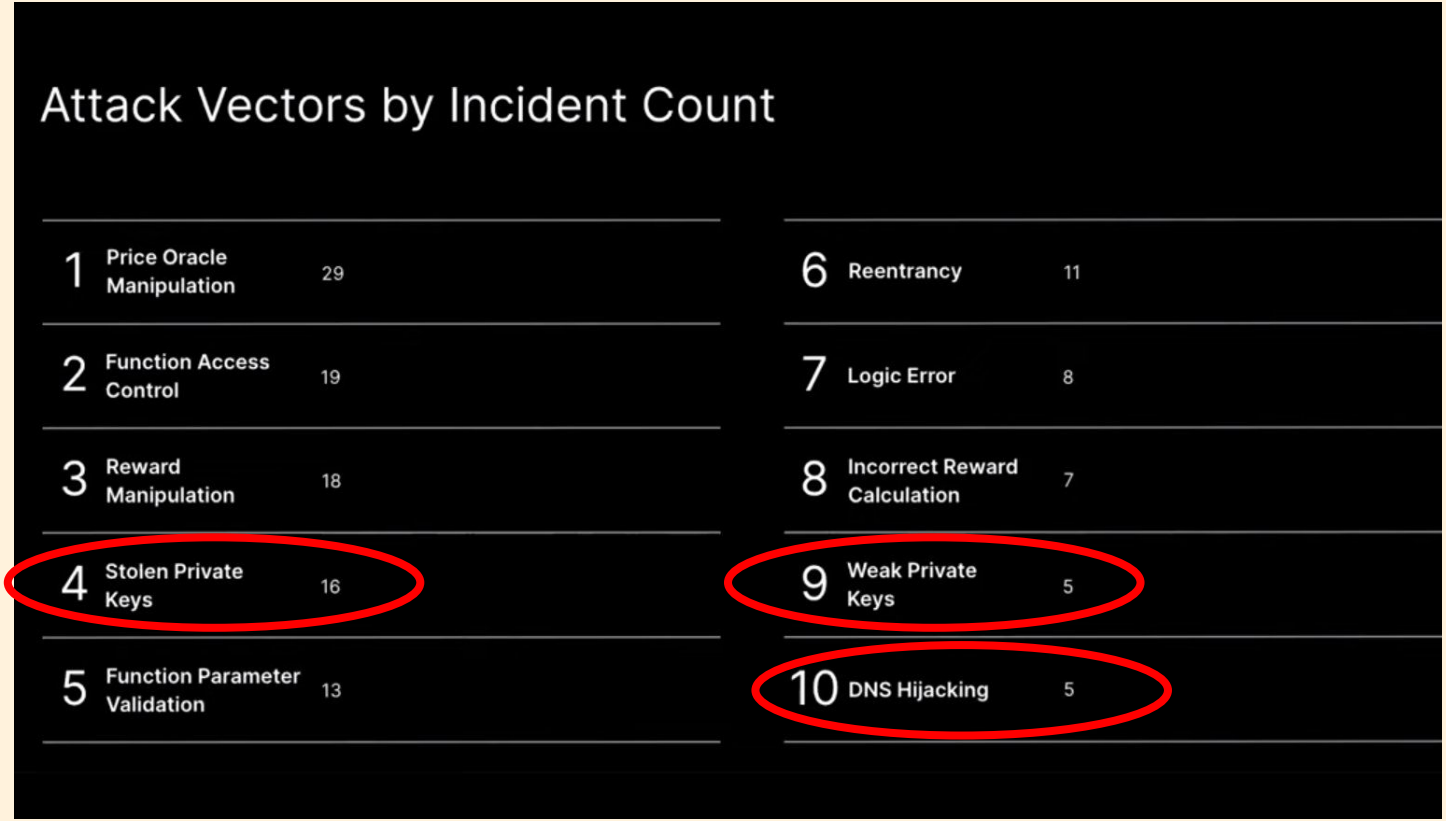
yAcademy

twyne

Electisec

Why Opsec Matters

Why OpSec Matters



Why OpSec Matters

How the Bybit hack happened: a $1.4 billion crypto breach explained

$50 Million Radiant Capital Hack Traced to North Korean Cybercriminals

Exclusive Curve Finance Founder Discusses Latest Hack and DeFi Vulnerabilities

Why OpSec Matters

- My theory: smart contract vulnerabilities will lose favor to web2 hacks
- Therefore, web2 security grows in importance in web3
- Web3 has often forgotten about web2 security, because web3 is shiny

Attack Vectors

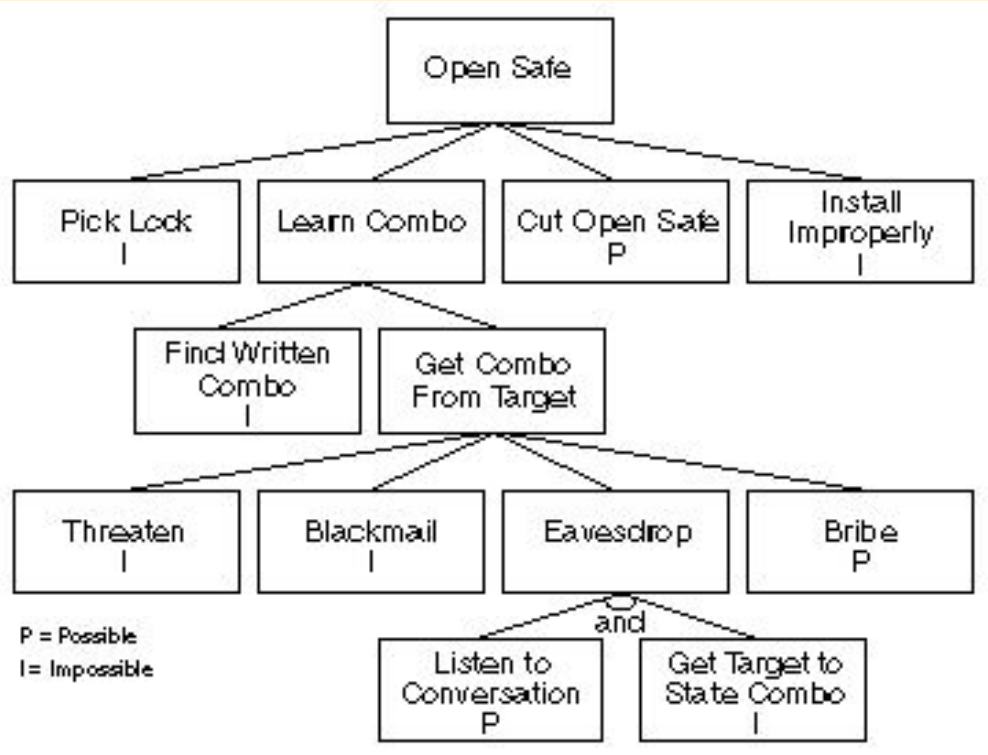
Attack Vectors

What is the attackers goal? Profit

How is this achieved?

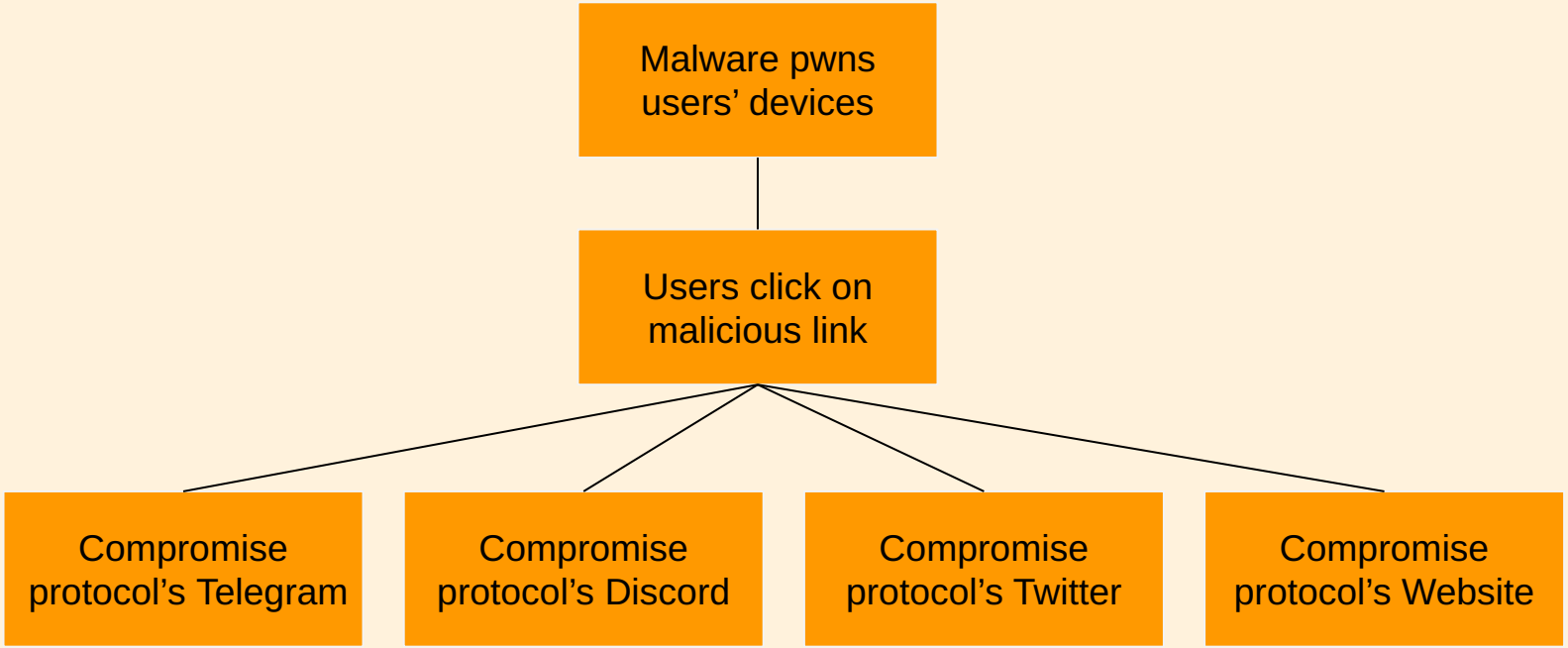
- Private key compromise -> hack the protocol
- Multisig attack -> hack the protocol
- DNS hijacking -> hack the users
- Inject malicious JS to frontend -> hack the users
- Email credentials compromise -> hack protocol reputation
- Telegram compromise -> hack protocol reputation
- Discord compromise -> hack protocol reputation
- etc.

Attack Vectors

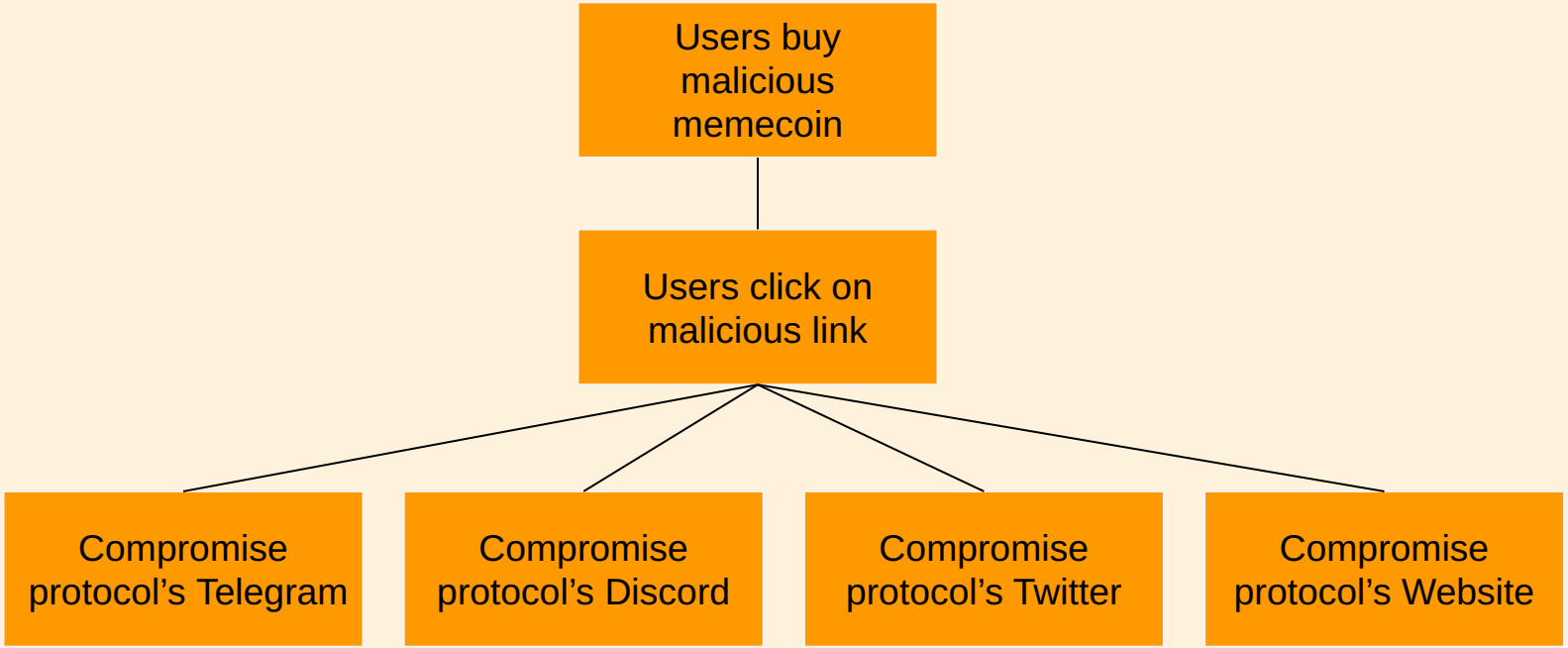


https://www.schneier.com/academic/archives/1999/12/attack_trees.html

Attack Vectors



Attack Vectors



Defensive Measures

Defensive measures

Back to tech basics!

- Is the entire team using updated software?
- Updated operating systems? Desktop and mobile?
- Is 2FA activated everywhere possible?
- Are code dependencies monitored for CVEs?
- Is everyone paranoid about cold outreach (AKA phishing)?

Full guide: engn33r.com/security-guide.html

Defensive measures

Quick tips:

- Got a suspicious file? Use virustotal.com
- Got a suspicious URL? Use urlscan.io (and virustotal.com)
- Set calendar reminders to check that your software is updated
- Enable 2FA for everything (yes, even personal accounts)
- Use a good password manager
- Use a separate browser profile for your crypto wallets

Emergency Plans

Emergency Plans

- How do you know if your protocol/system got hacked?
- Do you have someone on call 24/7? Or who will respond, and how?
- Do you have scripts for emergency governance actions?
- Do you know which contracts of the protocol are upgradeable?
- Do you have a checklist if starting a war room?

Yearn’s emergency checklist:
https://docs.yearn.fi/developers/security/EMERGENCY

Emergency Plans

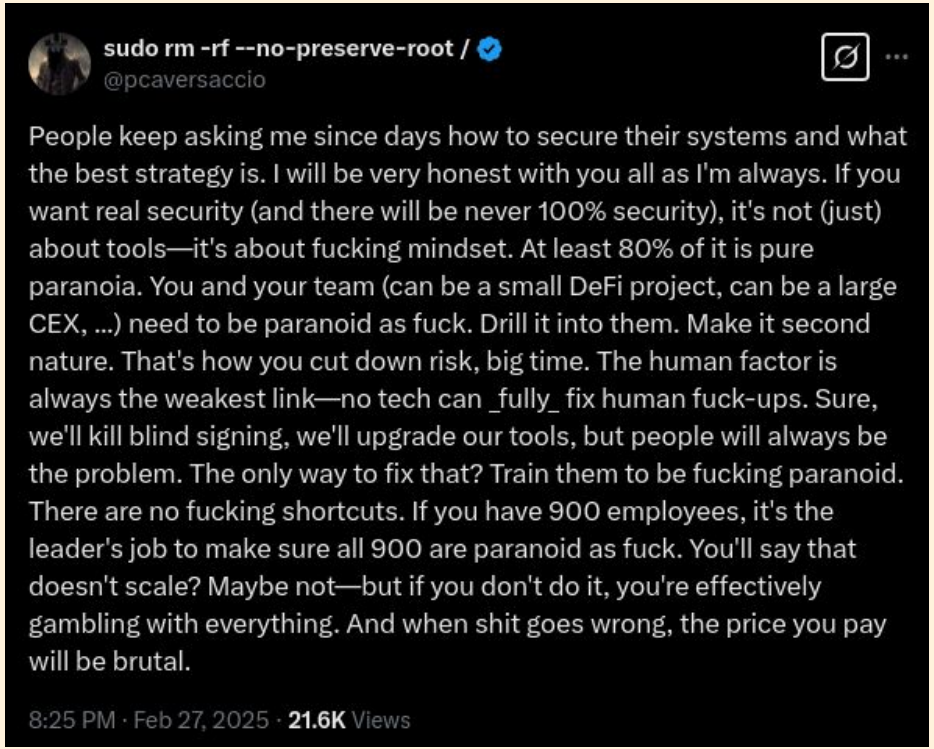
Prevent emergencies if possible

- Someone on your team should manage security
- Apply defensive measures
- Educate your team about the important of security
- Make an easy-to-find security page with contact info
- Recent addition: automated mempool hack protection (AKA firewall)

Spread paranoia

Spread paranoia

Spread paranoia



sudo rm -rf --no-preserve-root /
@pcaversaccio

People keep asking me since days how to secure their systems and what the best strategy is. I will be very honest with you all as I'm always. If you want real security (and there will be never 100% security), it's not (just) about tools—it's about fucking mindset. At least 80% of it is pure paranoia. You and your team (can be a small DeFi project, can be a large CEX, ...) need to be paranoid as fuck. Drill it into them. Make it second nature. That's how you cut down risk, big time. The human factor is always the weakest link—no tech can _fully_ fix human fuck-ups. Sure, we'll kill blind signing, we'll upgrade our tools, but people will always be the problem. The only way to fix that? Train them to be fucking paranoid. There are no fucking shortcuts. If you have 900 employees, it's the leader's job to make sure all 900 are paranoid as fuck. You'll say that doesn't scale? Maybe not—but if you don't do it, you're effectively gambling with everything. And when shit goes wrong, the price you pay will be brutal.

8:25 PM · Feb 27, 2025 · **21.6K** Views

https://x.com/pcaversaccio/status/1895087964910227459

Spread Paranoia

- Defensive measures only work if applied to the whole team
- If one weak link is exploited, the protocol can sink
- Chat with your team and confirm everyone is following security hygiene

Questions?

Thank you!