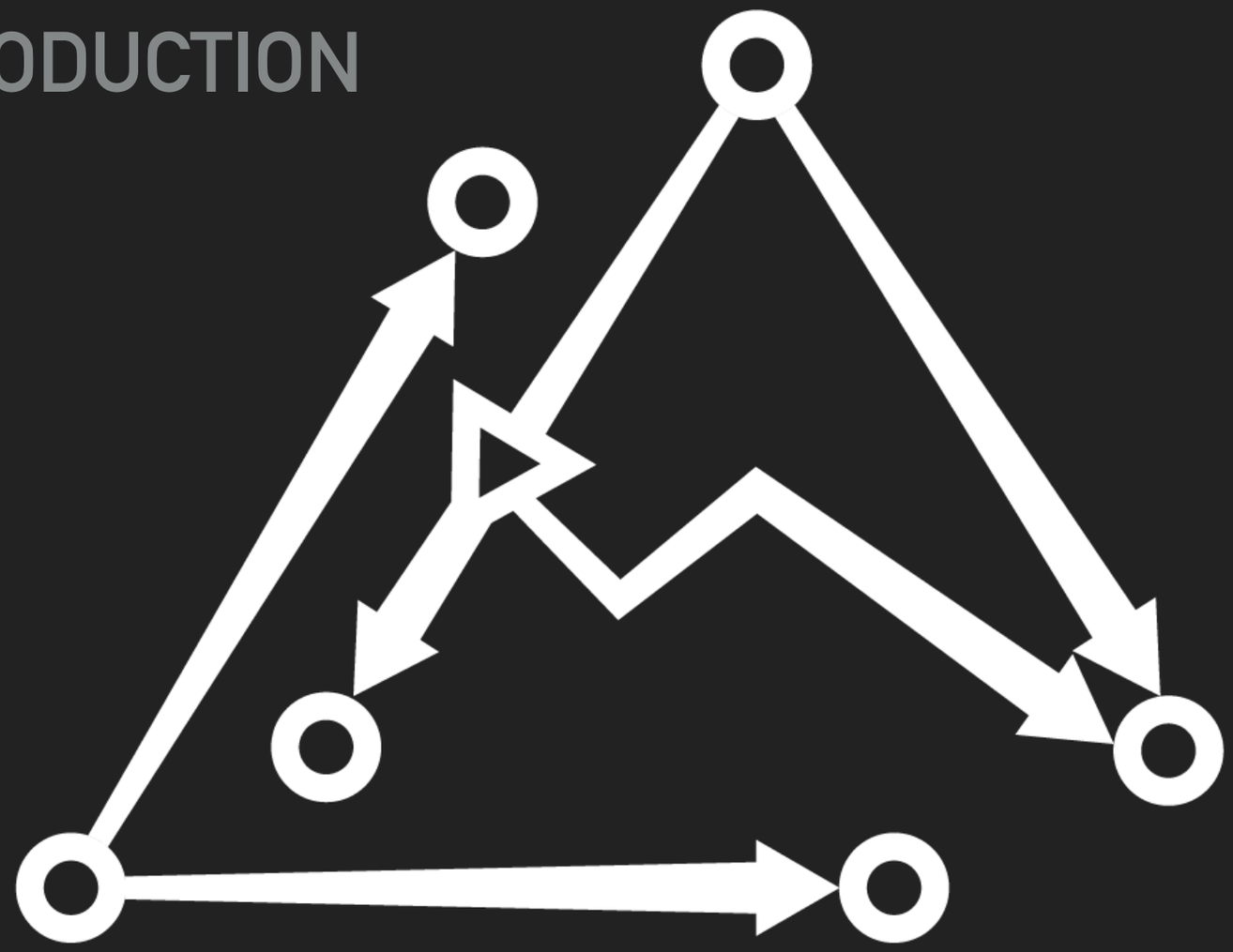
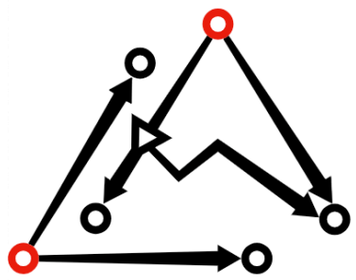
PRIVACY ENHANCING TECHNOLOGIES

INTRODUCTION



OUR MISSION

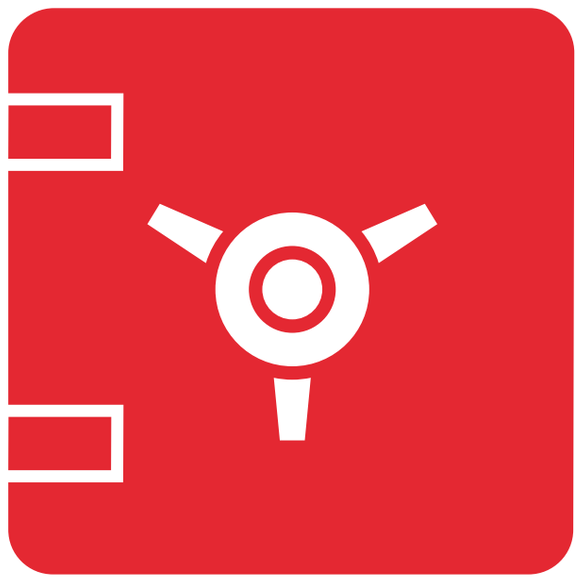
Least Authority's mission is to **build** and **support** ethical and usable technology solutions that advance digital security and privacy as fundamental human rights.



Least Authority

PRIVACY MATTERS

WHAT ARE PETS?



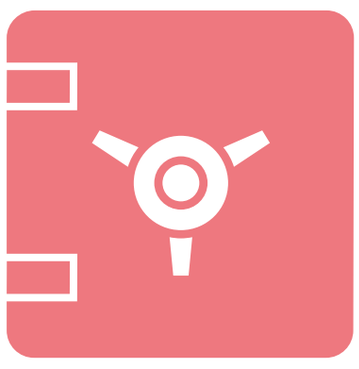
Protect personal data.

Privacy by design.

Require security.

Security by design, not policy.

Technical transparency.



WE MUST DEFEND OUR OWN PRIVACY IF WE EXPECT TO HAVE ANY.

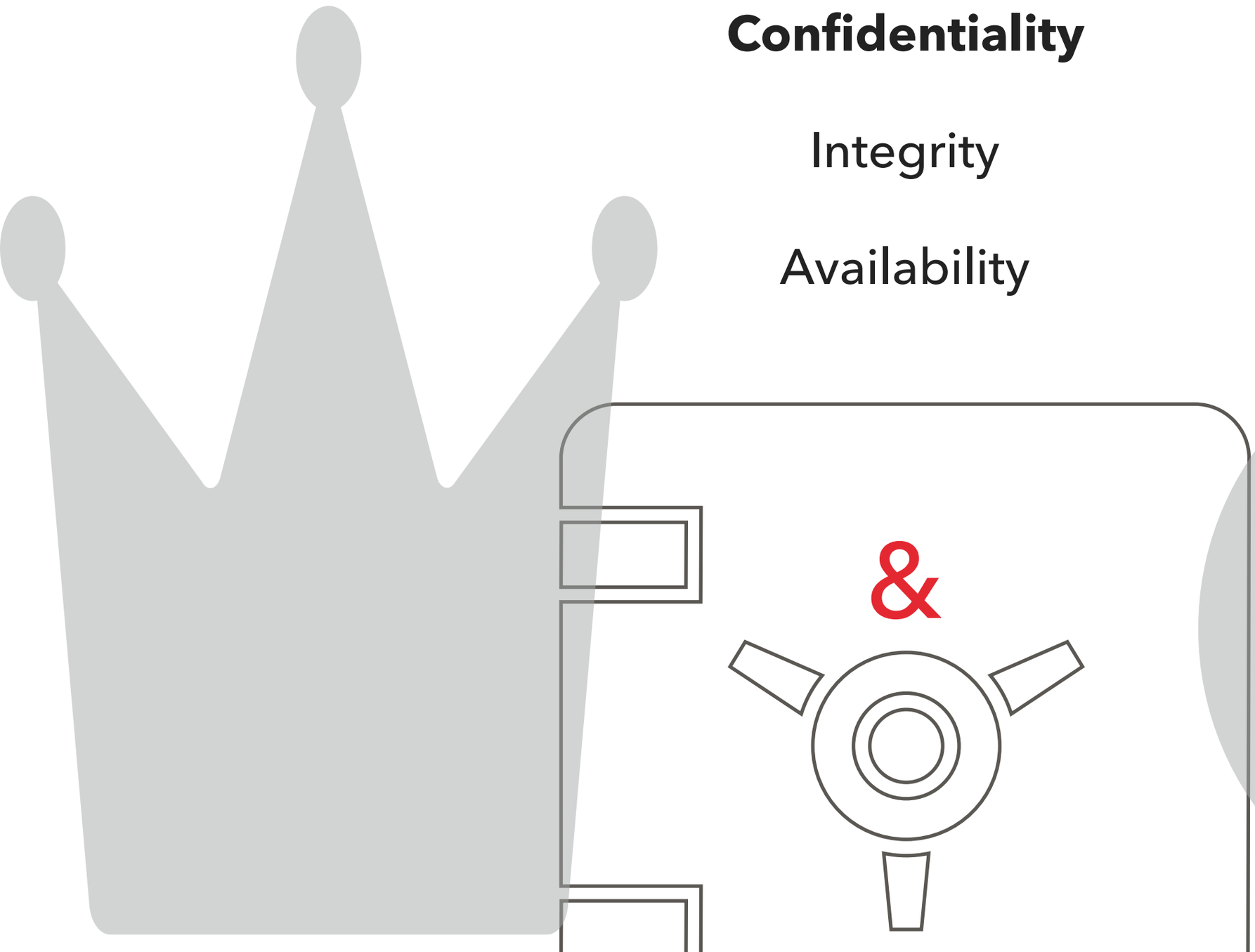
Eric Hughes
A Cypherpunk's Manifesto

SECURITY FACILITATES PRIVACY

Confidentiality

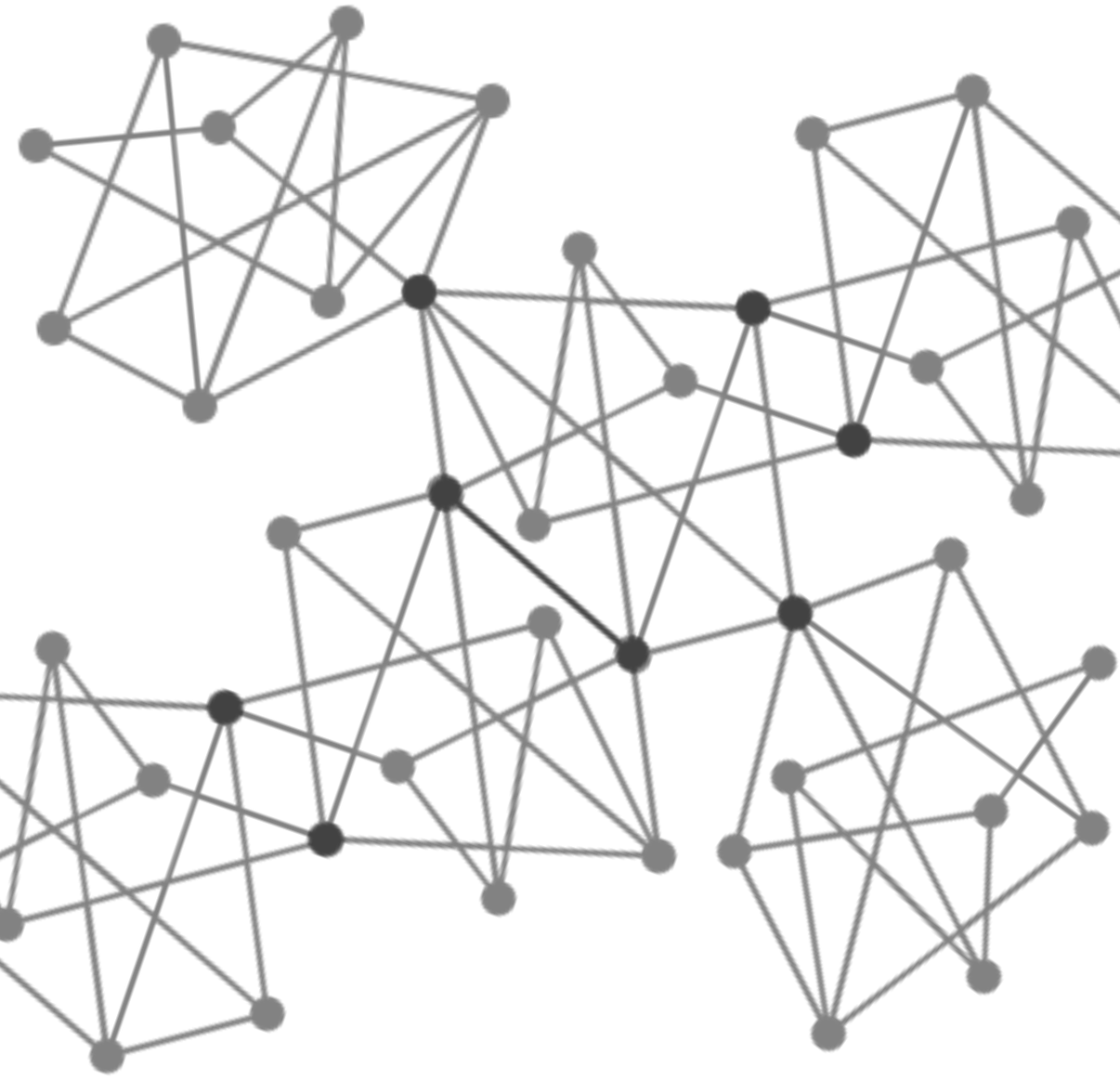
Integrity

Availability



PETS STRATEGIES

- Data minimisation
- Informed consent
- Obfuscation
- Decentralization
- Pseudonymity
- Anonymity
- Capability-based security (not identity-based)



= Control over Personal Data

TECHNICAL APPROACHES

- Public key infrastructure/digital signatures
- Hashes, salting and cryptographic hash algorithms
- Off-chain/out-of-network data storage
- Mixing & decoys
- Homomorphic Encryption
- Zero-knowledge proofs
- Secure multi-party computation

SECURITY IN IT IS 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

RISK MANAGEMENT

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

Nothing is 100% safe.

THREAT MODELING

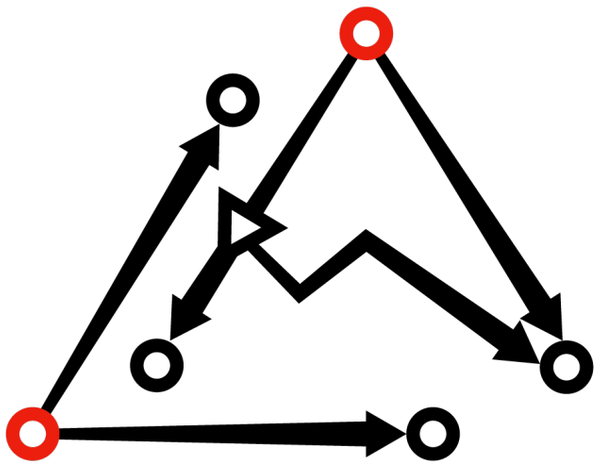
- What do you have that someone else might want?
- Who would want this information you have?
- How could they get this information?
- When could they get this information?
- What are they willing to do to get this information?
- What are you willing to do to prevent this?

ATTACK VECTORS

- 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)
- Voting and incentives (gaming attacks)

CHANGE THE PRIVACY PARADIGM

- Talk about why privacy matters and how the paradigm shift can happen
- Bridge learning from research to implementation teams utilising new technical approaches
- Publish regulations analysis, code, security audit reports and discuss lessons learned
- Fund new security research and implementation experiments, including UI/UX focus
- Make more developer resources that support security and privacy by design
- Engage in policy and governance discussions to ensure security is a priority
- Try new approaches to incentivize ethical design and issue disclosure
- Build partnerships and coalitions of privacy-tech professionals
- Set up training programs to help others be “privacy-minded”



Least Authority

PRIVACY MATTERS

https://leastauthority.com

Liz@LeastAuthority.com

Twitter: @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