Skip the Mac, Hit the iPhone: Evasive iMessage Attacks

Swantje Lange

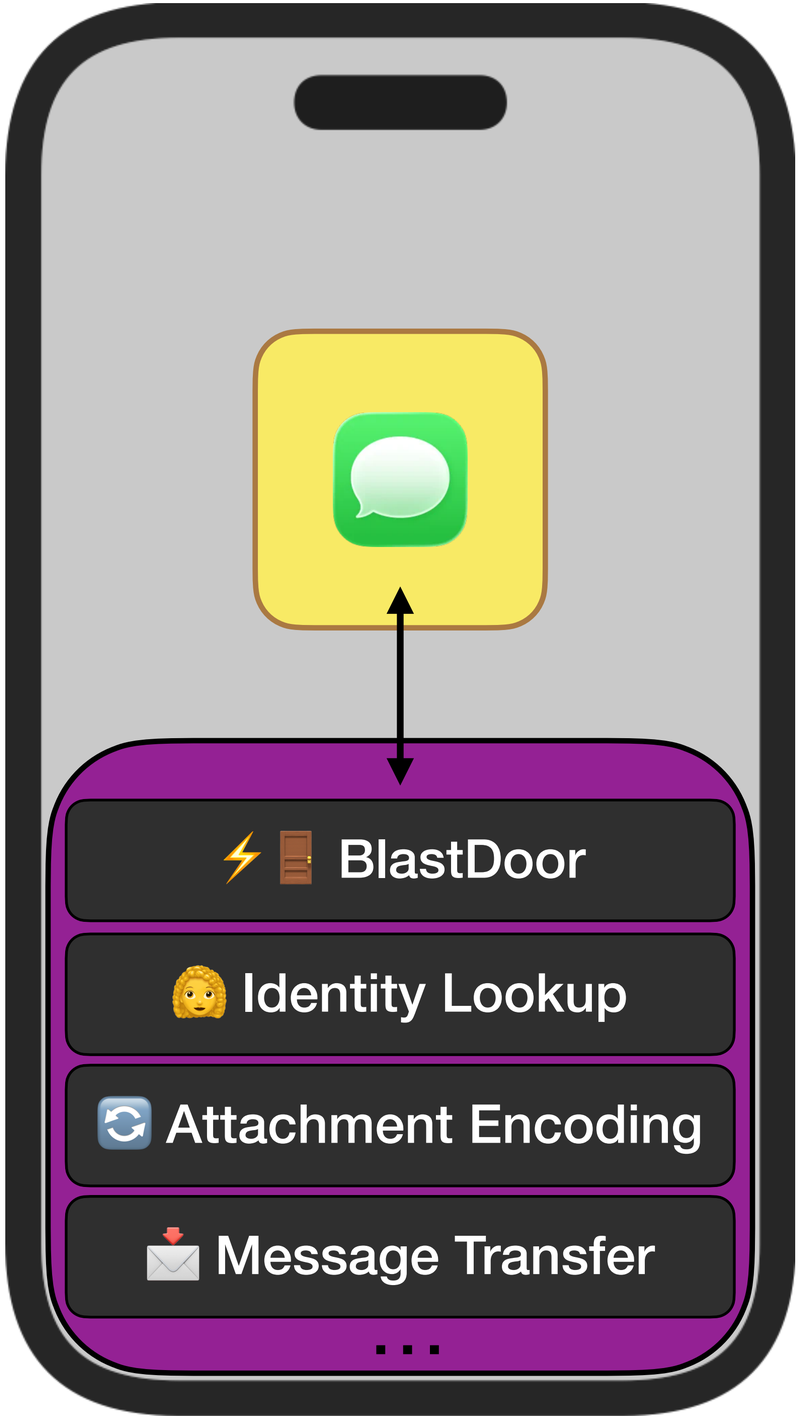
OFTW @ HPI 2026

Why iMessage?


Tue
1
shop
Uber
Booking
dm
2DF
DHL


Tue
1
shop
Booking
Uber
2DF
DHL


Tue
1
shop
Booking
Uber
2DF
DHL


⚡🚪 BlastDoor
👱 Identity Lookup
🔄 Attachment Encoding
📩 Message Transfer
...

Attacks discovered in the past

Attacks discovered in the past

FORCEDENTRY

0-click
.gif image files
Disguised pdfs

🔄 Attachment Encoding

Exploiting pdf parser
→ code execution

BLASTPASS

0-click
PassKit attachment
with malicious images

⚡🚪 BlastDoor

Exploiting webp parser
→ code execution

Operation Triangulation

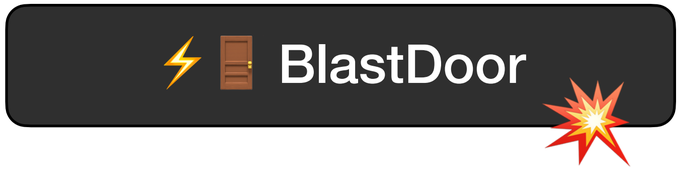
0-click
.watchface attachment

📶↑↓ Network traffic

Font parsing library
→ code execution

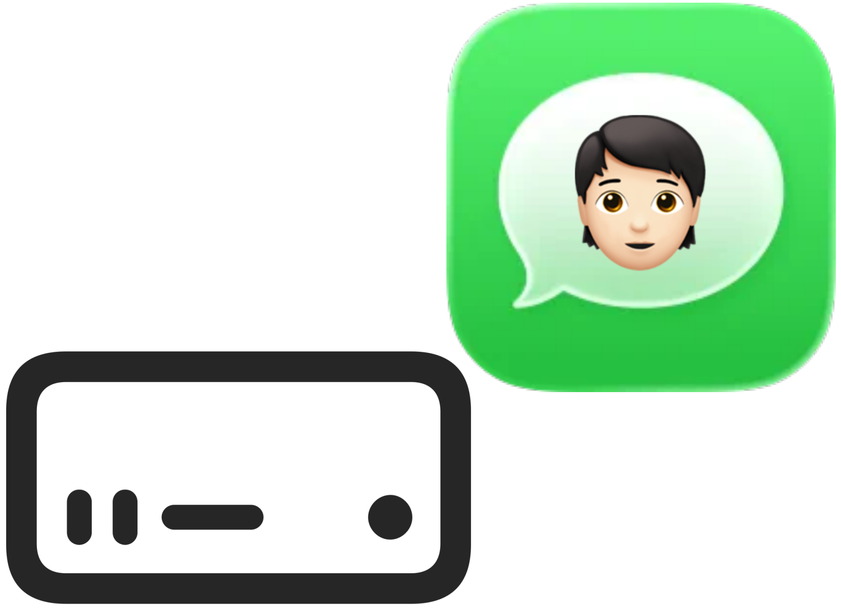
https://citizenlab.ca/research/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/
https://securitylab.amnesty.org/latest/2023/12/pegasus-zero-click-exploit-threatens-journalists-in-india/

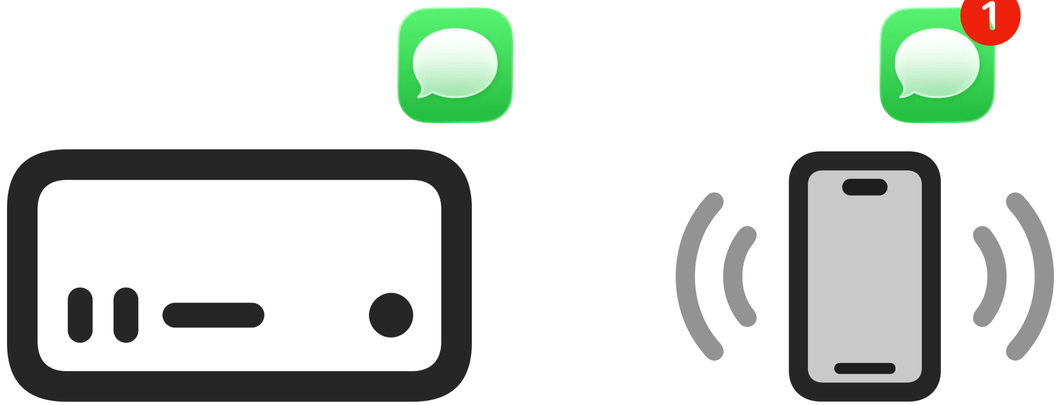
Exploits 101



Exploits 101

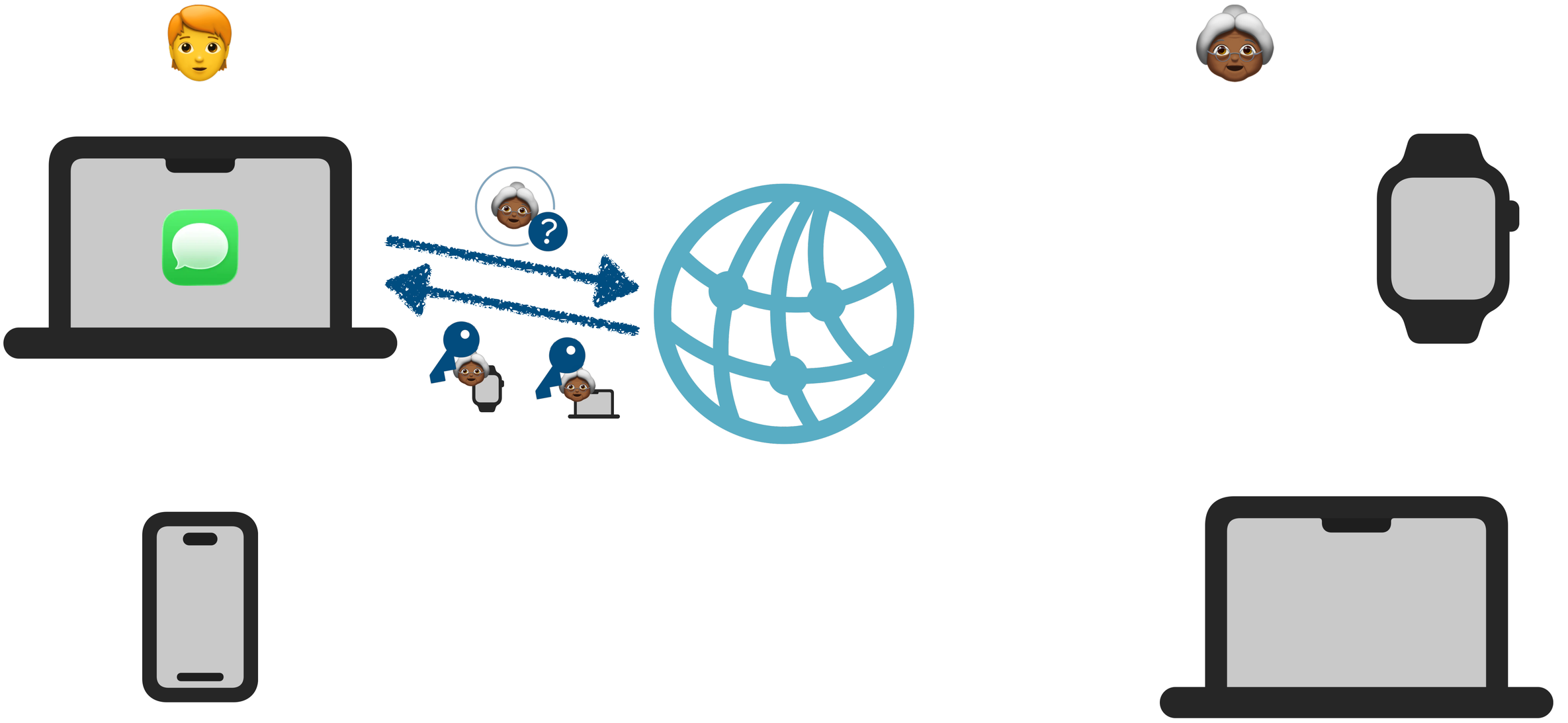
Operation Triangulation





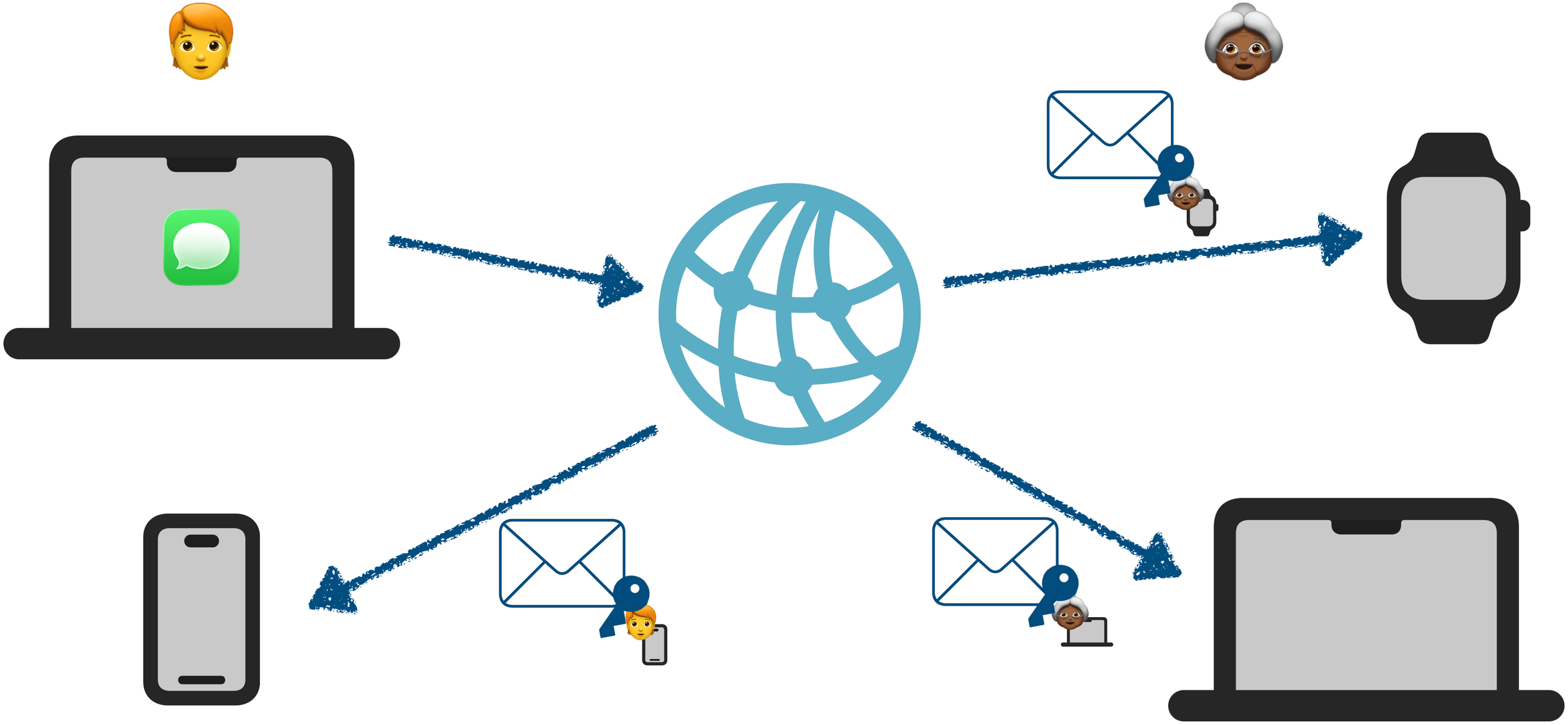
Why does the message not reach the Mac mini?

iMessage Protocol

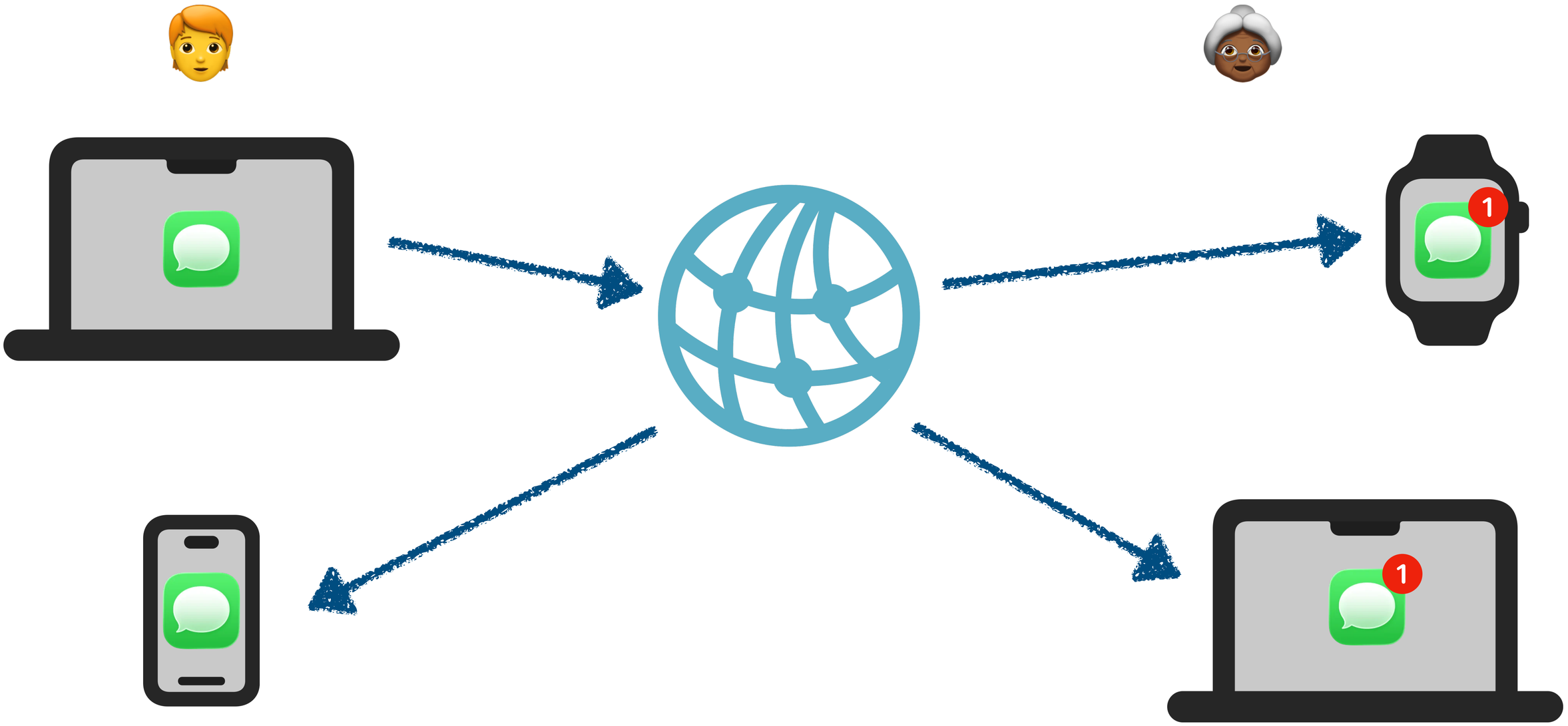


iMessage Protocol

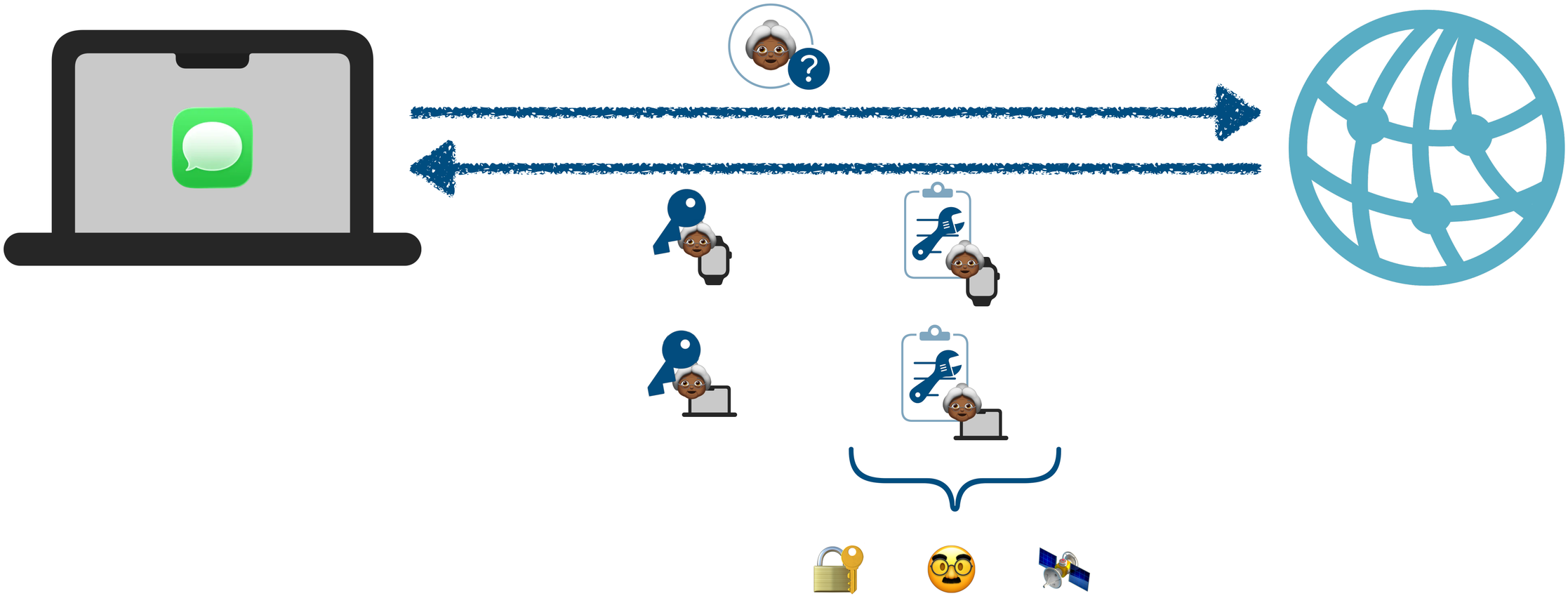
iMessage Protocol



iMessage Protocol



The Apple Identity Service



iMessage Capabilities

```
client-data.ec-version = 1.0
client-data.prefers-sdr = 1.0
client-data.show-peer-errors = T
client-data.supports-animoji-v2 = T
…
```

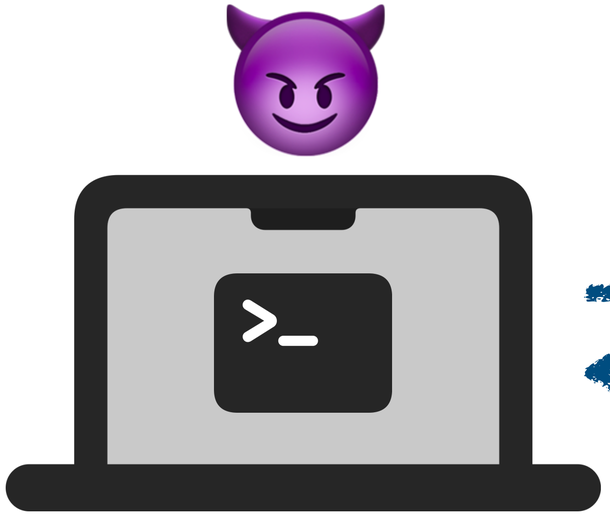
```
client-data.ec-version = 1.0
client-data.prefers-sdr = F
client-data.show-peer-errors = n/a
client-data.supports-animoji-v2 = T
…
```

iMessage Capabilities

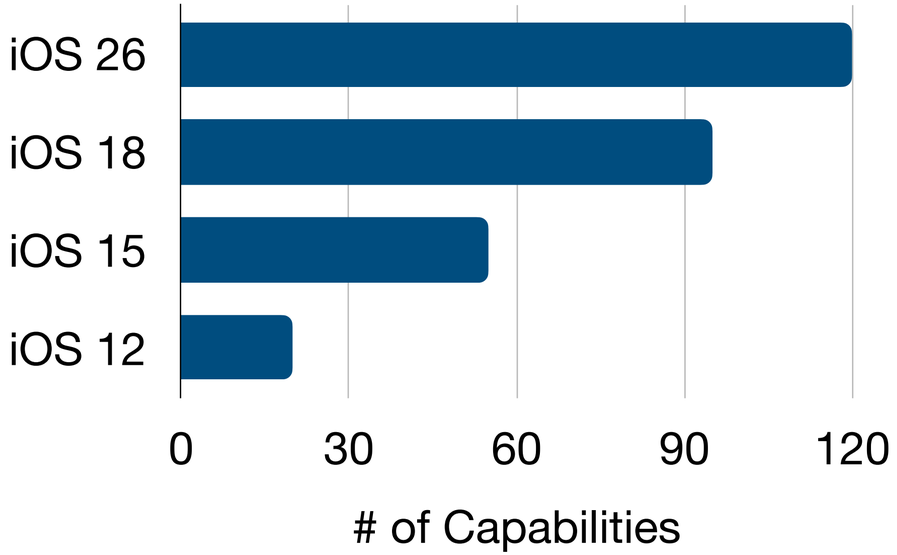
```
client-data.ec-version = 1.0
client-data.prefers-sdr = 1.0
client-data.show-peer-errors = T
client-data.supports-animoji-v2 = T
…
```

```
client-data.ec-version = 1.0
client-data.prefers-sdr = F
client-data.show-peer-errors = n/a
client-data.supports-animoji-v2 = T
…
```

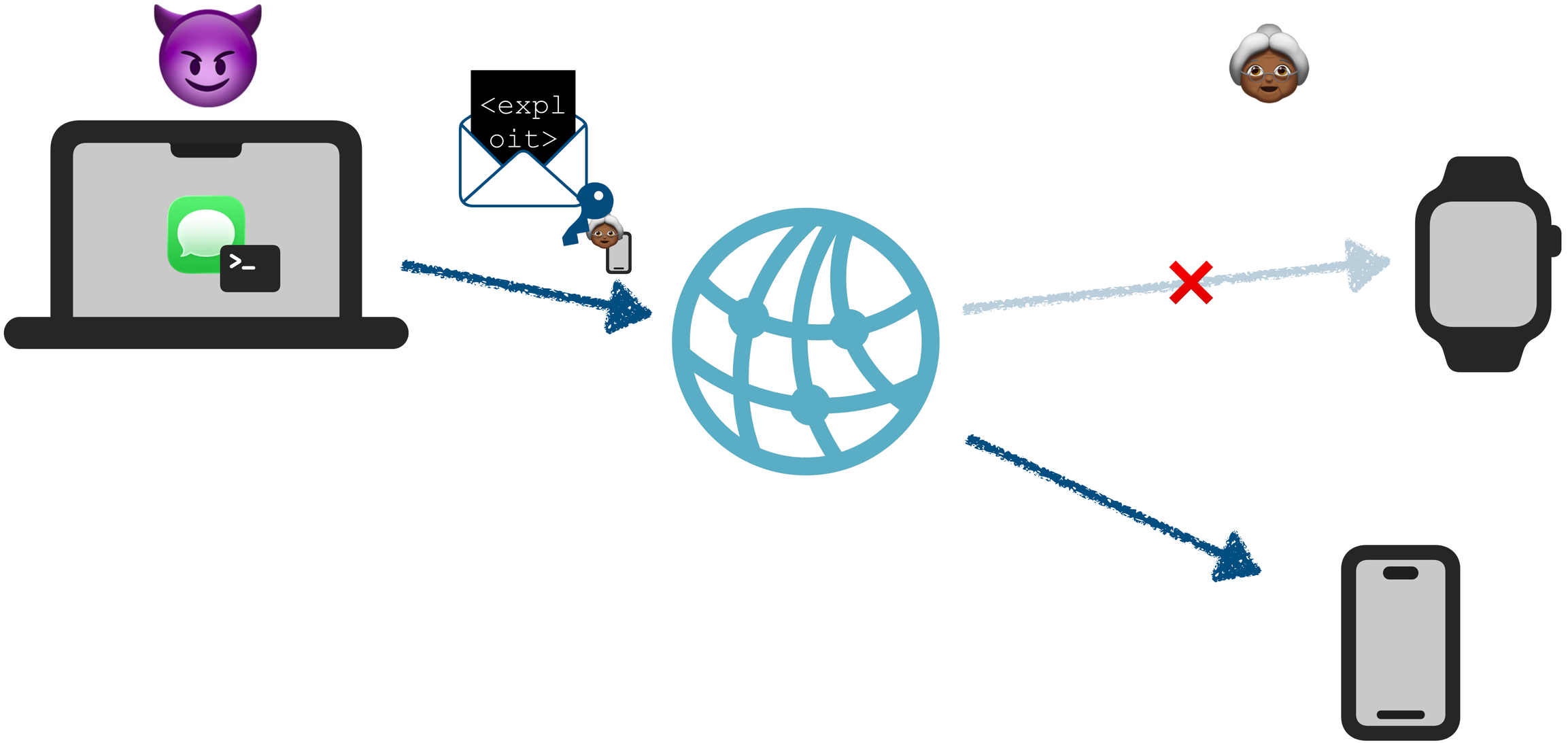
iMessage Capabilities



GET firmware_images

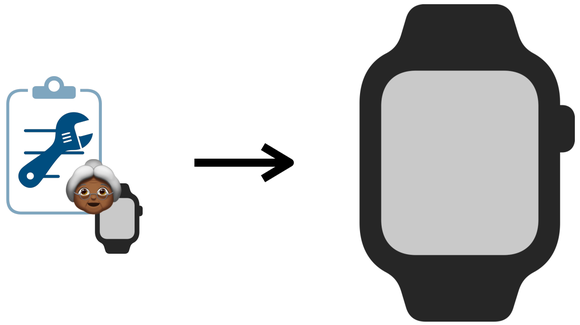


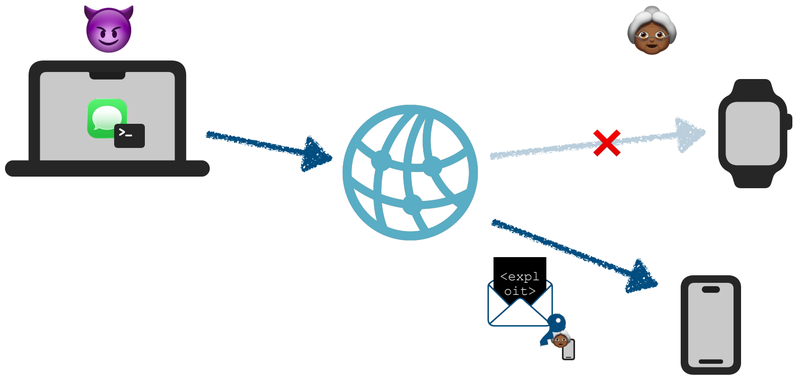
Targeting Single Devices



What does Apple say about this?

Disclosure





✅ Solve compatibility problems
Correct message formatting

❌ Break compatibility with new features 😕 or complex fallback logic

🔄 Continuous assessment

✅ Encrypted channels per device
Capabilities ensure devices can handle messages

❌ Impossible to reliably deliver correct format

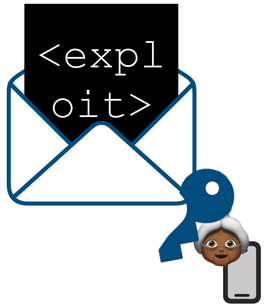
🌳 Natural consequence of channels

🤷

iMessage can be (ab)used to:

Infer a user's devices

Deliver exploit payload to specific devices only



→ Likely what happened in Operation Triangulation

Blue Bubbles, Red Flags:
Investigating Privacy Leakage in Apple iMessage

Viktor E. Garske*
ISMK, University of Applied Sciences Stralsund
Stralsund, Germany
viktor.garske@ismk-stralsund.de

Swantje Lange*
Hasso Plattner Institute, University of Potsdam
Potsdam, Germany
swantje.lange@hpi.de

Gabriel K. Gegenhuber
Interdisciplinary Transformation University (IT:U)
Linz, Austria
gabriel.gegenhuber@it-u.at

David Schmidt
University of Vienna, CDL AsTra

Andreas Noack
ISMK, University of Applied

Jiska Classen
Hasso Plattner Institute, University of Potsdam

swantje.lange@hpi.de
@swantje@chaos.social
linkedin.com/in/swantje-lange