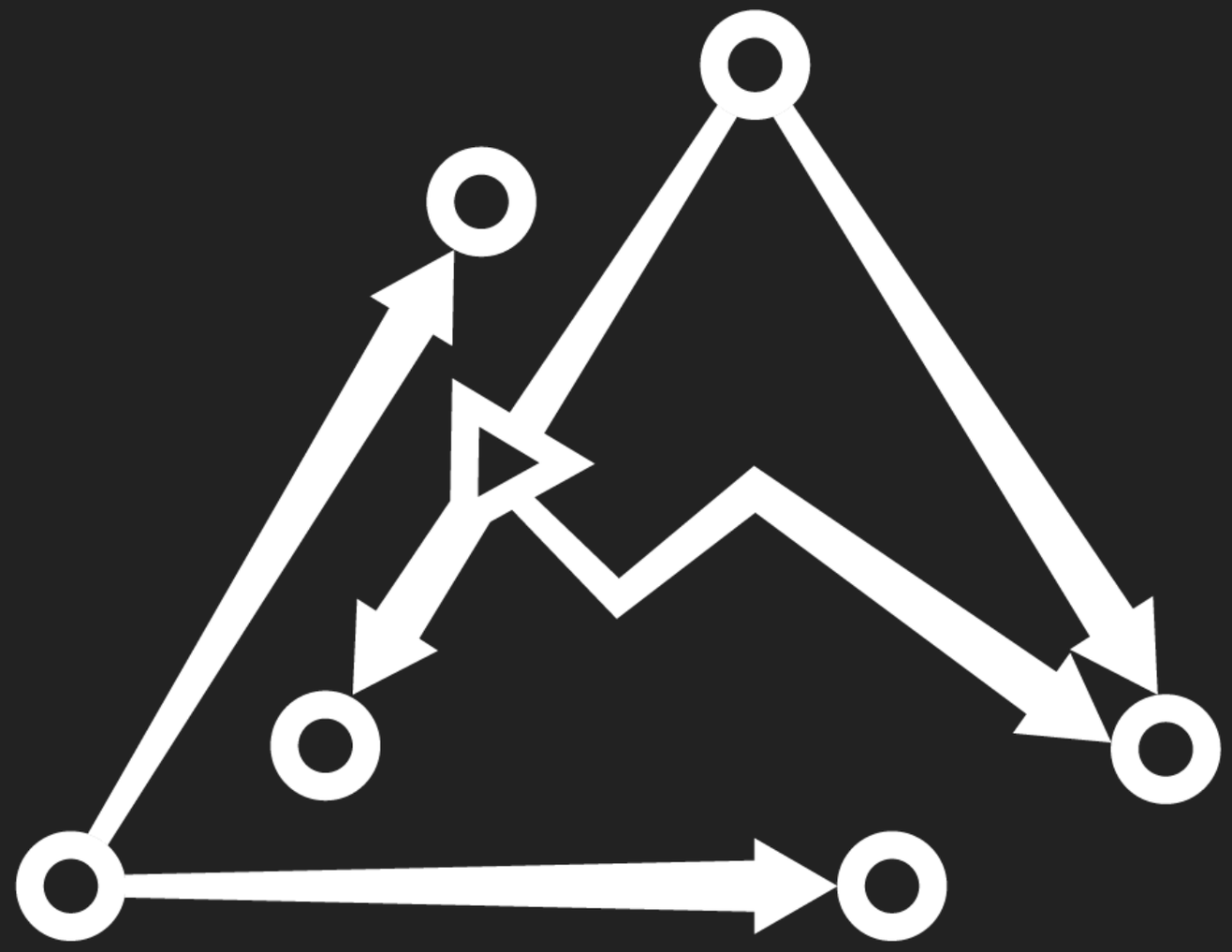
LEAST AUTHORITY

SECURITY SESSIONS



MEET THE SPEAKERS

Liz Steininger
CEO / Managing Director

Hind Kurhan
Senior Program Manager

AGENDA

1. Who We Are?
2. Why Does Security Matter?
3. Security Risk Management
4. Common Vulnerabilities
5. Security Consulting
6. How to Prepare for an Audit
7. What an Audit Engagement Looks Like

OUR MISSION

We believe people have a right to privacy.

We build and help others build usable secure technology that incorporates privacy by design. We give people control over their personal data with the use of decentralized and open source technology.

WHY DOES SECURITY MATTER?

We rely on data to make decisions.

Information is power.

“Data is the new oil.”

“Data is the new toxic waste.”

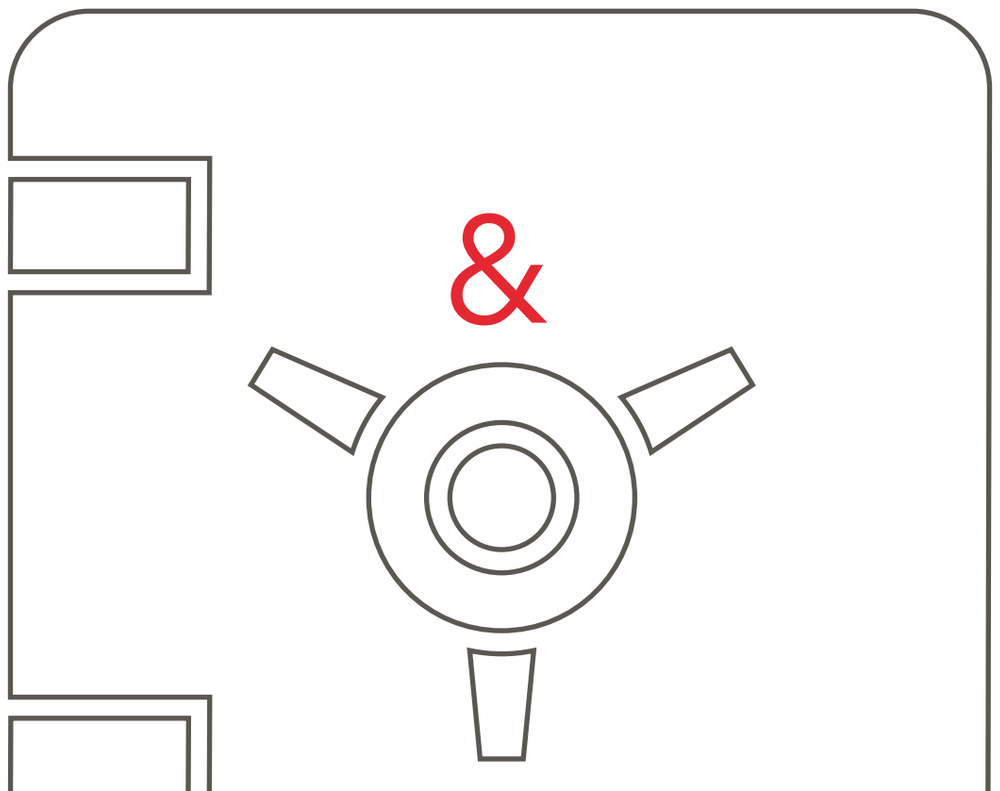
Least Authority
PRIVACY MATTERS

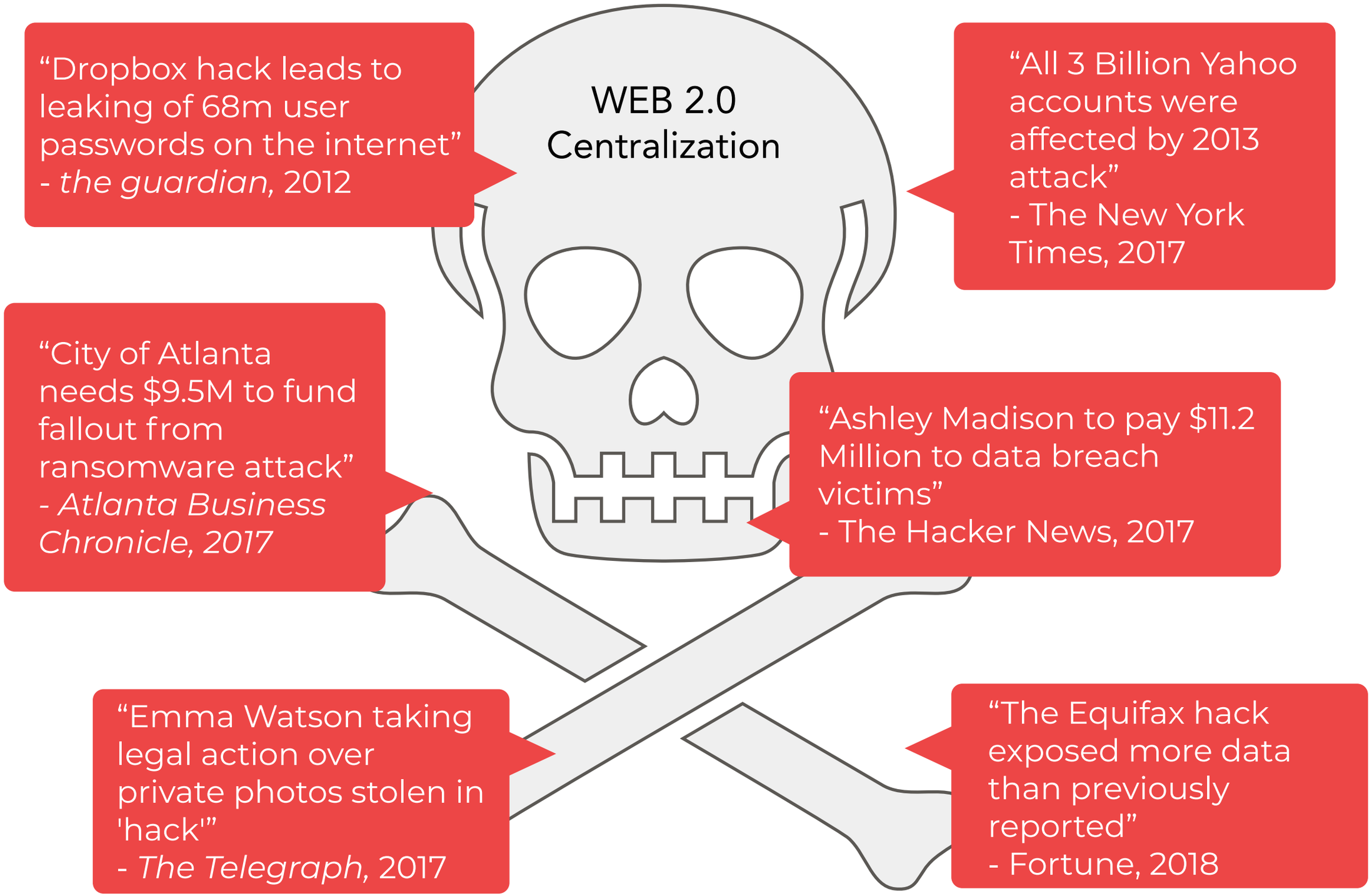
SECURITY IS ABOUT RETAINING CONTROL

Integrity

Confidentiality

Availability

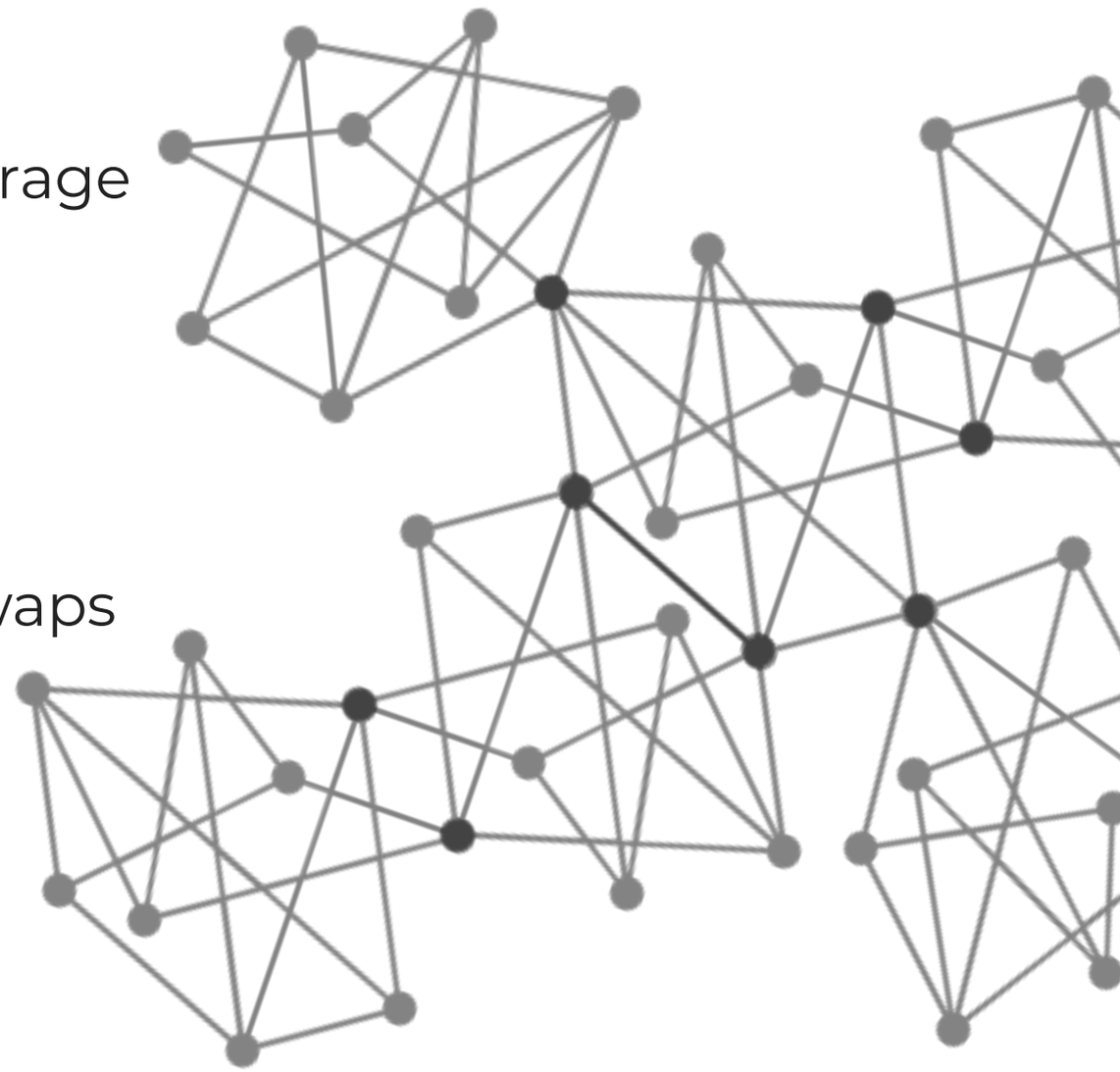



WEB 2.0
Centralization
“Dropbox hack leads to leaking of 68m user passwords on the internet”
- *the guardian*, 2012
“All 3 Billion Yahoo accounts were affected by 2013 attack”
- The New York Times, 2017
“City of Atlanta needs $9.5M to fund fallout from ransomware attack”
- *Atlanta Business Chronicle, 2017*
“Ashley Madison to pay $11.2 Million to data breach victims”
- The Hacker News, 2017
“Emma Watson taking legal action over private photos stolen in 'hack'”
- *The Telegraph*, 2017
“The Equifax hack exposed more data than previously reported”
- Fortune, 2018

Web3 Decentralization

- Ledgers, Blockchain protocols
- Consensus algorithms, Proof-of-Work, Proof-of-Stake
- Distributed data storage, off-chain storage
- Virtual Machines, smart contracts
- Governance and voting mechanisms
- Layer 2, cross-chain actions, atomic swaps

= New security models



RISK MANAGEMENT

- **Identify risks and assess:**
  - Probability
  - Impact
  - Responsibility
- **Then decide:**
  - Accept
  - Transfer
  - Avoid
  - Reduce

THREAT MODELING

- What do you have that someone else might want?
- Who would want this information you have?
- How could they get this information?
- When could they get this information?
- What are they willing to do to get this information?
- What are you willing to do to prevent this?

Identify

Define

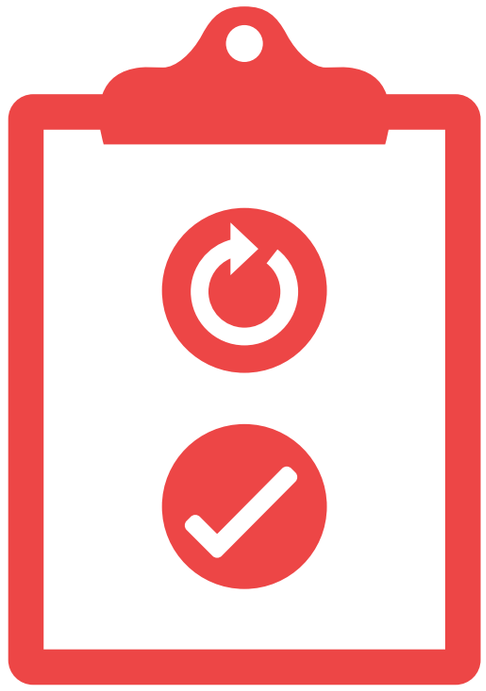
Prioritize

VULNERABILITIES: Protocol Design

- Central authority certification and admission control (denial-of-service attacks)
- Permissionless admission and proof-of-humanness (bots/botnets)
- Reputation management and multiple identities (Sybil attacks)
- Consensus methods and truth (Byzantine faults)
- Peer communications and data integrity (man-in-the-middle and poisoning attacks)
- Race conditions and front-running
- Reentrancy attacks in smart contracts
- Voting and incentives (gaming attacks)

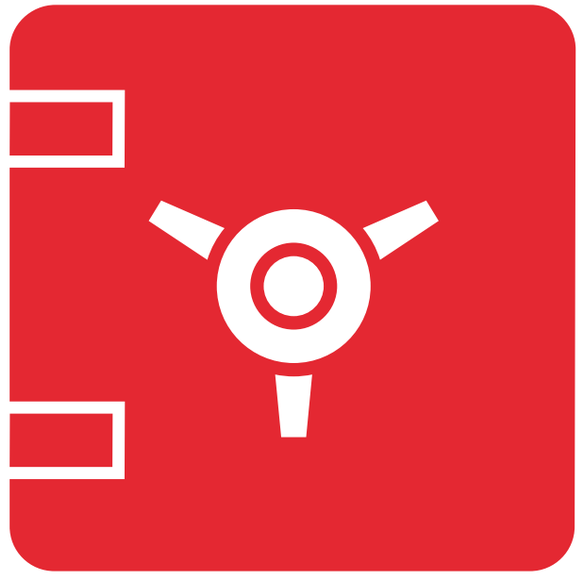
GOOD SECURITY PRACTICES

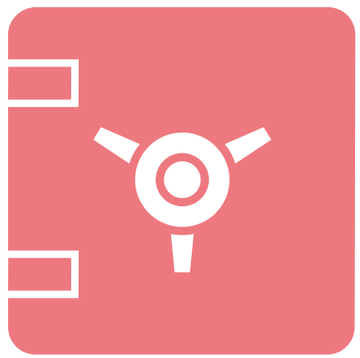
- Security by Design
- Principle of Least Authority/Privilege
- Transparency, open source code
- No single points of failure
- Build quality software
- Research and stay aware of new threats
- Perform internal reviews
- Hire external/independent reviewers
- Incentivize your community to participate in security



SECURITY BY DESIGN

- Security as a priority, from the start
- Incorporate
- Stay up to date on security research
- Share in the industry
- Improve technical documentation
- Provide development tools
- Share experiences and failures





SECURITY AUDITS

Goals of a security audit:

- Discover vulnerabilities before attackers
- Improve system quality to perform better
- Engage independent support and verification for feedback
- Assure stakeholders of due diligence
- Build community support for efforts

SECURITY ISN’T LIKE LOCKING YOUR HOUSE OR CAR – IT DOESN'T STOP THE BAD GUYS, BUT IF IT'S GOOD ENOUGH THEY MAY MOVE ON TO AN EASIER TARGET.

Paul Herbka, Director, Cloud and Managed Services, Denovo

SECURITY CONSULTING

Through our security consulting work, we aim to help teams minimize the potential for malicious attacks against users and protect user data privacy.

We mostly do this in 3 ways:

1. Security Audits
2. Limited Security Evaluations
3. Security by Design Consulting

SECURITY CONSULTING

1. Security Audits

- **Purpose:** Security audits are good for teams whose code is mostly feature complete and are looking to increase security prior to important milestones in their roadmap (for example, a mainnet launch or a token sale).

- **Define:** Design Specifications, Whitepapers and Source Code. The types of projects we work on include:

  Blockchains, cryptocurrencies, distributed ledgers, wallets, smart contracts, p2p network protocols, storage solutions, decentralized systems, incentive mechanisms, network and traffic analysis, key management, and more

SECURITY CONSULTING

2. Limited Security Evaluation

- **Purpose:** Not a full audit, yet highlights areas that are potentially vulnerable and require further investigation.

- **Define:** Smaller engagements, typically 1-2 days

  This typically entails a presentation by the client team and technical discussion on a very limited and defined scope (for example: an authentication flow or a specific solution).

SECURITY CONSULTING

3. Security by Design Consulting

- **Purpose:** Engage teams earlier in order to consider security earlier in the development lifecycle.

- **Define:** Advise on how a project can take security into consideration through each phase of the software and hardware lifecycle.

  This is done by partnering with a client to make an assessment of the current approach and recommend how to better integrate security considerations into the development processes, the roadmap, and the overall mission of a project.

HOW TO PREPARE FOR AN AUDIT

Why prepare for an audit? Preparing for an audit can help you efficiently utilize your resources and team to make the best use of the time.

1. Identify your goals

2. Plan ahead (if you can)

3. Find the sweet spot

4. Documentation!

5. Small steps go a long way

HOW TO PREPARE FOR AN AUDIT

1. Identify your goals

- **Scope priorities and constraints:** Develop an understanding of your scope, your priorities and your constraints in addition to understanding who your stakeholders are and who the audit is for (an exchange? the community? To improve internal security practices?).
- **Areas of Concern**

HOW TO PREPARE FOR AN AUDIT

1. Identify your goals

- **Scope priorities and constraints**
- **Areas of Concern:** We take a broad and comprehensive approach to our reviews - but you're the most familiar with your codebase so knowing what worries you, **whether it be Denial of Service attacks, race conditions, key management and handling, gaming of smart contracts, secure interaction between network components, or inappropriate permissions, for example, helps us eliminate unknowns.** If you don't have a specific set of concerns, that's ok too!

HOW TO PREPARE FOR AN AUDIT

1. **Identify your goals**

2. **Plan ahead (if you can):** Have a good understanding of where an audit fits in your roadmap allowing for features to be mostly complete and with enough time to address the issues identified during an audit before launch.

HOW TO PREPARE FOR AN AUDIT

1. **Identify your goals**

2. **Plan ahead (if you can)**

3. **Find the sweet spot:** Identify at which point you're comfortable enough for an auditing team to look at a snapshot of your code that is "feature complete" so they're not trying to hit a moving target.

HOW TO PREPARE FOR AN AUDIT

1. **Identify your goals**
2. **Plan ahead (if you can)**
3. **Find the sweet spot**
4. **Documentation!** You would be surprised how helpful even some documentation is to an auditing team. Documentation allows us to check for the correctness of the implementation and also allows new contributors and reviewers to better understand the entire system. This is one way to save costs.

HOW TO PREPARE FOR AN AUDIT

1. **Identify your goals**
2. **Plan ahead (if you can)**
3. **Find the sweet spot**
4. **Documentation!**
5. **Small steps go a long way:** Clean up your code, fix known issues, write unit tests, code comments, keep up with the latest version of your dependencies and look into whether they've had audits or have been victim of attacks, open source (if you can), and get involved with your community.

WHAT AN AUDIT ENGAGEMENT LOOKS LIKE

1. **Get in touch!**
2. Help you define your audit goals (if needed)
3. Send Proposal
4. Audit Kickoff
5. Establish Channels of Communication
6. Audit Report Delivery - Initial & Final
7. Publish your report (optional)
8. Follow-up audits

WHAT AN AUDIT ENGAGEMENT LOOKS LIKE

2. Help you define your audit goals (if needed)

- Our team can help in defining your audit goals by better understanding your project and your priorities.

WHAT AN AUDIT ENGAGEMENT LOOKS LIKE

3. Send Proposal

- **Process:** We look at everything and anything you've provided us, including code, design documentation, additional scope details, and the notes from our initial discussion to help inform our proposal.
- **1 week turnaround:** We turn our proposals around within 1 business week, which include a detailed scope, schedule, areas of concern, and cost for the audit.
- **Complete any revisions**

WHAT AN AUDIT ENGAGEMENT LOOKS LIKE

4. Audit Kickoff:

- **Meet the team:** A good auditing team is as diverse as the projects we work on, allowing for a variety of perspectives and different approaches to problem solving.
- **Schedule the kick-off**

WHAT AN AUDIT ENGAGEMENT LOOKS LIKE

5. Establish Channels of Communication:

- **Channel Options:** Slack, Github, Telegram, Discord - sky is the limit.
- **Communication is key:**
  - Allows us to provide our client team with full visibility into what is being done
  - Gives the client team an early heads up for issues found providing a headstart in fixing them

WHAT AN AUDIT ENGAGEMENT LOOKS LIKE

6. Audit Report Delivery: Initial & Final

- **Initial Audit Report:** After our initial investigation and analysis, we deliver an initial audit report that includes general feedback, specific issues, and best practice suggestions. **We also provide a mitigation and / or remediation strategy for each issue to help guide the development team in implementing the optimal solution.**
- **Verification & FInal Audit Report**

WHAT AN AUDIT ENGAGEMENT LOOKS LIKE

6. Audit Report Delivery: Initial & Final

- **Initial Audit Report**
- **Verification & FInal Audit Report:** Once the development team has taken the time to fix the issues outlined in the report - we go through and conduct a verification to make sure the issue has been addressed based on the agreed upon mitigation / remediation strategy.

WHAT AN AUDIT ENGAGEMENT LOOKS LIKE

7. Publish your report (optional)

- Our teams can coordinate to publish a version of the final audit report to share with stakeholders, users and the community - reinforcing that you've taken the steps towards making your project as secure as possible.

WHAT AN AUDIT ENGAGEMENT LOOKS LIKE

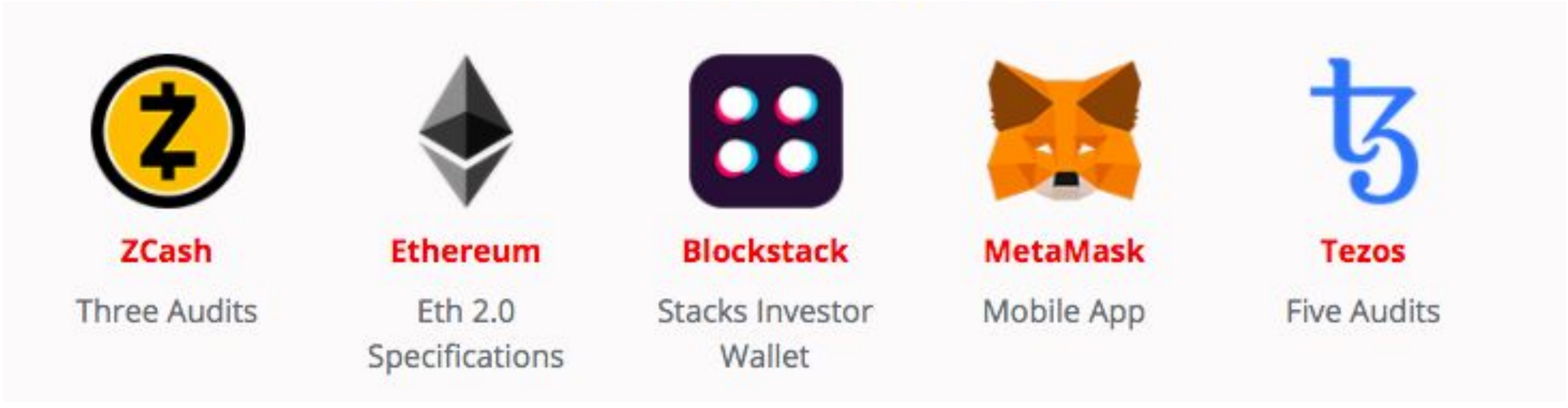
8. Follow-up audits

- We recommend follow up review at major milestones including introduction features, updates, upgrades, etc.

PUBLISHED AUDITS

Wondering if we've audited a project similar to yours?
Check out our list of published reports >>
leastauthority.com/security-consulting

- ProgPow Algorithm
- Nervos Network
- ConsenSys AG's MetaMask
  - Permissions System + Capnode
  - Plugin System + LavaMoat
- Centrifuge Tinlake Contracts + Actions



WHAT'S NEXT

If you found this informative and relevant to you, and you'd like to book a 1-on-1 specific to your project, you can do so here:

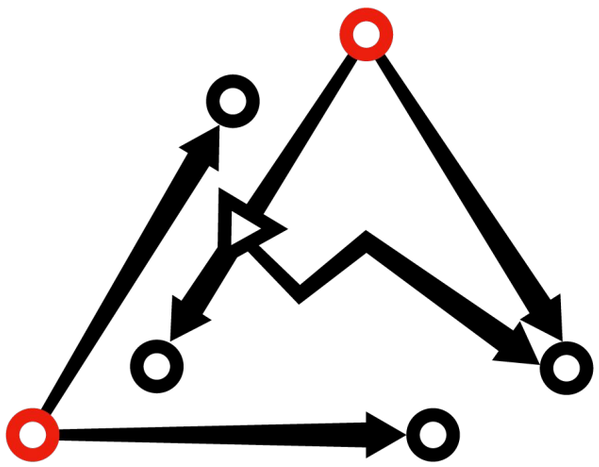
leastauthority.com

FOCUS ON SECURITY

We help projects improve their security and build secure technology.

From prototype to production, we work closely with teams through the complete development cycle to identify security issues and promote best practices. Our consulting services include security audits, design reviews and multi-phase engagements.

Learn More **Schedule a Call**



Least Authority

PRIVACY MATTERS

https://leastauthority.com

contactus@LeastAuthority.com

@LeastAuthority

EVERY PROGRAM AND EVERY PRIVILEGED USER OF THE SYSTEM SHOULD OPERATE USING THE LEAST AMOUNT OF PRIVILEGE NECESSARY TO COMPLETE THE JOB.

Jerome Saltzer