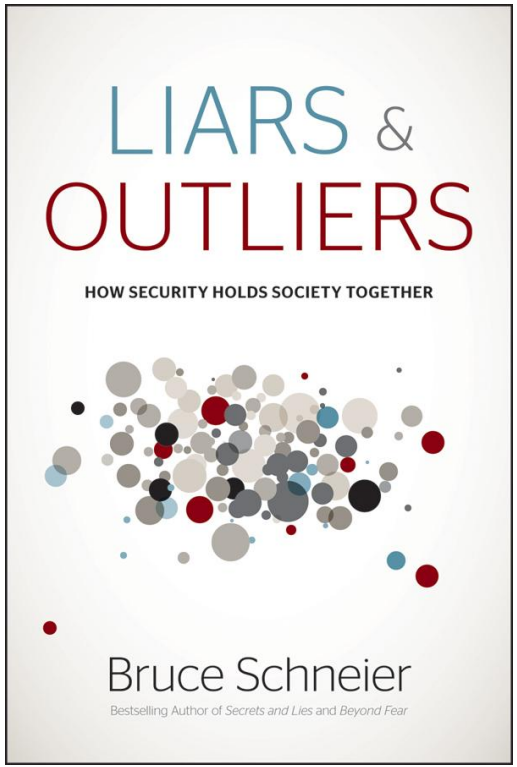
Trust I

Liars and Outliers



https://www.schneier.com/images/proposed-covers/liars-and-outliers.orig.jpg

Basic Definitions

Trust describes a situation in which the security of a system depends on the decisions made by other systems outside of its control.

Basic Definitions

- Security of system A depends on decisions made by system B
  - “A trusts B”
- Trust ≠ trustworthiness
- System A relies on system B, but security isn’t necessarily affected
  - “A relies on B”
  - Superset of trust

Reliance is Necessary for Society

- Allows for specialization
- Allows for institutions

Goals

- Reason about reliance and trust
- Manage reliance and trust; reduce risk from untrustworthy systems

Transitive vs. Intransitive Trust

- Transitive trust
  - You trust the people that the people you trust trust
  - If A trusts B, and B trusts C, then A trusts C
  - Examples?

Transitive vs. Intransitive Trust

- Transitive trust
  - You trust the people that the people you trust trust
  - If A trusts B, and B trusts C, then A trusts C
  - Examples
    - If I give you a key to my house, you could give it to anybody you trust
    - Whenever I trust a company, I trust all of their employees, subcontractors, etc

Transitive vs. Intransitive Trust

- Transitive trust
  - Facebook's Data Policy

    We transfer information to vendors, service providers, and other partners who globally support our business, such as providing technical infrastructure services, analyzing how our Services are used, measuring the effectiveness of ads and services, providing customer service, facilitating payments, or conducting academic research and surveys. These partners must adhere to strict confidentiality obligations in a way that is consistent with this Data Policy and the agreements we enter into with them.

Transitive vs. Intransitive Trust

- Intransitive Trust
  - You trust only the people you trust
  - If A trusts B, and B trusts C, A does not necessarily trust C
  - Examples?

Transitive vs. Intransitive Trust

- Intransitive Trust
  - You trust only the people you trust
  - If A trusts B, and B trusts C, A does not necessarily trust C
  - Examples
    - If I let you in my house, I don't have to let in the people you claim are trustworthy
    - Security clearances: you don't get to tell people you trust

Control vs. Choice

- If A controls B, then A doesn't trust B
- But A probably can't control B…
  - Subcontractors
  - Service providers (restaurants, ISPs, etc)
  - Supply chains
- What A *can* do is make a judgment:
  - "Is B trustworthy?"
  - Then choose whether or not to trust B

Control vs. Choice

- Big question: how do we know if B is trustworthy?

Trustworthiness

- Reputation
  - Past experience with B
  - Learn about trust from others with experience with B
  - Reputation management systems
    - Examples?

Trustworthiness

- Reputation
  - Past experience with B
  - Learn about trust from others with experience with B
  - Reputation management systems
    - Examples
      - Comments/ratings (eBay, Amazon, Yelp, etc)
      - Consumer Reports

Trustworthiness

- Third-party mediators
  - Trust a third party to make trustworthiness decisions
  - Examples?

Trustworthiness

- Third-party mediators
  - Trust a third party to make trustworthiness decisions
  - Examples
    - FDA
    - Certificate Authority system
    - Private/Invite-Only Torrent Trackers
      - Trusting tracker (to ban misbehaving members)
      - Trusting other members (to invite trustworthy people)
    - App store

Trustworthiness

- Third-party mediators
  - Trust a third party to make trustworthiness decisions
  - Failure of the trusted third party can be *big*
  - e.g., 2008 financial crisis

Trustworthiness

- Incentives
  - “Some men just want to watch the world burn”
    - ...yeah, but not usually
  - Most people have interests/goals
  - Make it so that *being trustworthy* is in their interest
  - Examples?

Trustworthiness

- Incentives/disincentives
  - Examples
    - Reputation systems (reputation affects success)
    - Regulation with punishments
      - Ensures not just vague “trustworthiness,” but prevents certain undesired behaviors
      - Casinos and probability regulation
      - Environmental regulation
    - Bitcoin mining

Scope

- Trust for as little as possible
- If you hire a plumber…
  - Don’t let their friends into your house (transitivity)
  - Don’t listen to them for medical advice
- When you can’t do this, the risk is higher
  - Sysadmins

Process vs. Outcome

- We've seen ways to ensure trustworthiness
- Ensuring that the *process* is trustworthy
- Another approach is to verify the *outcome*
  - *Rely* on systems, but not *trust*
- Examples?

Process vs. Outcome

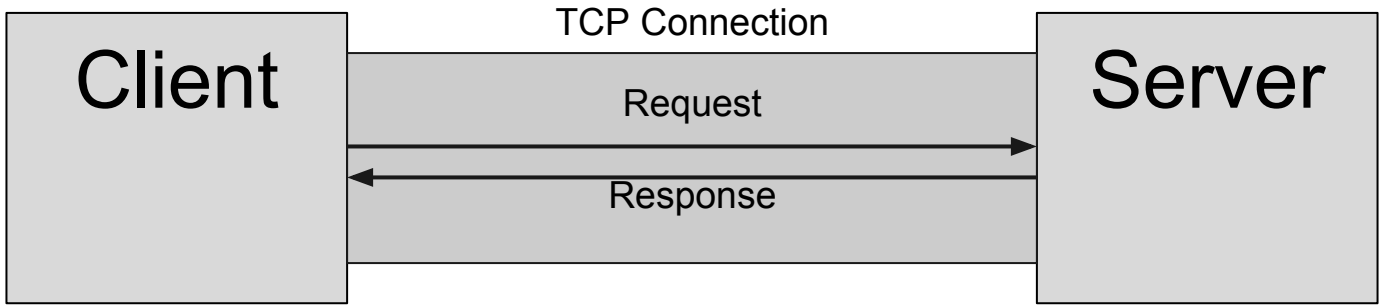
- We've seen ways to ensure trustworthiness
- Ensuring that the *process* is trustworthy
- Another approach is to verify the *outcome*
  - *Rely* on systems, but not *trust*
- Examples
  - Test-drive a car before buying it
  - End-to-end encryption
    - "Over an *untrusted* network" (not *untrustworthy*)

Stop...

Example time.

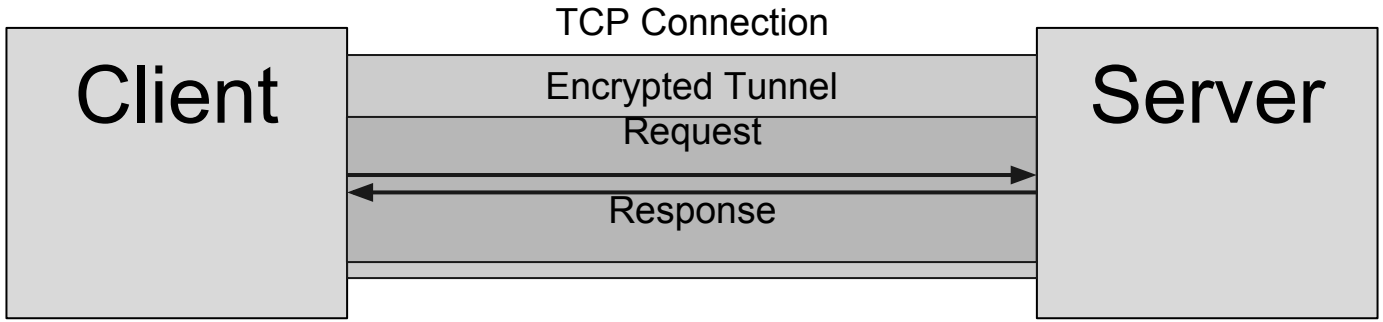
Certificate Authority System

- HTTP is a simple, unencrypted protocol
- Connect over TCP to server, request data



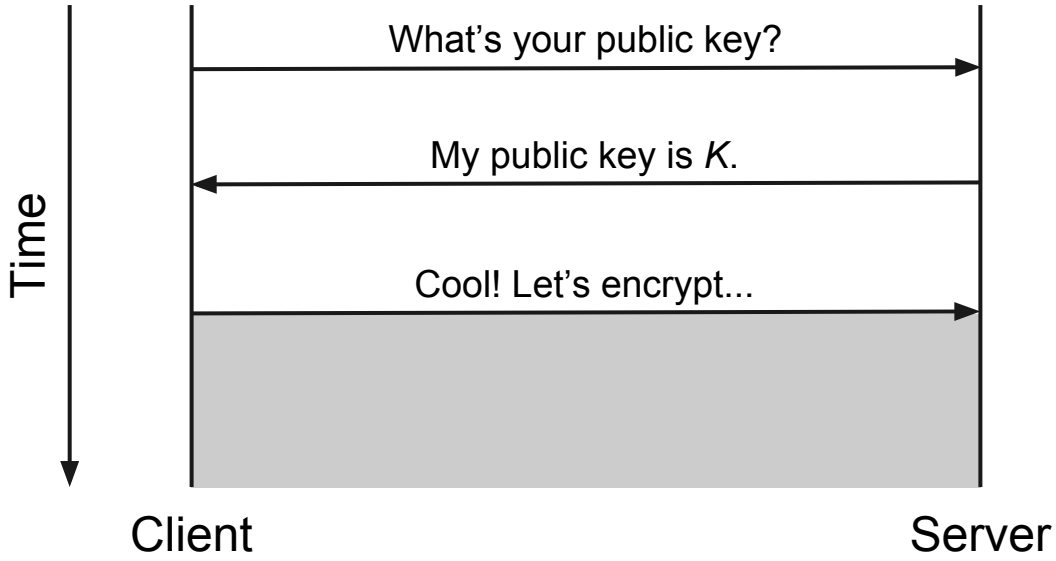
Certificate Authority System

- HTTPS is the secure version of HTTP
- Create encrypted tunnel, perform HTTP



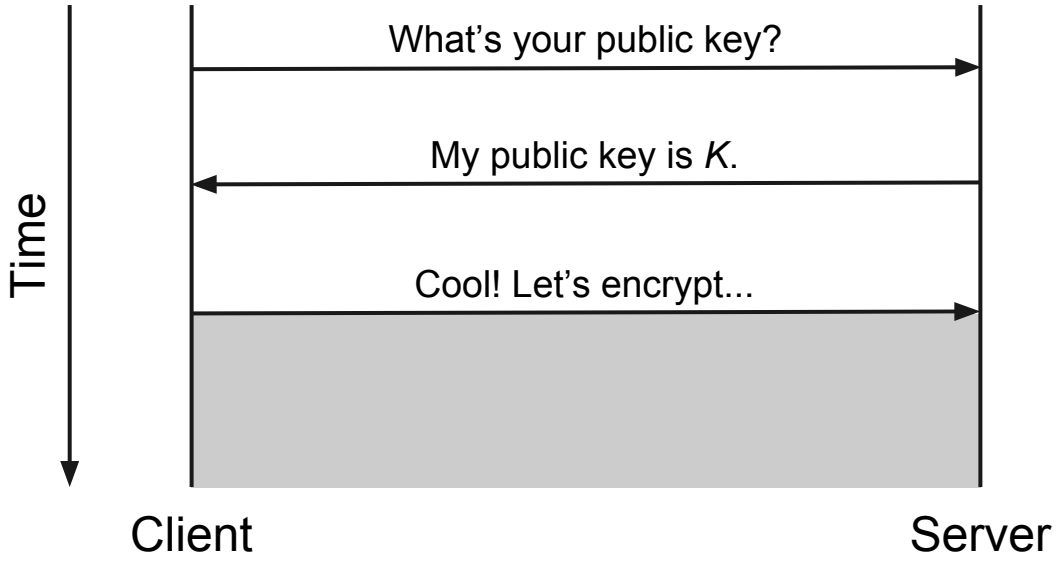
Certificate Authority System

- Simplified version of the protocol



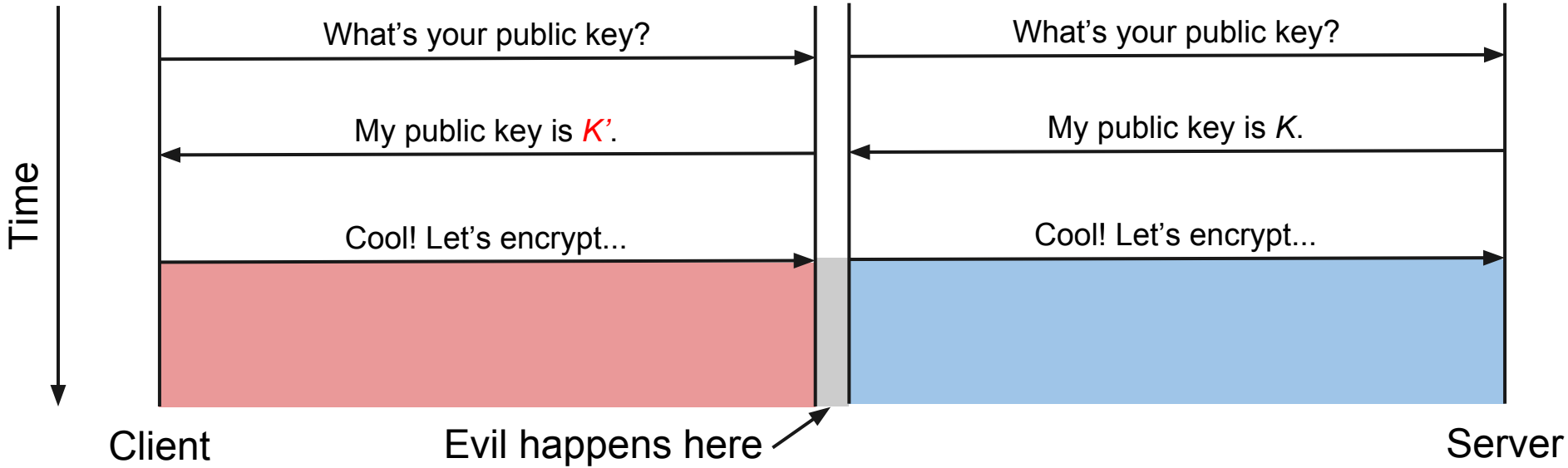
Certificate Authority System

- What's wrong with this?



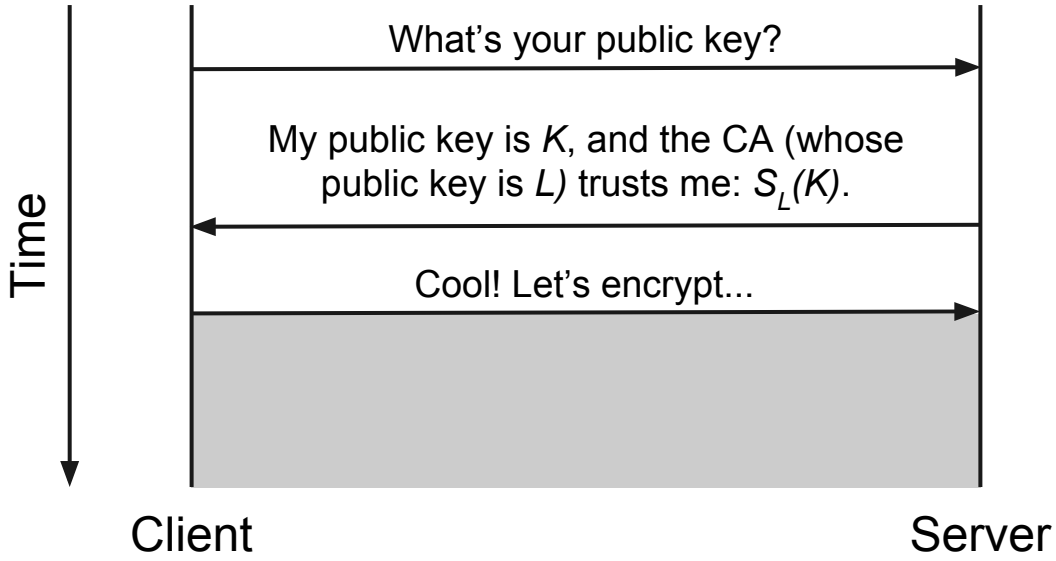
Certificate Authority System

- Man-in-the-Middle!



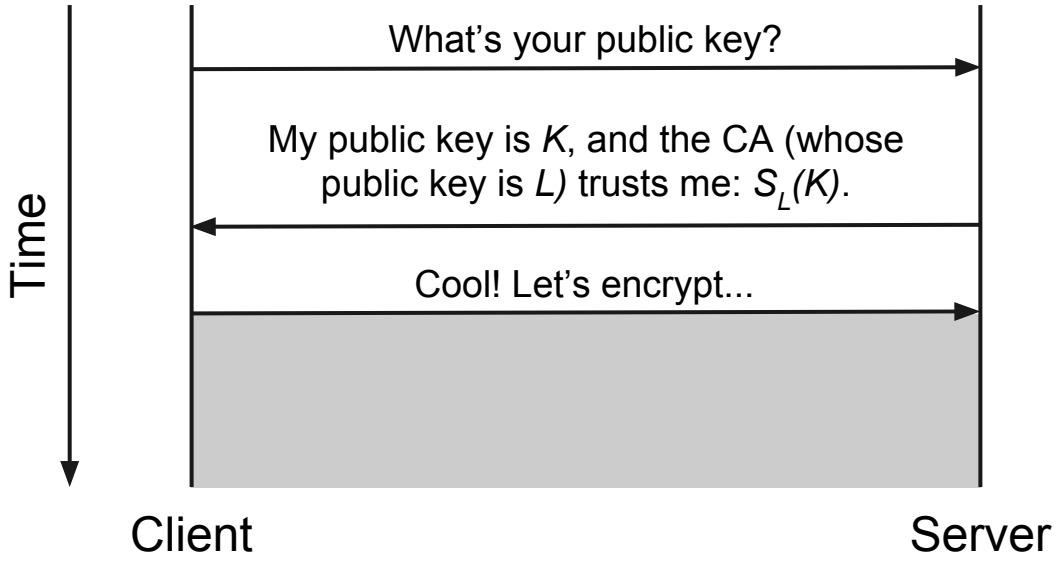
Certificate Authority System

- Second attempt: trusted “certificate authority” verifies



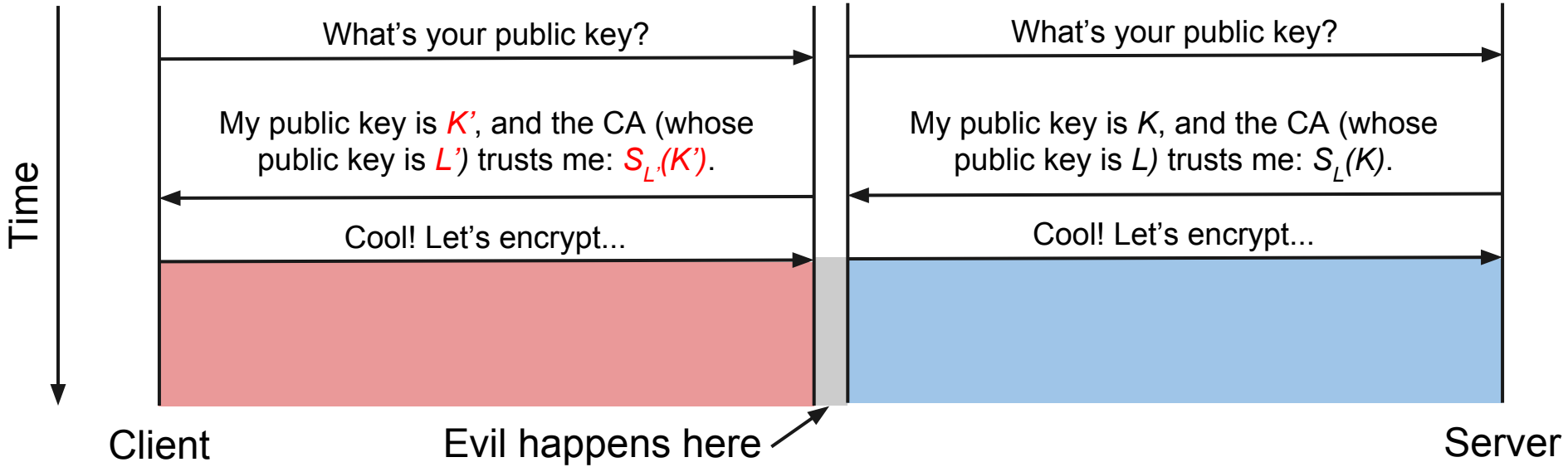
Certificate Authority System

- What could go wrong?



Certificate Authority System

- Man-in-the-Middle!



Certificate Authority System

- Clearly this will go on forever…
- Is there a way to solve this problem?

Certificate Authority System

- The answer: Root CAs
- Know the root CAs' certificates ahead of time
- Root CA -> CA A -> CA B -> … -> Website
- Trust is *transitive*, but very limited in scope

Certificate Authority System

- The answer: Root CAs
- Know the root CAs' certificates ahead of time
- Root CA -> CA A -> CA B -> … -> Website
- Trust is *transitive*, but very limited in scope
- What could go wrong?

Certificate Authority System

- 2011: Dutch CA DigiNotar compromised
  - Attackers stole private keys
  - Forged fake certificates (including for *.google.com)
- Was DigiNotar trustworthy?
- Were the CAs that trusted them trustworthy?

Certificate Authority System

- 2015: Lenovo shipped a fake root certificate from the advertising company Superfish
- Advertisers could inject advertising into pages, the computer would raise no alarms
- Basically, a Man-in-the-Middle attack
- Is there any way to avoid trusting Lenovo?

Certificate Authority System

- The NSA performs *interdiction*
  - Intercepts packages in shipping
  - Modifies them
  - Sends them on their way
- Could easily install fake root certificates
  - In practice, it's often hardware bugs or malware
- Is there any way to avoid trusting UPS, etc?

Certificate Authority System

- 10-Second Plug
- Let's Encrypt is a free CA
  - Started by EFF, Mozilla, others
- Makes setting up HTTPS very easy
- If you run a website, you should do it!

Fin

- Next time: computer security and trust