Computer Security and Privacy: A Taste of Attacks and Defenses

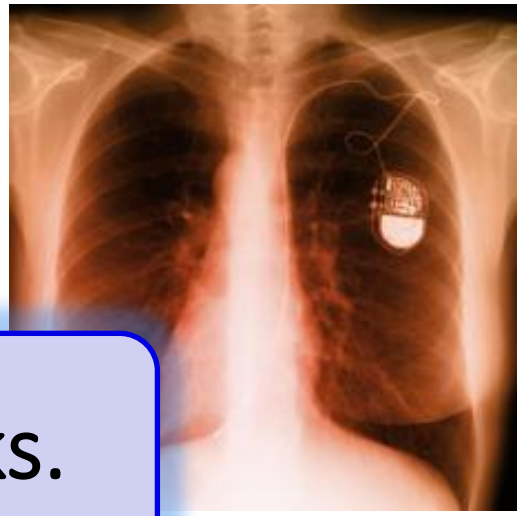
Franziska (Franzi) Roesner

franzi@cs.washington.edu

Associate Professor
Paul G. Allen School
University of Washington

SECURITY & PRIVACY
RESEARCH LAB
UNIVERSITY OF WASHINGTON

New technologies bring new benefits…



… but also new risks.

Security & Privacy (Research)

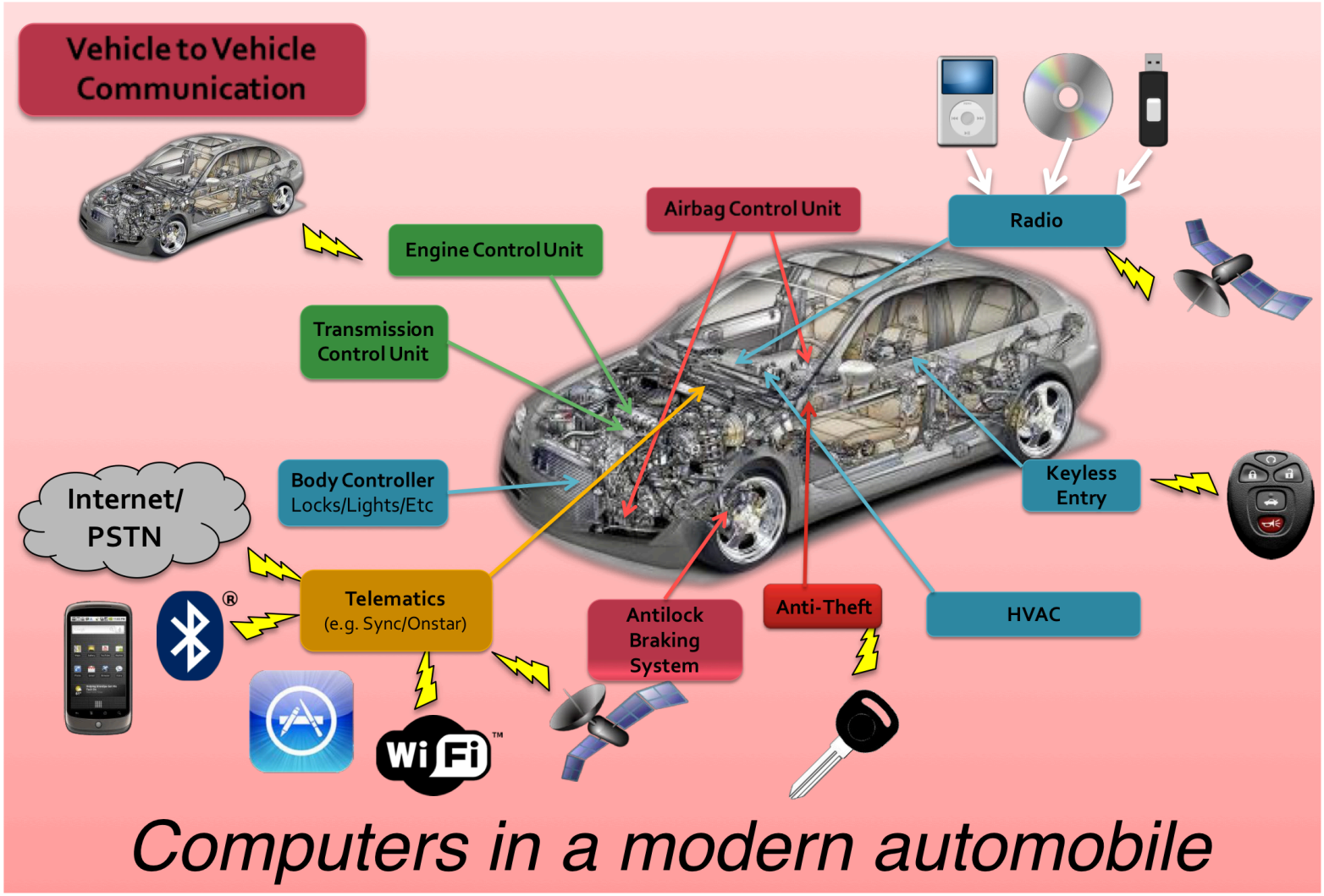
Goal: Improve security & privacy of technologies.

Security mindset: Challenge assumptions, think like an attacker.

Study existing technologies: attack and measure.

Design and build defenses and new technologies.

Example: Modern Automobiles



Exercise: Security Mindset

Assets

(what should be protected)

Adversaries

(possible attackers)

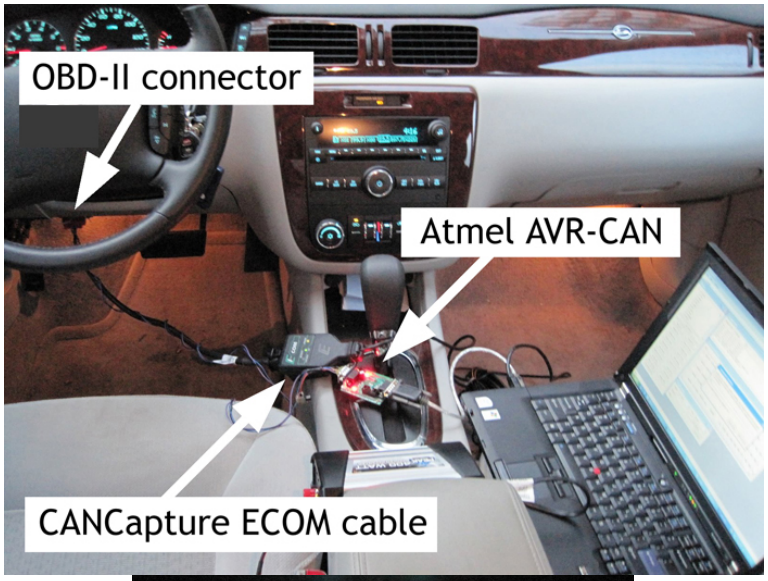
Threats and Vulnerabilities

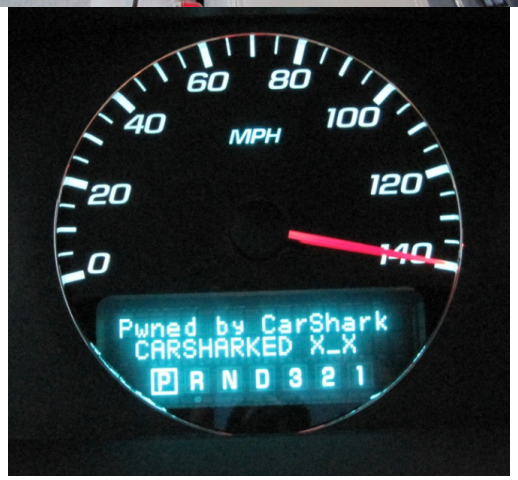
(how an adversary might try to attack the system)

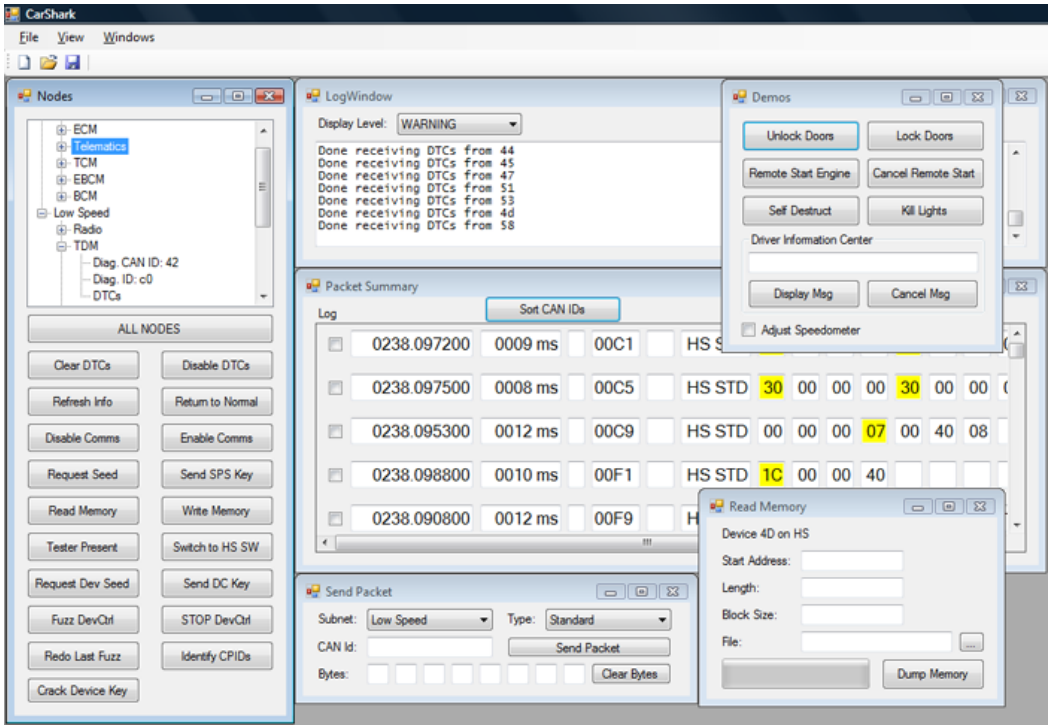
Risk

(how important are assets, how likely are exploits)

We experimented with a real car!







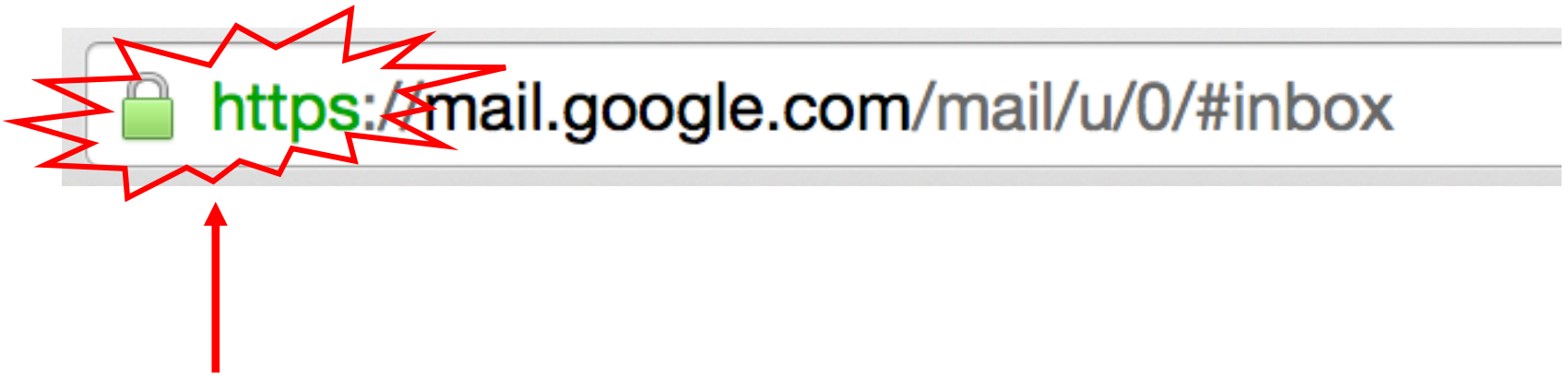
We experimented with a real car!

Example: Force Brakes On

Example: Force Brakes Off

Example: Keyless Theft

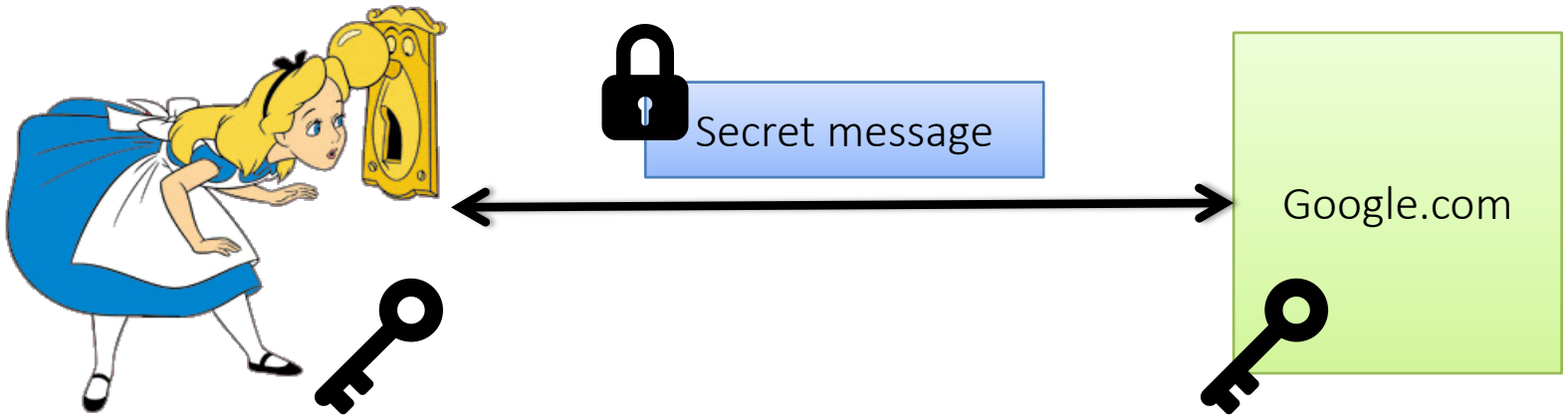
Now for something completely different…



What does this actually mean?

1. Your communication with Google is encrypted.
2. You know you're actually talking to Google *(probably)*.

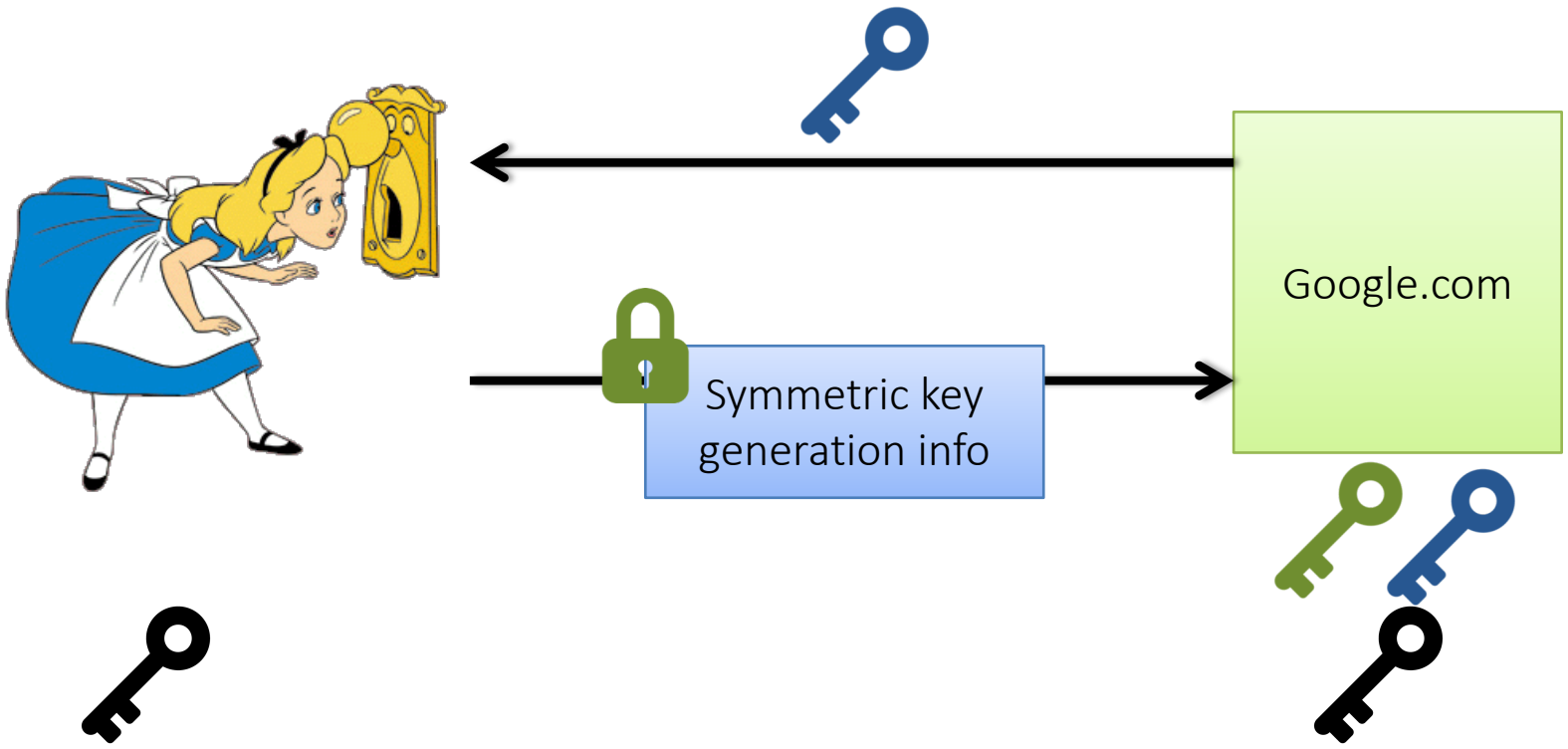
Encryption



How to exchange keys?

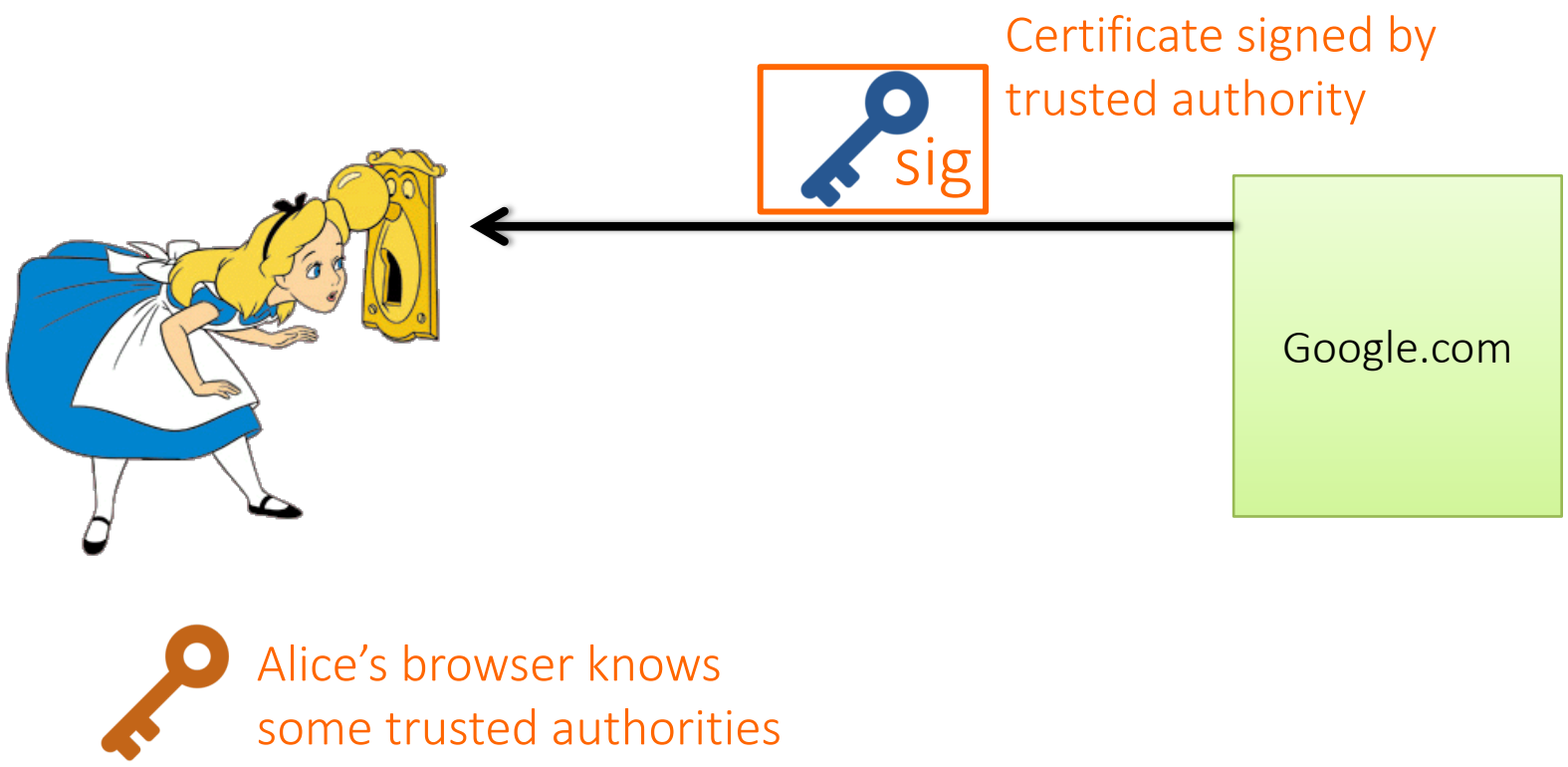
Encryption

Asymmetric (public key) crypto to bootstrap symmetric key

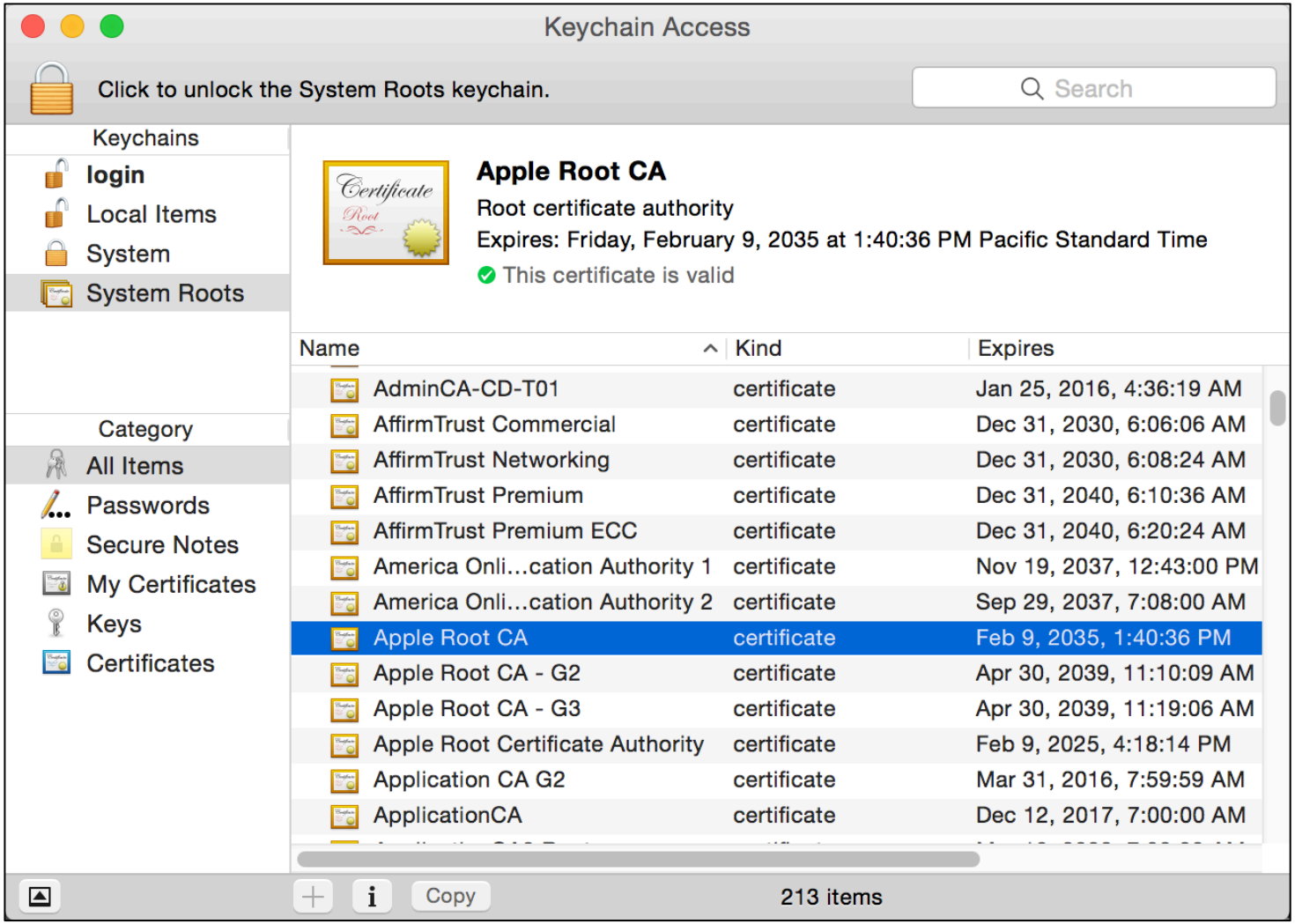


Authentication

How does Alice know this is actually Google?



Trusted(?) Certificate Authorities

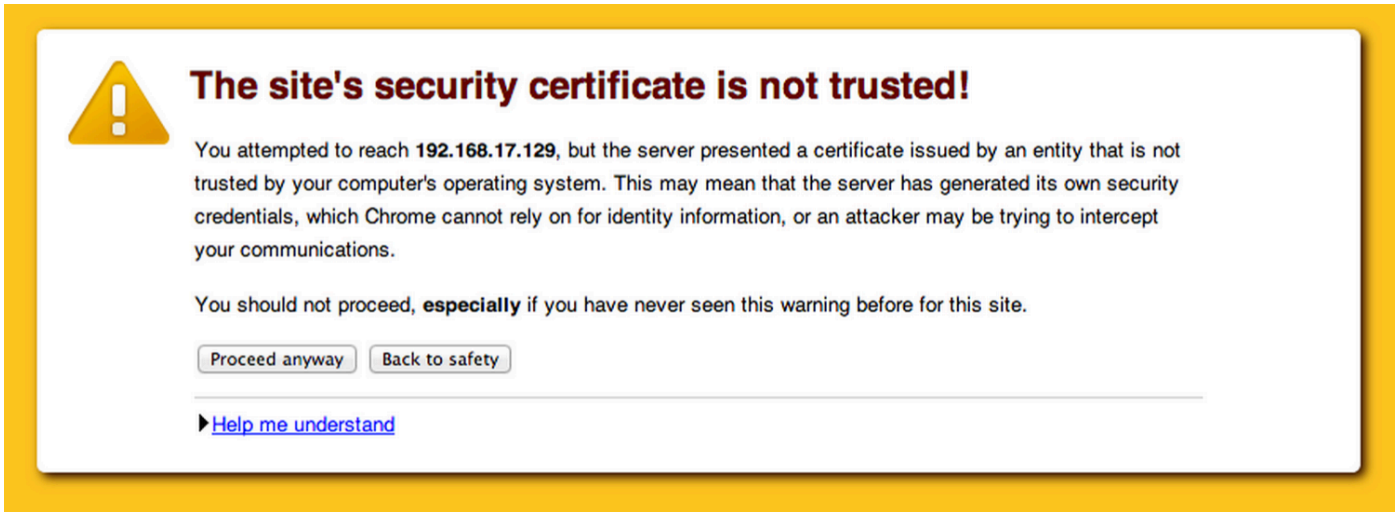


Challenge: Usability

1. People **don’t notice the absence** of a lock icon (when connection is not encrypted)
2. People **ignore browser warnings** (shown when certificate is untrusted)

[Felt et al.]

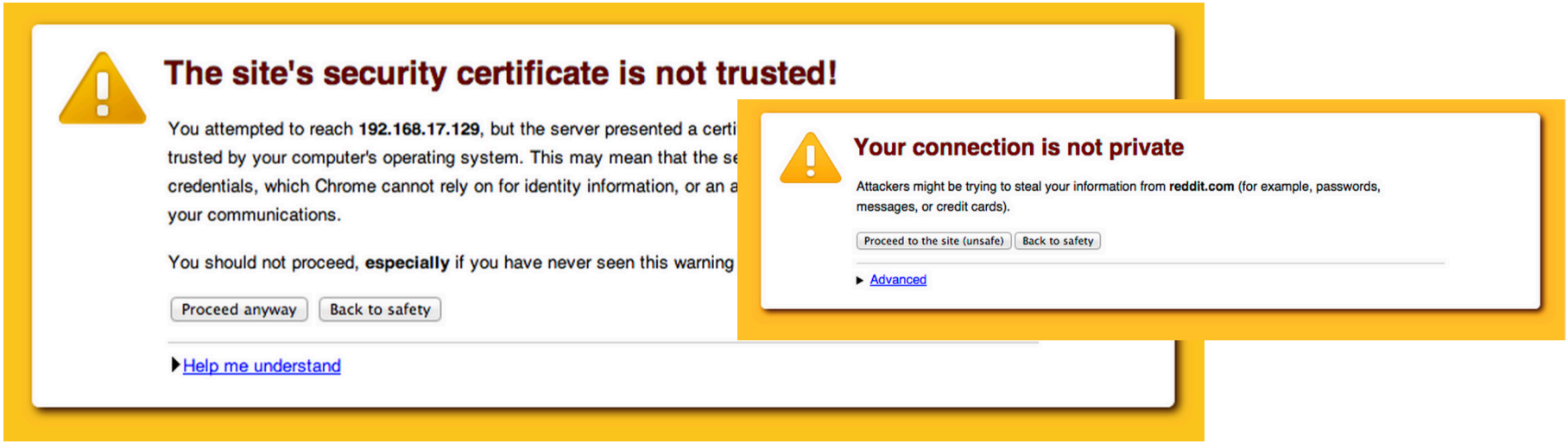
Opinionated Design Helps!

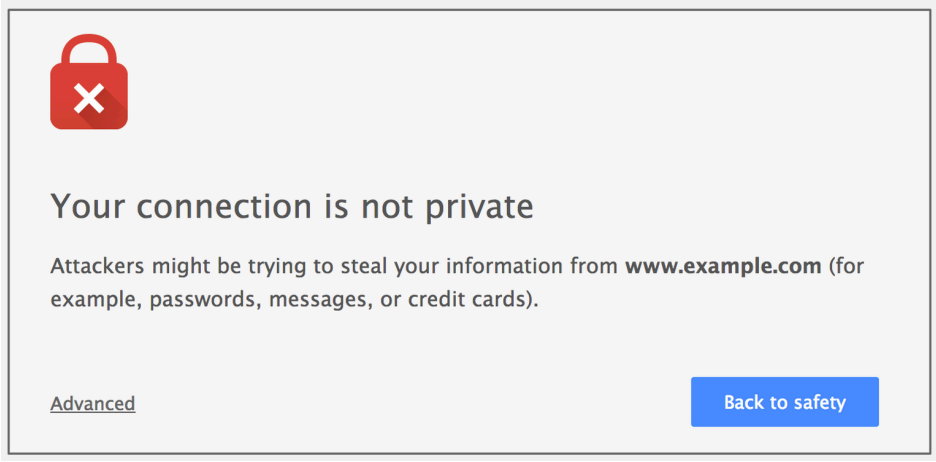


Adherence	N
30.9%	4,551

[Felt et al.]

Opinionated Design Helps!





Adherence	N
30.9%	4,551
32.1%	4,075
58.3%	4,644

Conclusion

- Security mindset: different way of looking at the world; applies not just to technology
- Many aspects of computer security
  - Attacks, Defenses
  - System Design
  - Cryptography
  - Human Factors