

Computer Security: A Taste of Attacks and Defenses

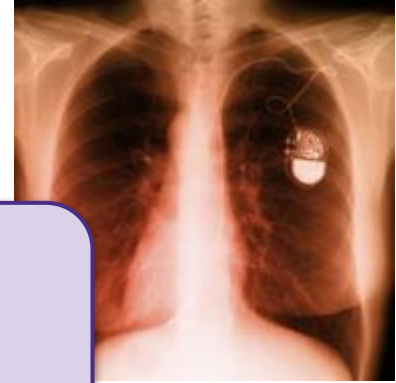
Eric Zeng
ericzeng@cs.washington.edu

Graduate Research Assistant
University of Washington



SECURITY AND PRIVACY
RESEARCH LAB

New technologies bring new benefits...



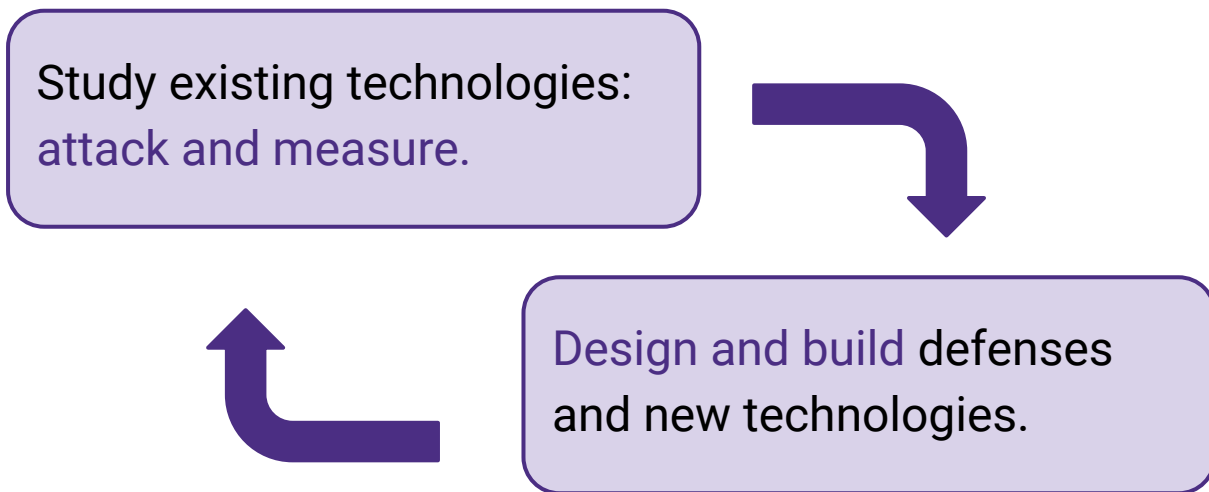
... but also new risks



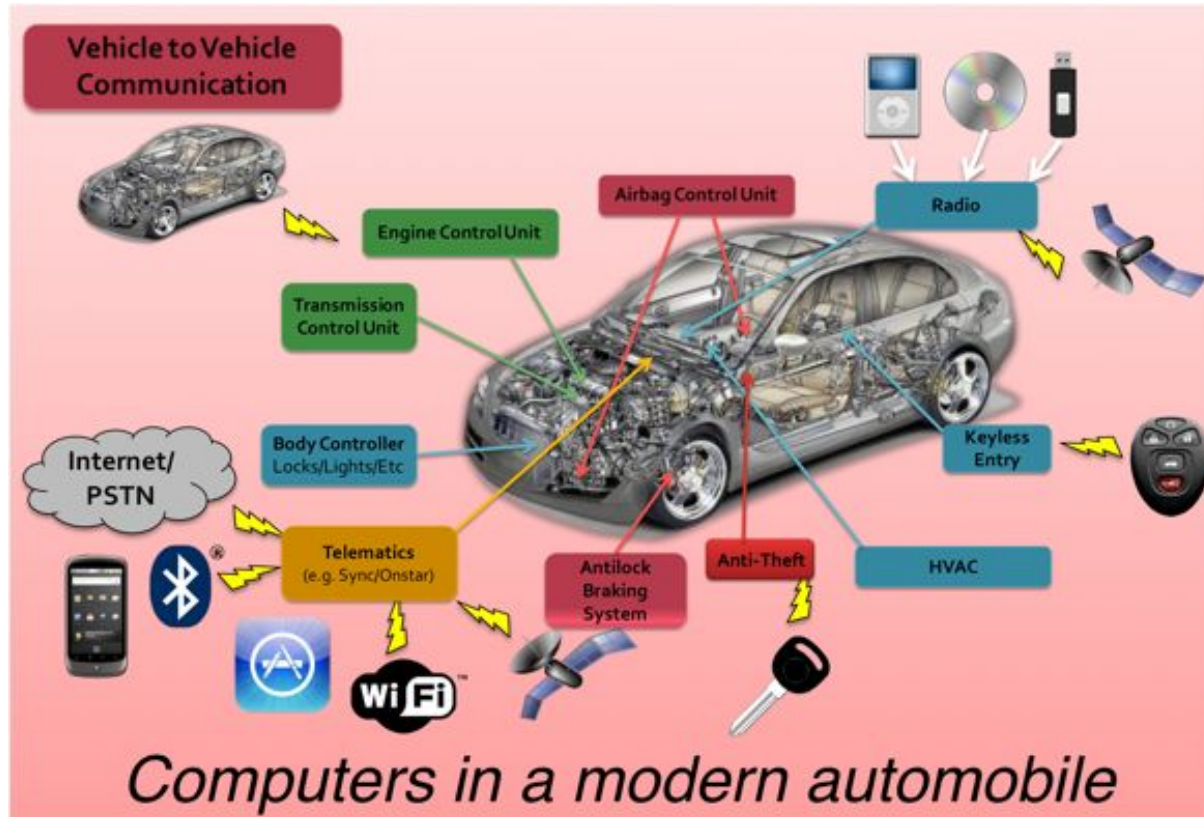
Security and Privacy Research

Goal: Improve the security and privacy of technologies

Security mindset: Challenge assumptions, think like an attacker.



Example: Modern Automobiles



Exercise: Security Mindset

Assets

What should be protected?

Adversaries

Who are possible attackers?

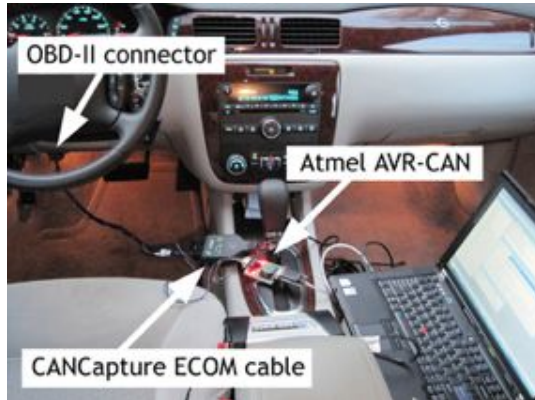
Threats and Vulnerabilities

How might an adversary try to attack the system?

Risk

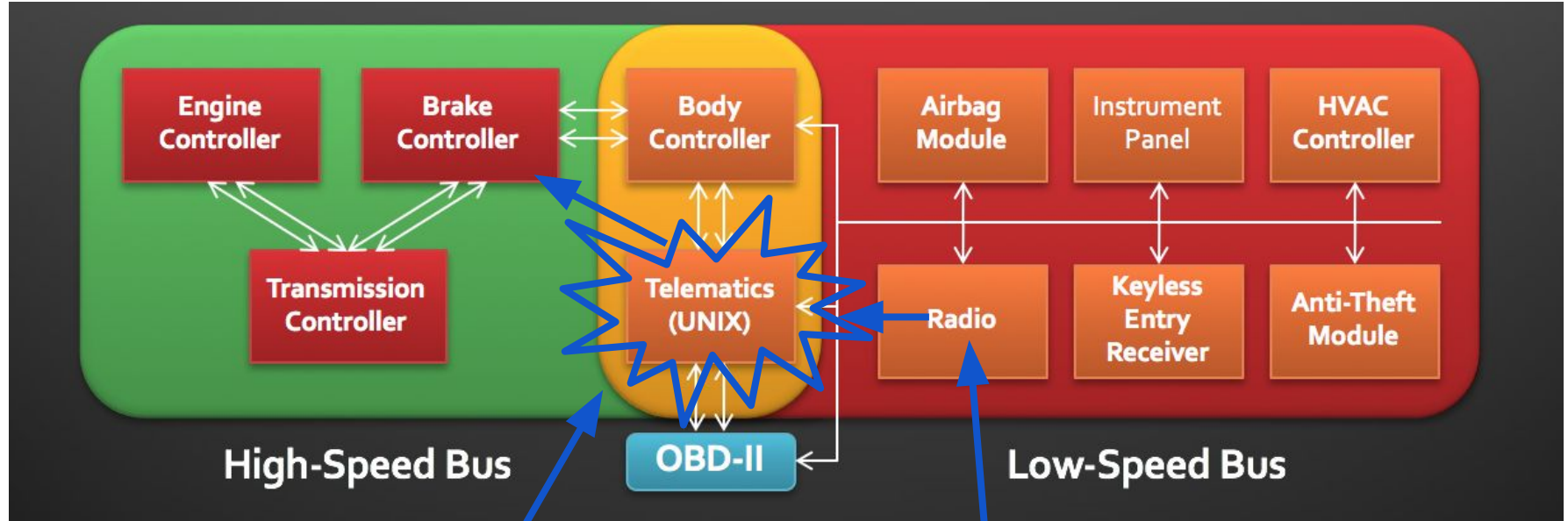
How important are the assets? How likely are the exploits?

Hacking a real car!



How did they do it?

[Checkoway et al. '11]



Long-range wireless attack
(cellular connection)



Physical attack
(malicious CD)

Ethics

What ethical guidelines should you follow when doing security research?

1. Do no harm
2. Don't attack systems unless you have permission
 - ✓ OK if you own it
 - ✓ OK if there is a bug bounty program
3. If you find a vulnerability, disclose it responsibly
 - ✓ Report it to the manufacturer
 - ✗ Don't sell it to hackers



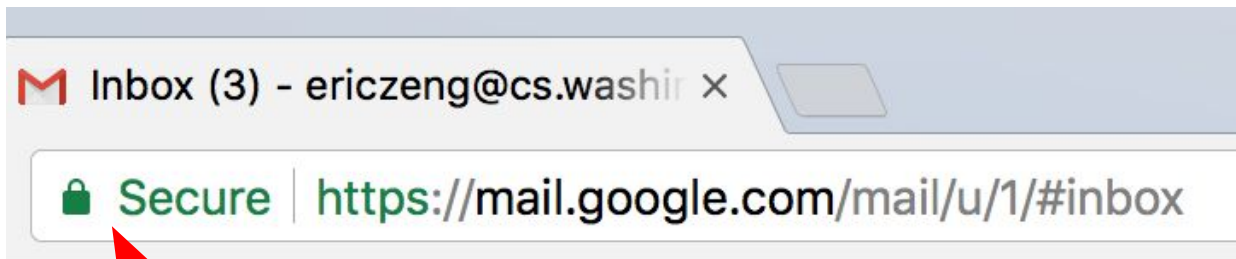
Attacks

In what ways are technologies insecure?

Defenses

How can we make our technology more secure?

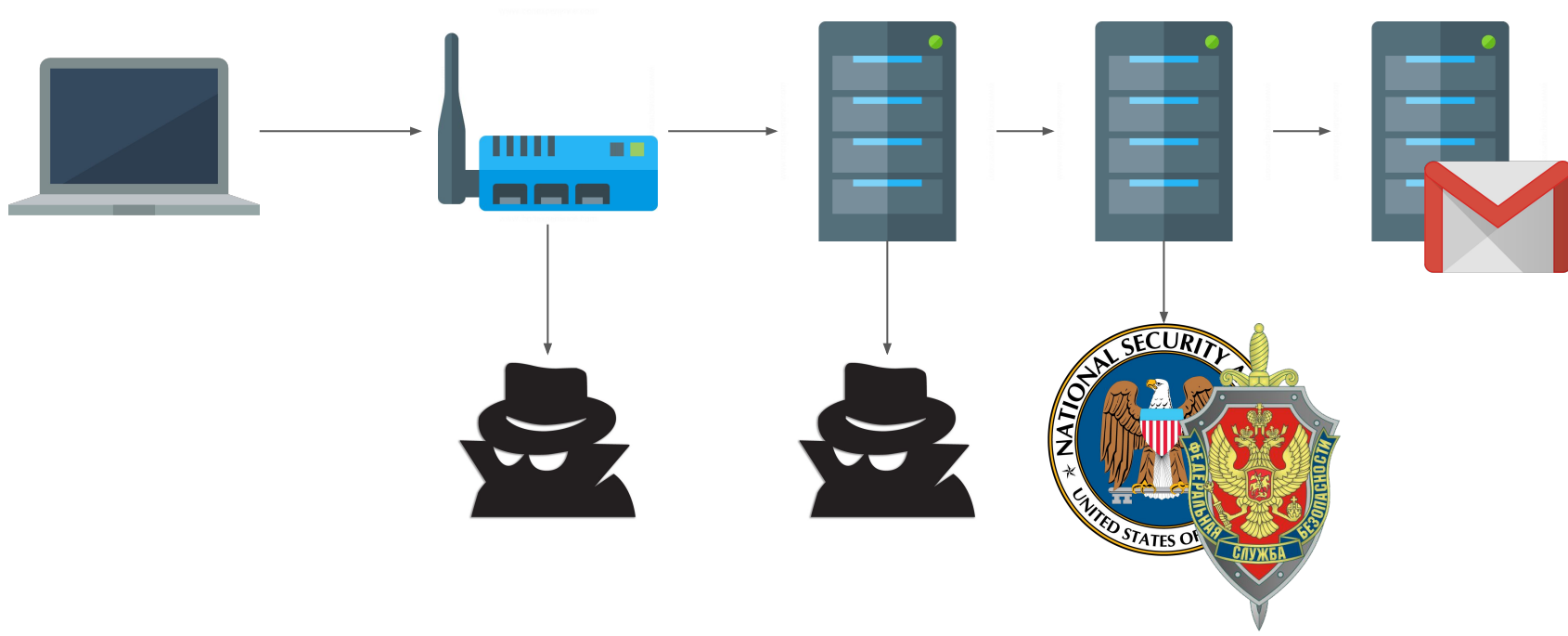
What does the green lock mean?



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

Encryption

Why?



Encryption

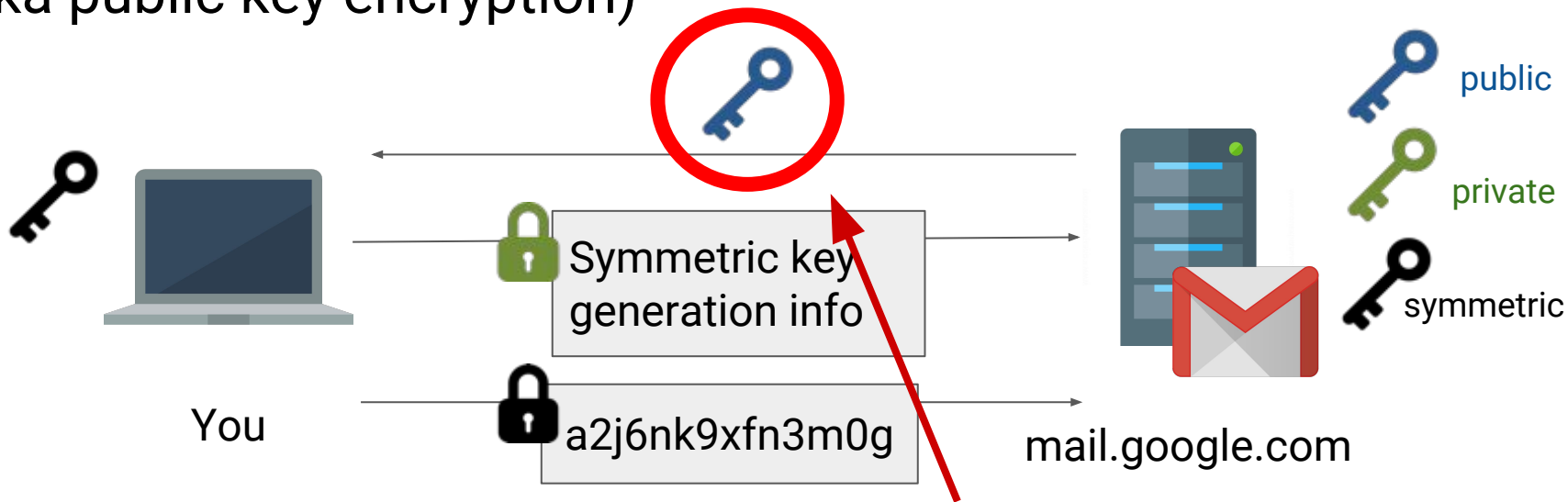
Symmetric key encryption



How do we exchange keys?

Asymmetric Encryption

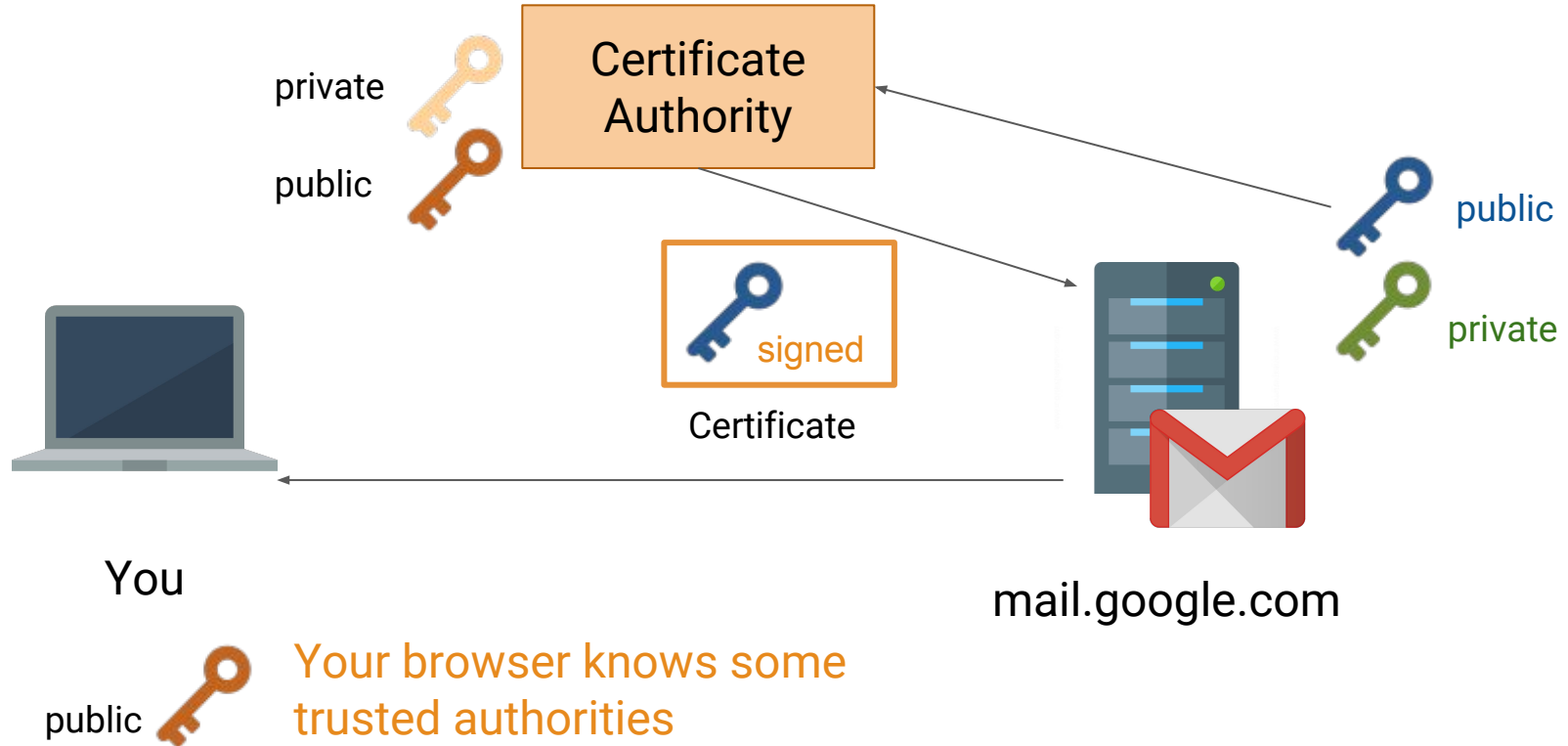
(aka public key encryption)



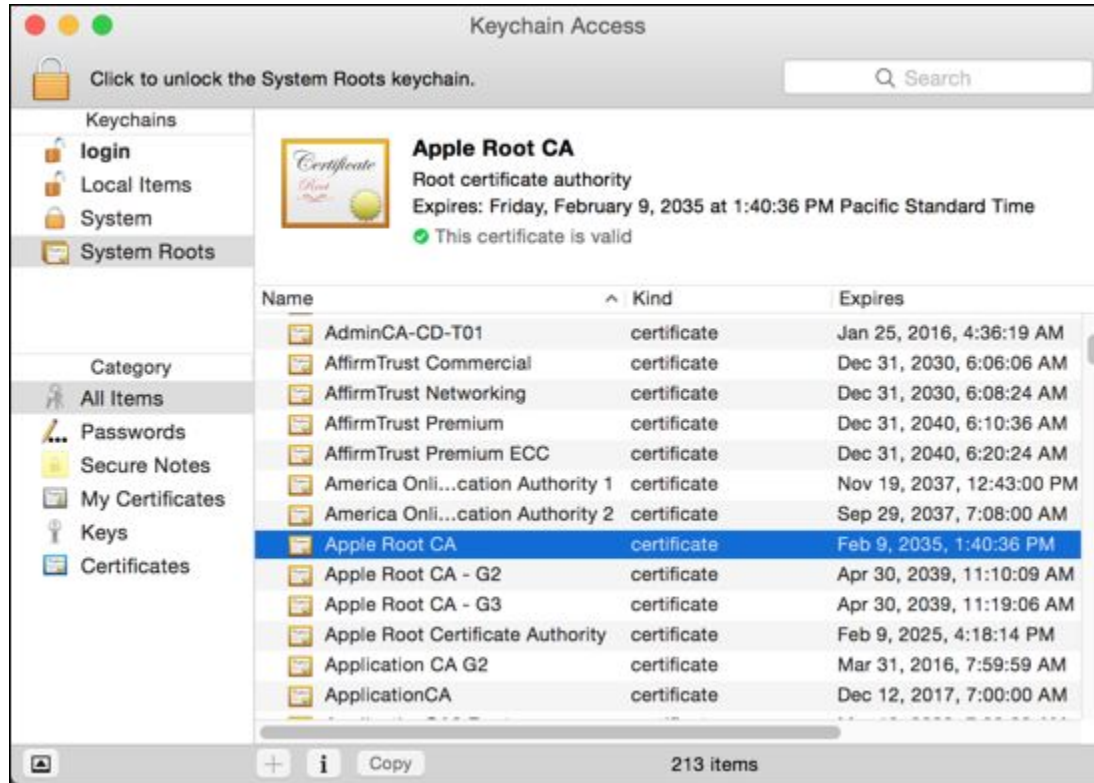
Why not just use public key encryption? It's much slower than symmetric key encryption

How do we know this key is really from Google?

Certificate Authorities



Trusted(?) Certificate Authorities



What if the certificate is bad?

[Felt et al. '15]



The site's security certificate is not trusted!

You attempted to reach **192.168.17.129**, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications.

You should not proceed, **especially** if you have never seen this warning before for this site.

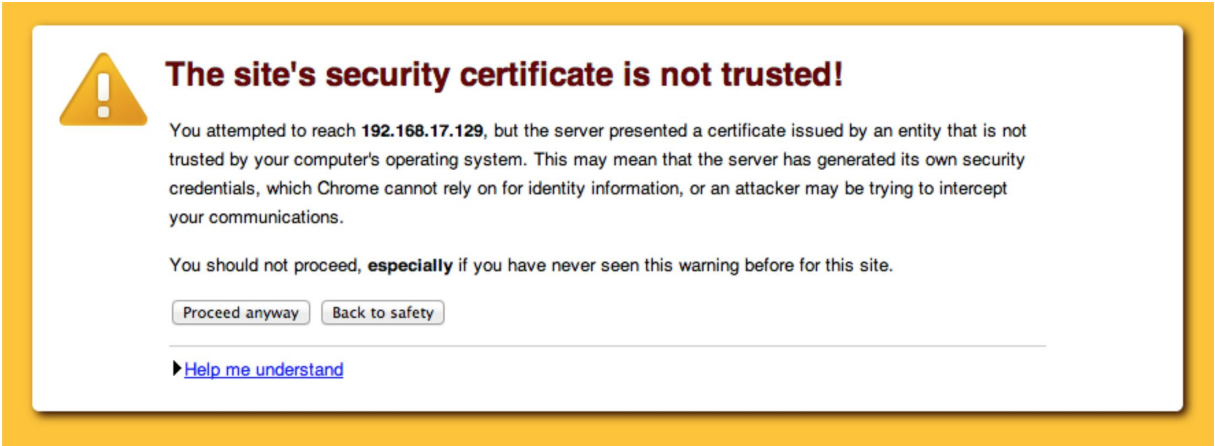
▶ [Help me understand](#)

Problem: 70% of people ignored this warning!

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)

Security Warning Design

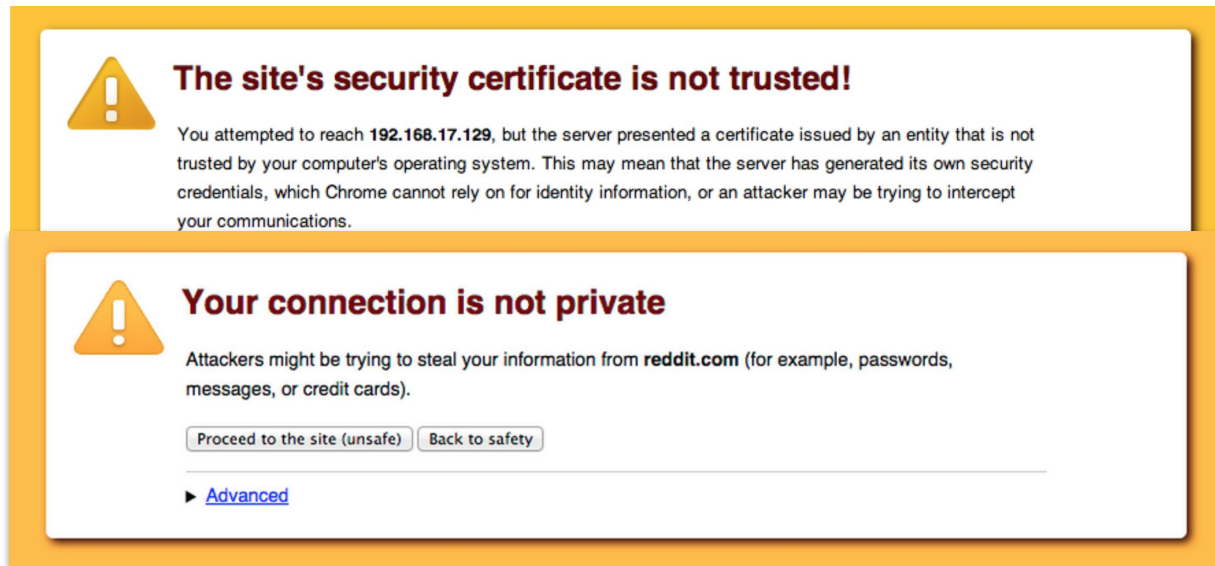


Original Warning (Chrome 36)

Adherence	N
30.9%	4,551

Security Warning Design

[Felt et al. '15]

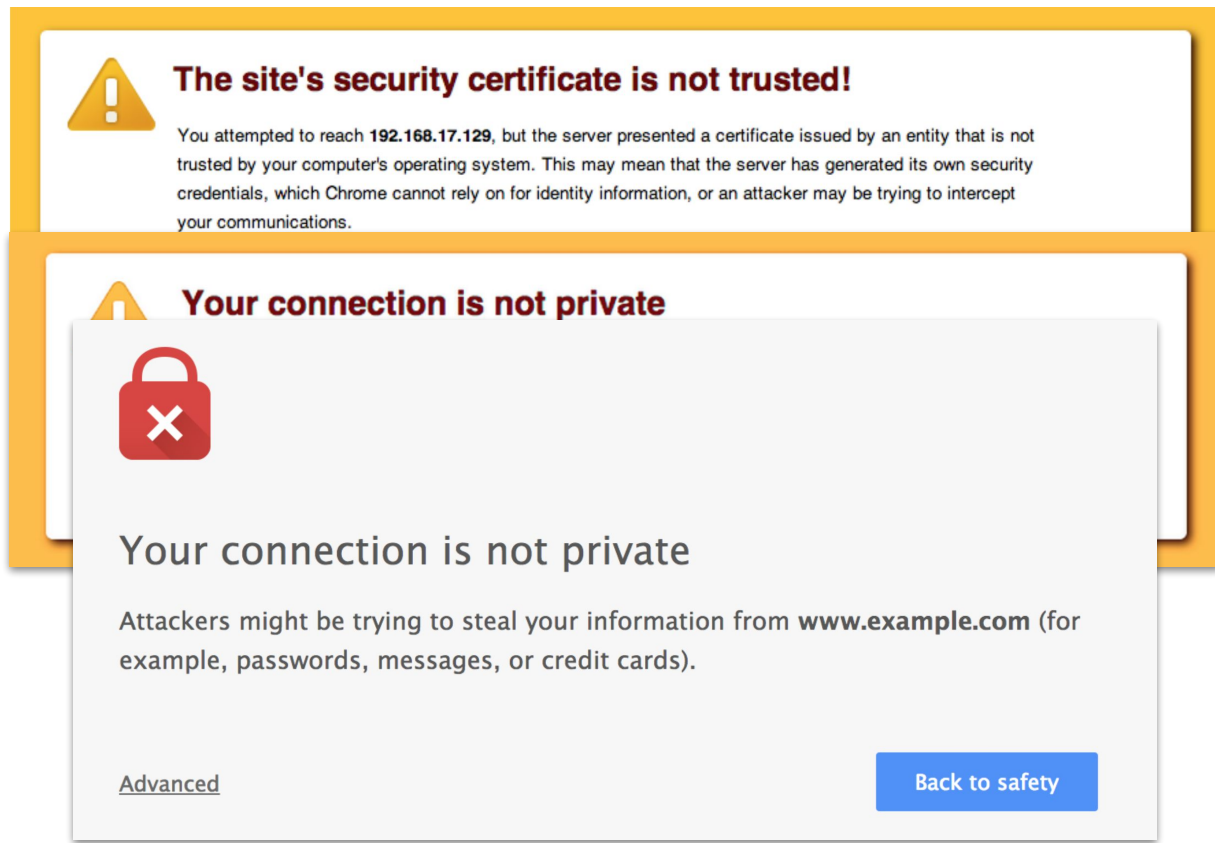


Adherence	N
30.9%	4,551
32.1%	4,075

Less technical jargon

Security Warning Design

[Felt et al. '15]



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

Opinionated Design:
Choice visibility, choice attractiveness

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