Computer Security:
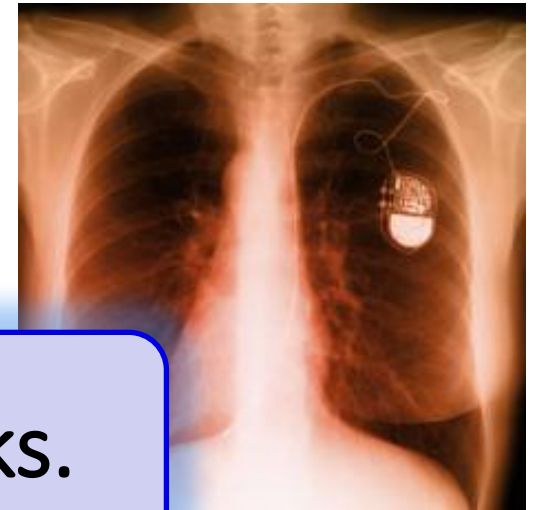# A Taste of Attacks and Defenses

Franziska Roesner

franzi@cs.washington.edu

Assistant Professor
University of Washington

PAUL G. ALLEN SCHOOL
OF COMPUTER SCIENCE & ENGINEERING

SECURITY AND PRIVACY
RESEARCH LAB

UNIVERSITY of WASHINGTON

New technologies bring new benefits...

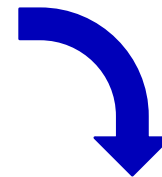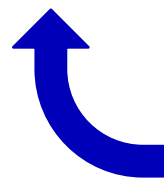... but also new risks.

Security & Privacy Research

Goal: Improve security & privacy of technologies.

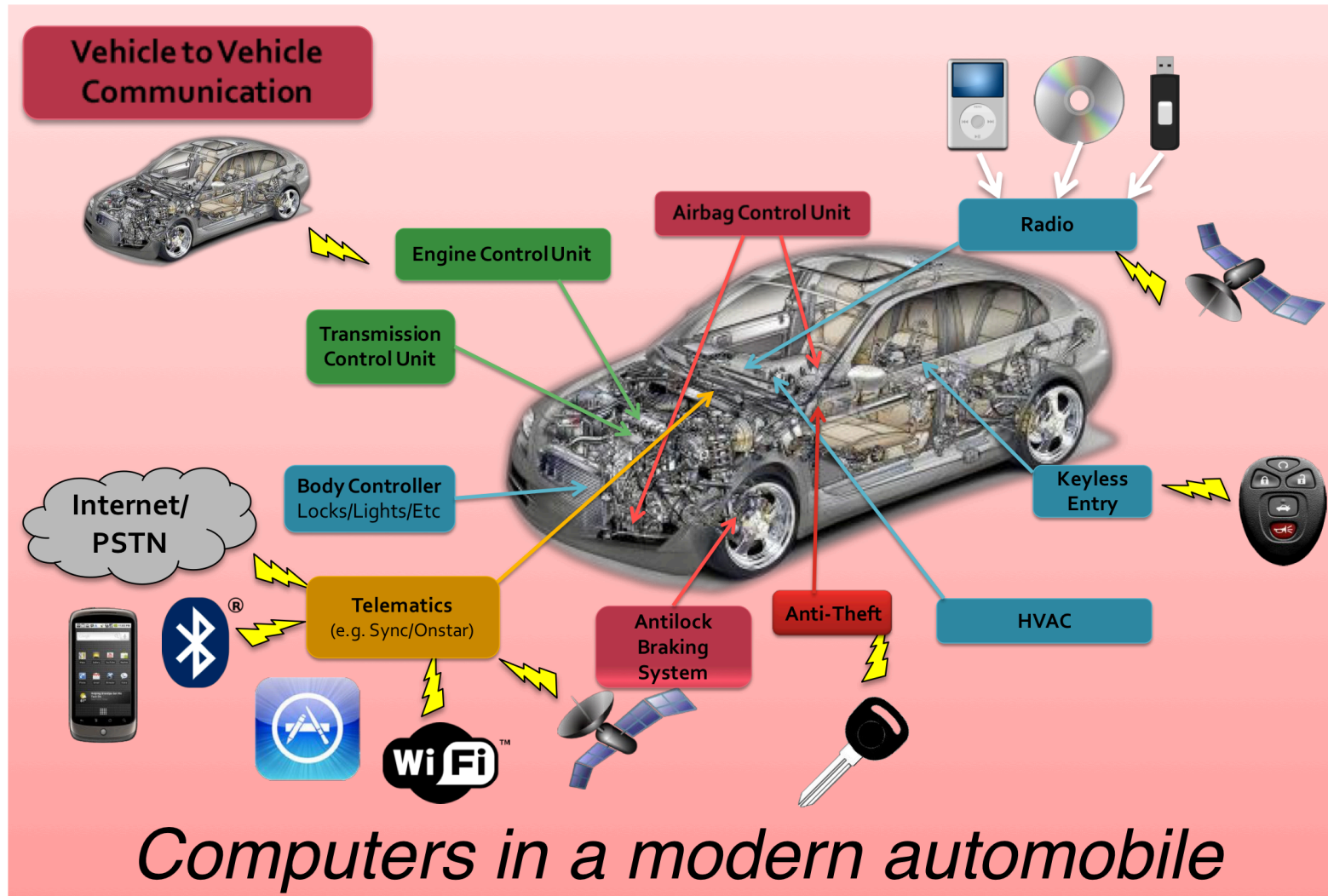**Security mindset:** Challenge assumptions, think like an attacker.

Study existing technologies: attack and measure.

Design and build defenses and new technologies.

Example: Modern Automobiles

Computers in a modern automobile

Exercise: Security Mindset

Assets
(what should be protected)
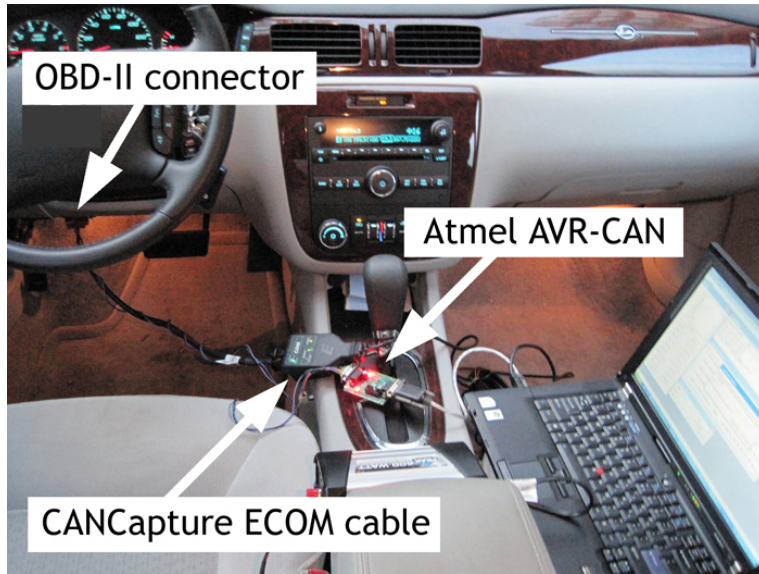
Adversaries
(possible attackers)

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

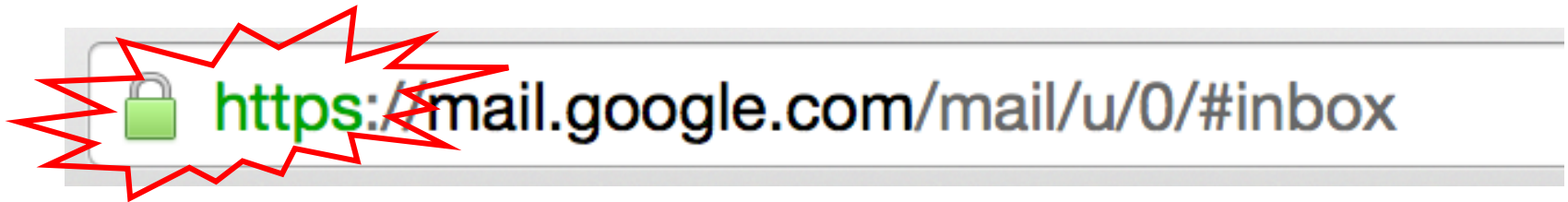Engaging Brakes At 20 MPH

Example: Force Brakes Off

Disabling Brakes At 20 MPH

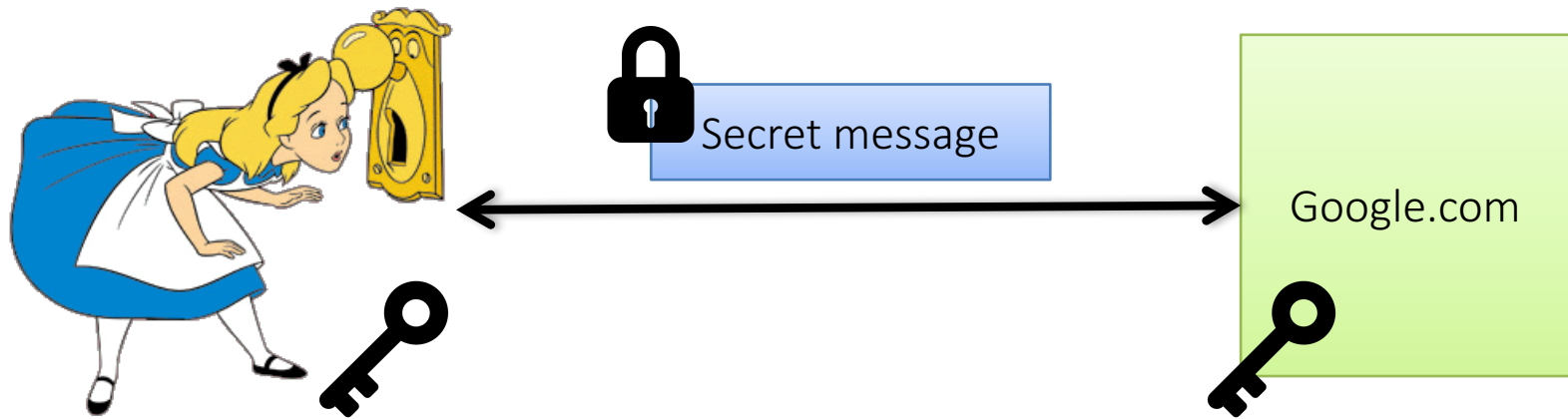# Example: Keyless Theft

Now for something completely different...

What does this actually mean?

1. Your communication with Google is encrypted.

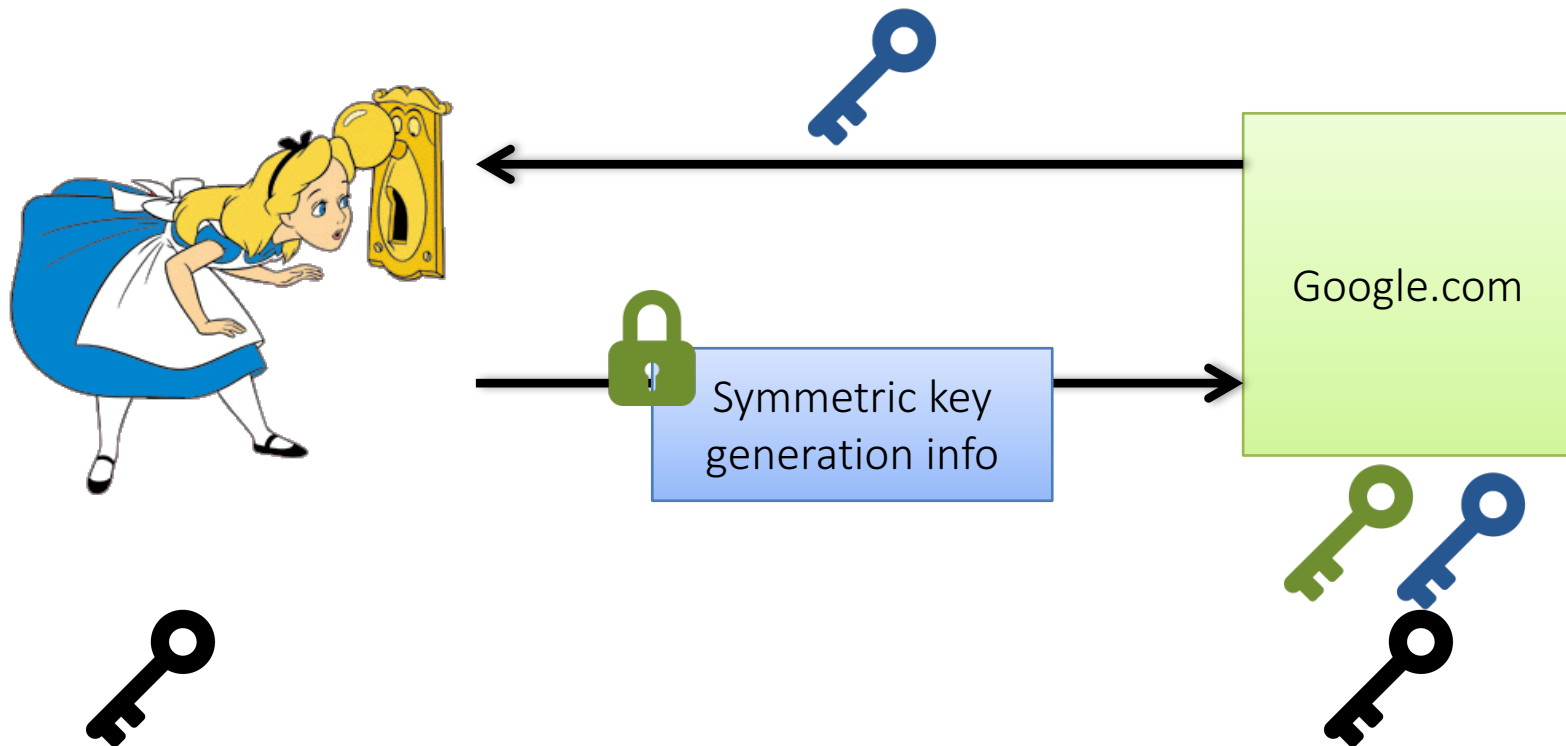2. You know you're actually talking to Google *(probably)*.

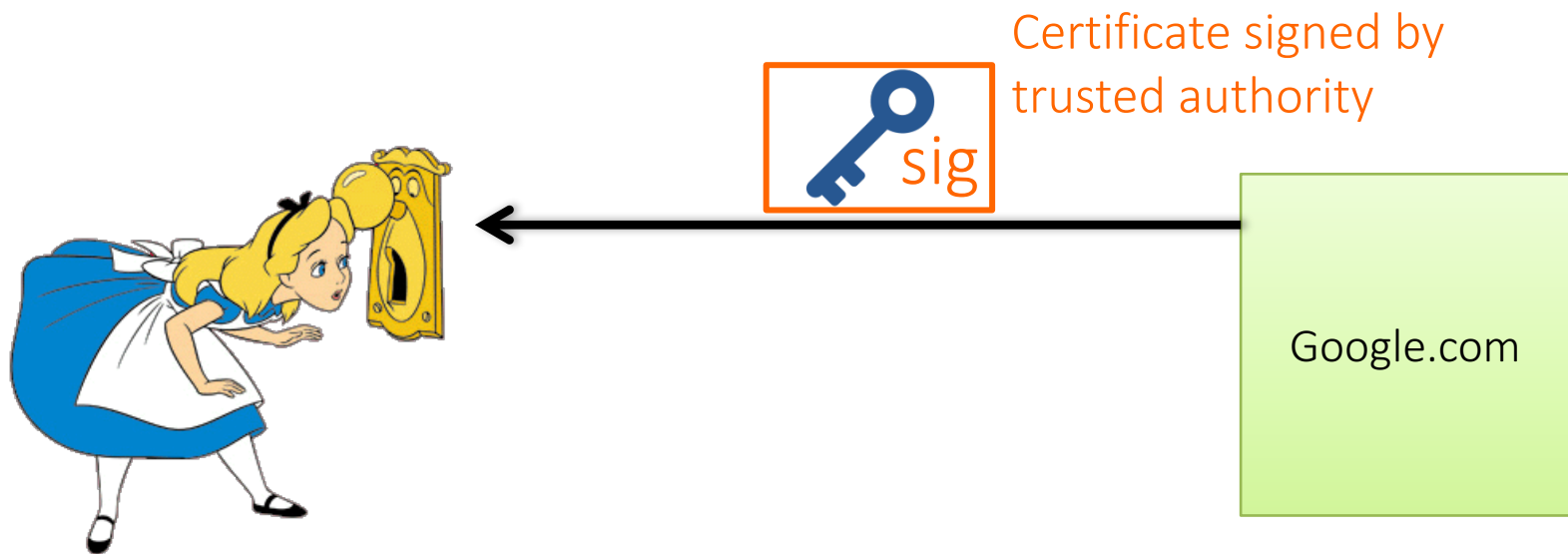# Encryption

Secret message

Google.com

How to exchange keys?

Encryption

Asymmetric (public key) crypto to bootstrap symmetric key

Authentication

How does Alice know this is actually Google?

Certificate signed by trusted authority

sig

Google.com

Alice's browser knows some trusted authorities

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)

Opinionated Design Helps!

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.

[Proceed anyway] [Back to safety]

▶Help me understand

Adherence	N
30.9%	4,551

Opinionated Design Helps!

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.

[Proceed anyway] [Back to safety]

▶Help me understand

Adherence	N
30.9%	4,551

Opinionated Design Helps!

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