

Computer Security and Privacy: A Taste of Attacks and Defenses

Franziska (Franzi) Roesner

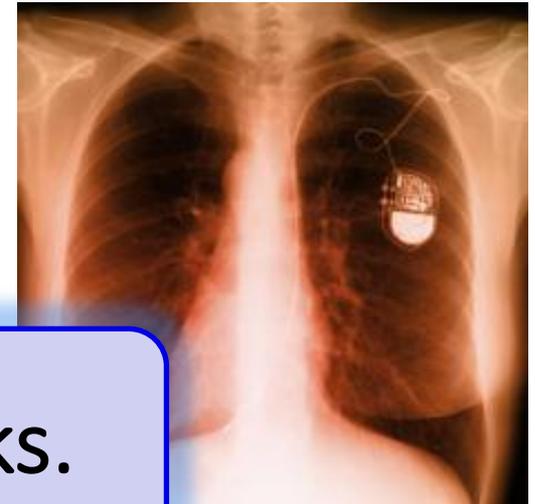
franzi@cs.washington.edu

*Associate Professor
Paul G. Allen School
University of Washington*

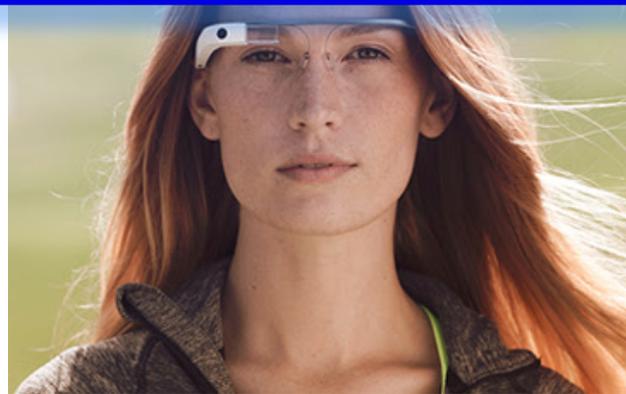


SECURITY & PRIVACY
— RESEARCH LAB —
UNIVERSITY OF WASHINGTON

New technologies bring new benefits...



... but also new risks.



Security & Privacy (Research)

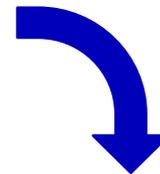
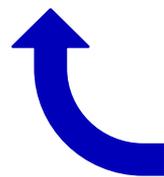
Goal: Improve security & privacy of technologies.

Security mindset: Challenge assumptions, think like an attacker.

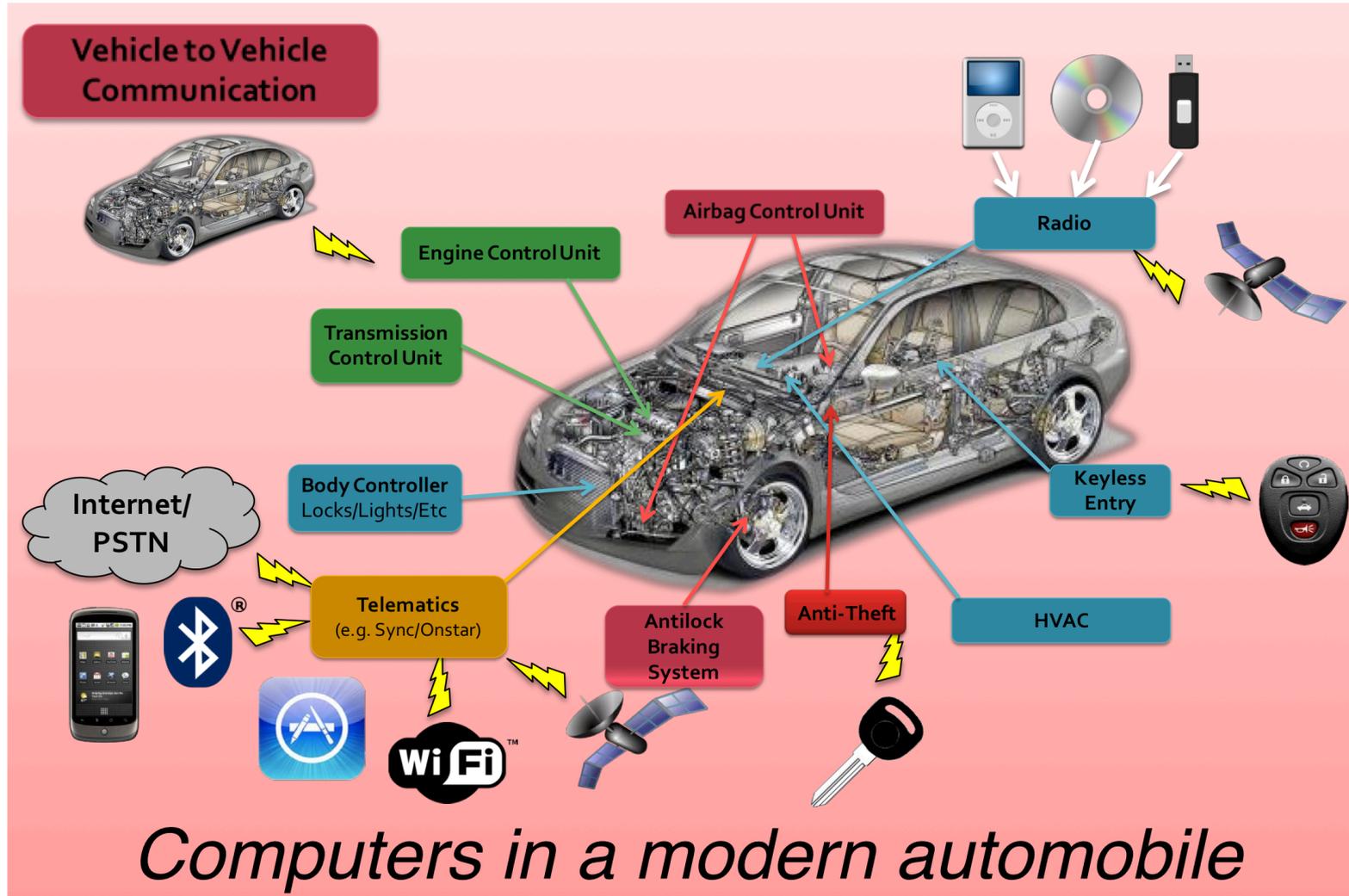


Study existing technologies:
attack and measure.

Design and build defenses
and new technologies.



Example: Modern Automobiles



Exercise: Security Mindset

Assets

(what should be protected)

Adversaries

(possible attackers)

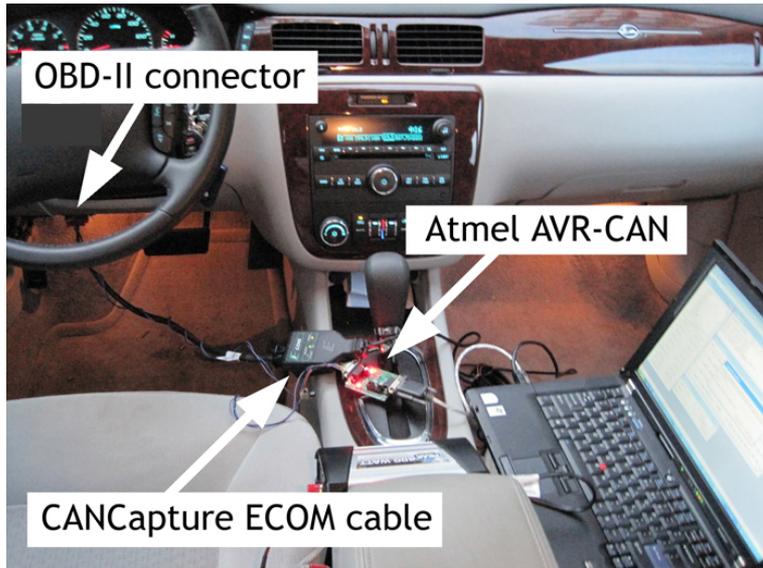
Threats and Vulnerabilities

(how an adversary might try to attack the system)

Risk

(how important are assets, how likely are exploits)

We experimented with a real car!



CarShark

File View Windows

Nodes

- ECM
- Telematics
- TCM
- EBCM
- BCM
- Low Speed
- Radio
- TDM

Diag. CAN ID: 42
Diag. ID: c0
DTCs

ALL NODES

Clear DTCs Disable DTCs
Refresh Info Return to Normal
Disable Comms Enable Comms
Request Seed Send SPS Key
Read Memory Write Memory
Tester Present Switch to HS SW
Request Dev Seed Send DC Key
Fuzz DevCtrl STOP DevCtrl
Redo Last Fuzz Identify CPIDs
Crack Device Key

LogWindow

Display Level: WARNING

Done receiving DTCs from 44
Done receiving DTCs from 45
Done receiving DTCs from 47
Done receiving DTCs from 51
Done receiving DTCs from 53
Done receiving DTCs from 4d
Done receiving DTCs from 58

Packet Summary

Log

Log	Sort CAN IDs
<input type="checkbox"/> 0238.097200	0009 ms 00C1 HS S
<input type="checkbox"/> 0238.097500	0008 ms 00C5 HS STD 30 00 00 00 30 00 00
<input type="checkbox"/> 0238.095300	0012 ms 00C9 HS STD 00 00 00 07 00 40 08
<input type="checkbox"/> 0238.098800	0010 ms 00F1 HS STD 1C 00 00 40
<input type="checkbox"/> 0238.090800	0012 ms 00F9 H

Send Packet

Subnet: Low Speed Type: Standard

CAN Id: Send Packet

Bytes: Clear Bytes

Demos

Unlock Doors Lock Doors
Remote Start Engine Cancel Remote Start
Self Destruct Kill Lights
Driver Information Center
Display Msg Cancel Msg
Adjust Speedometer

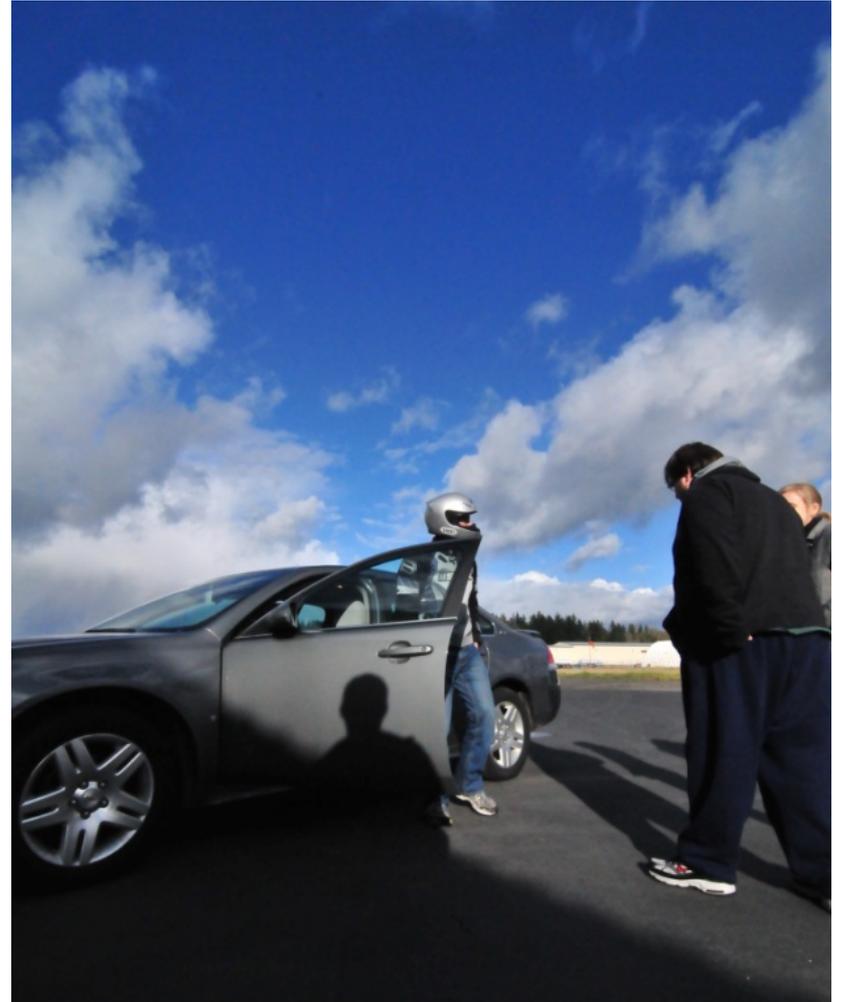
Read Memory

Device 4D on HS
Start Address: Length: Block Size: File: Dump Memory

The screenshot shows the CarShark software interface. It features a 'Nodes' tree on the left with 'Telematics' selected. Below it are various control buttons like 'Clear DTCs', 'Refresh Info', and 'Request Seed'. The 'LogWindow' displays a list of received DTCs with their IDs, times, and codes. The 'Packet Summary' section shows a table of CAN packets with their IDs, times, and data. The 'Send Packet' section allows for sending custom packets. On the right, there are 'Demos' buttons for actions like 'Unlock Doors' and 'Remote Start Engine', and a 'Read Memory' dialog box.



We experimented with a real car!



Example: Force Brakes On



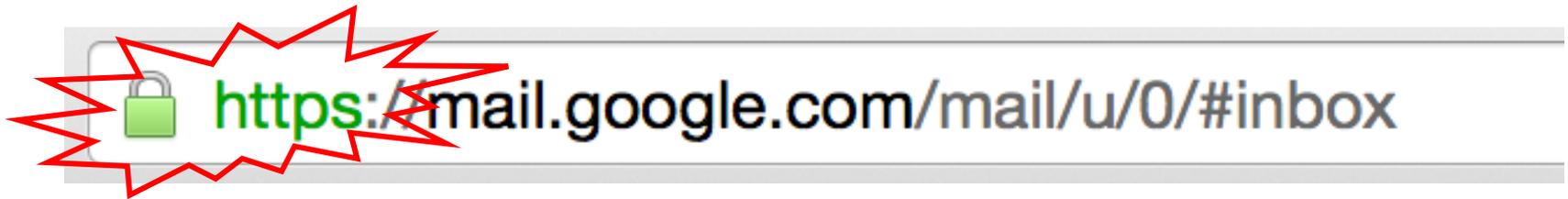
Example: Force Brakes Off



Example: Keyless Theft



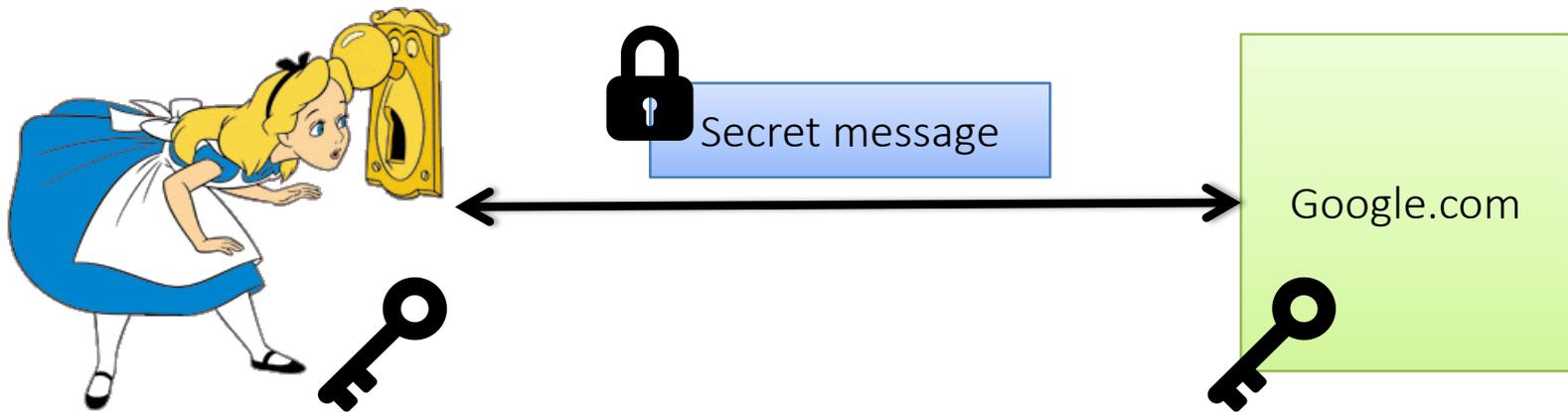
Now for something completely different...



What does this actually mean?

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

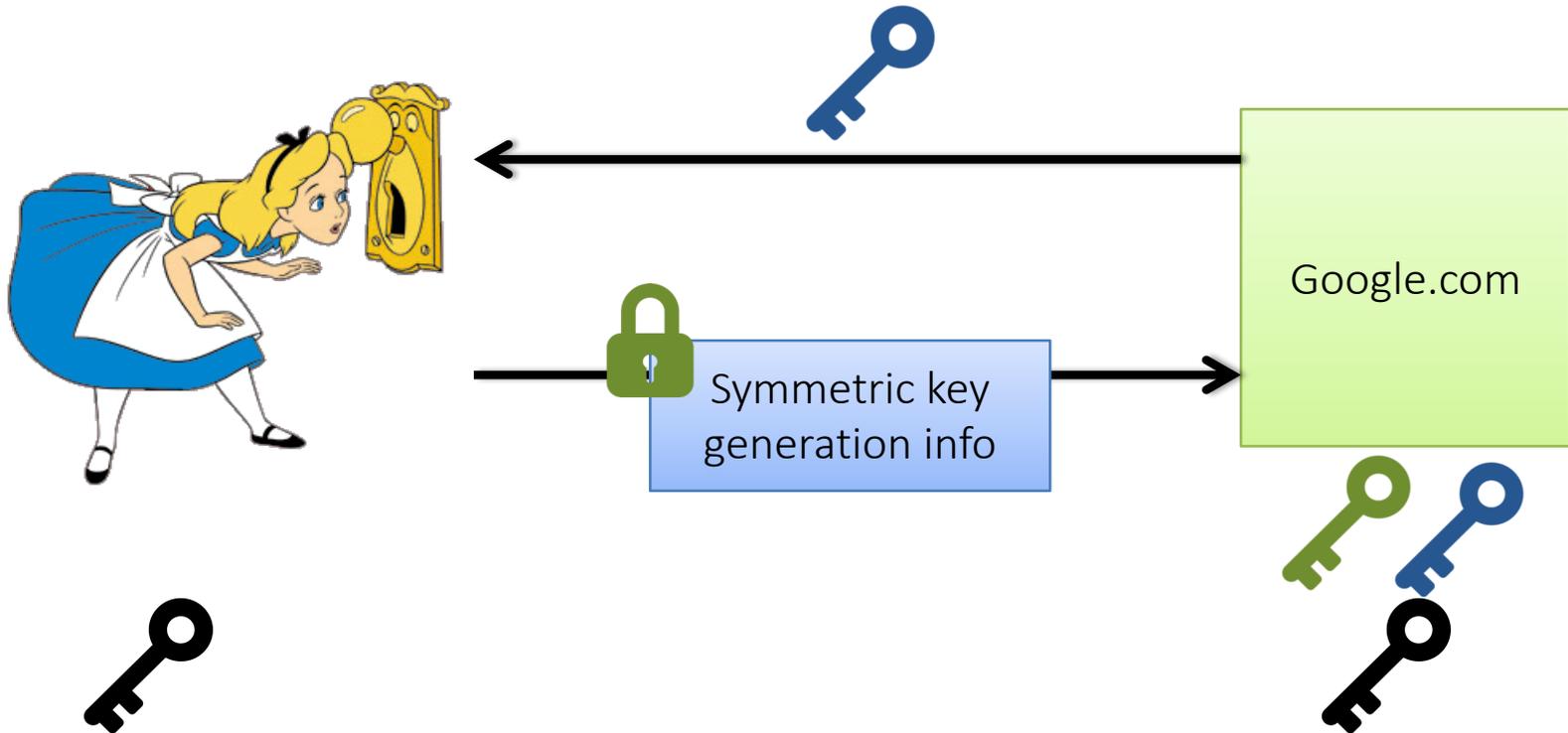
Encryption



How to exchange keys?

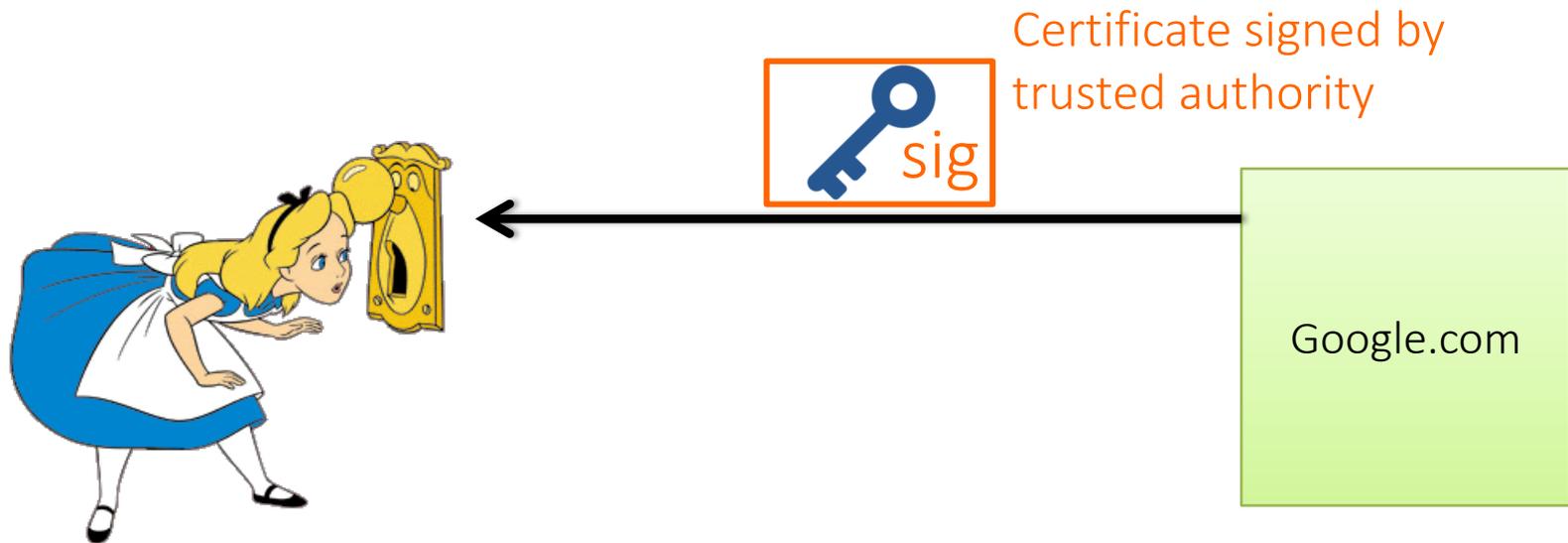
Encryption

Asymmetric (public key) crypto to bootstrap symmetric key



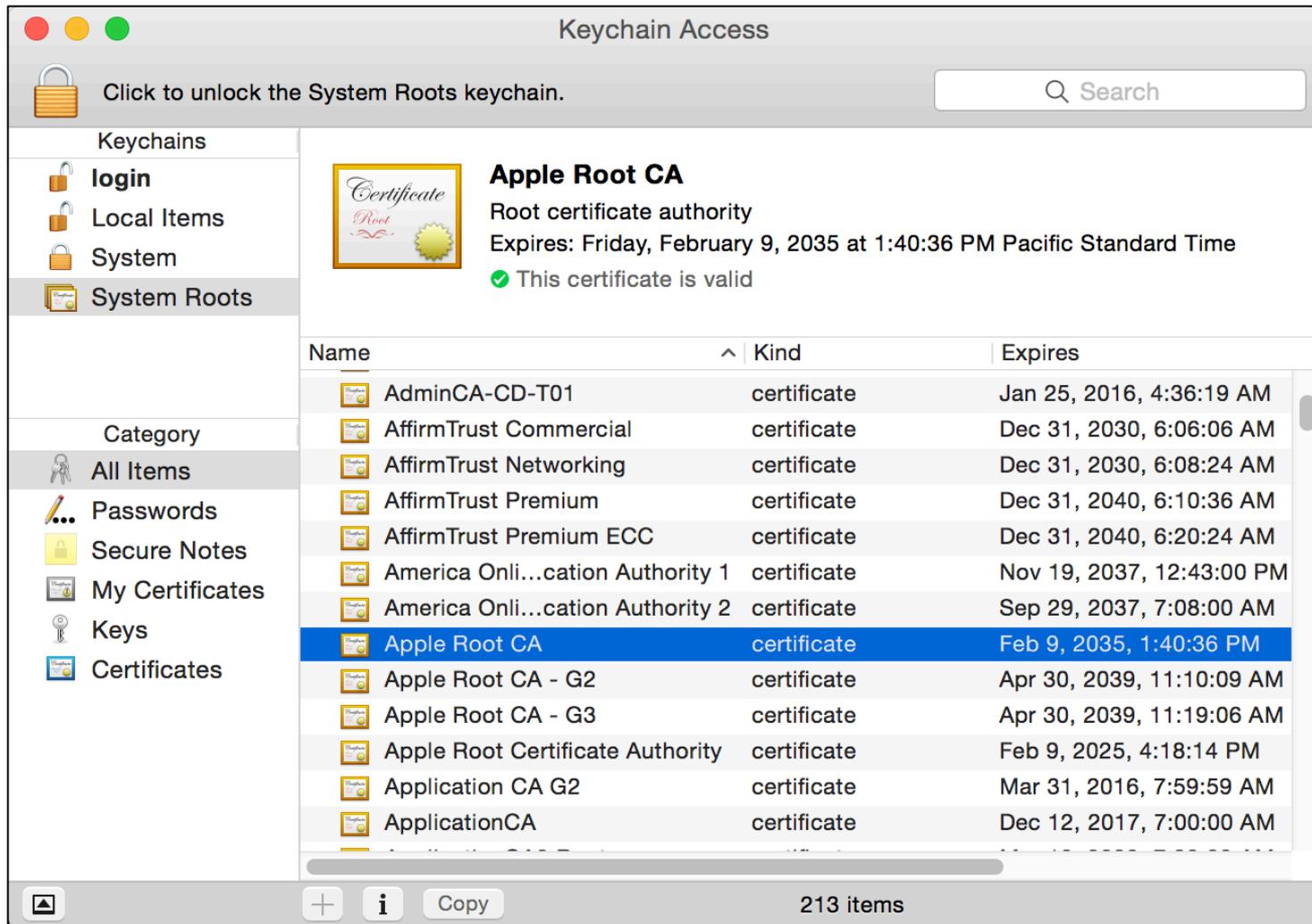
Authentication

How does Alice know this is actually Google?



 Alice's browser knows some trusted authorities

Trusted(?) Certificate Authorities



Keychain Access

Click to unlock the System Roots keychain.

Search

Keychains

- login
- Local Items
- System
- System Roots**

Category

- All Items
- Passwords
- Secure Notes
- My Certificates
- Keys
- Certificates

Apple Root CA
Root certificate authority
Expires: Friday, February 9, 2035 at 1:40:36 PM Pacific Standard Time
✔ This certificate is valid

Name	Kind	Expires
AdminCA-CD-T01	certificate	Jan 25, 2016, 4:36:19 AM
AffirmTrust Commercial	certificate	Dec 31, 2030, 6:06:06 AM
AffirmTrust Networking	certificate	Dec 31, 2030, 6:08:24 AM
AffirmTrust Premium	certificate	Dec 31, 2040, 6:10:36 AM
AffirmTrust Premium ECC	certificate	Dec 31, 2040, 6:20:24 AM
America Onli...cation Authority 1	certificate	Nov 19, 2037, 12:43:00 PM
America Onli...cation Authority 2	certificate	Sep 29, 2037, 7:08:00 AM
Apple Root CA	certificate	Feb 9, 2035, 1:40:36 PM
Apple Root CA - G2	certificate	Apr 30, 2039, 11:10:09 AM
Apple Root CA - G3	certificate	Apr 30, 2039, 11:19:06 AM
Apple Root Certificate Authority	certificate	Feb 9, 2025, 4:18:14 PM
Application CA G2	certificate	Mar 31, 2016, 7:59:59 AM
ApplicationCA	certificate	Dec 12, 2017, 7:00:00 AM

213 items

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 not trusted by your computer's operating system. This may mean that the server's credentials, which Chrome cannot rely on for identity information, or an attacker intercepted your communications.

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

Proceed anyway

Back to safety

► [Help me understand](#)



Your connection is not private

Attackers might be trying to steal your information from **reddit.com** (for example, passwords, messages, or credit cards).

Proceed to the site (unsafe)

Back to safety

► [Advanced](#)



Your connection is not private

Attackers might be trying to steal your information from **www.example.com** (for example, passwords, messages, or credit cards).

[Advanced](#)

Back to safety

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