ETH zürich

Sound-Proof: Usable Two-Factor Authentication Based on Ambient Sound

Nikos Karapanos, Claudio Marforio,
Claudio Soriente and Srdjan Čapkun
ETH Zurich

USENIX Security 2015

Supplementing passwords

Supplementing passwords

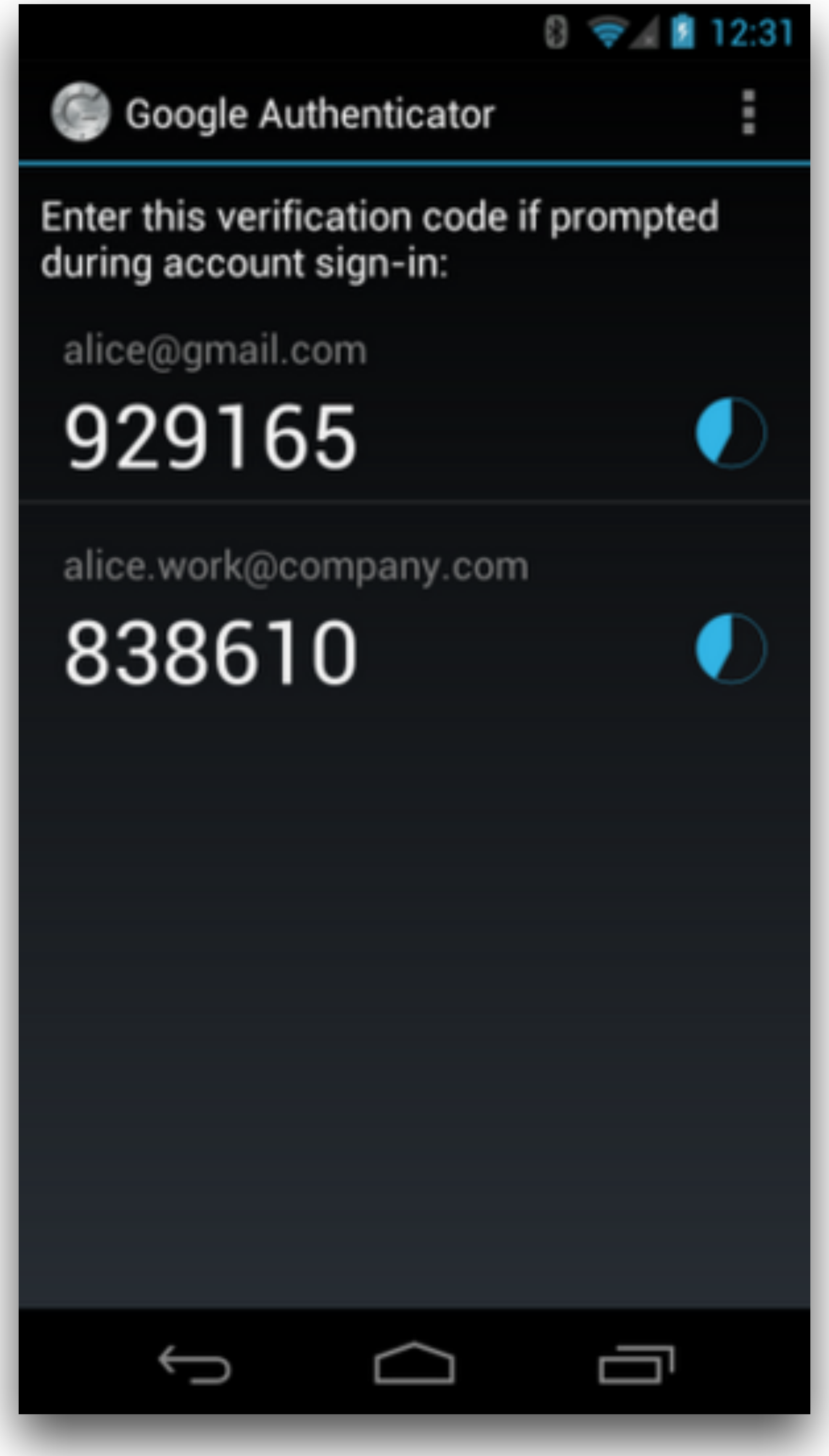
- Passwords are used everywhere
  - Password reuse, leakage, guessing, phishing…

Supplementing passwords

- Passwords are used everywhere
  - Password reuse, leakage, guessing, phishing…
- Two-factor authentication to the rescue

Supplementing passwords

- Passwords are used everywhere
  - Password reuse, leakage, guessing, phishing…
- Two-factor authentication to the rescue
- Password + Token (one-time code)
  - Typically smartphones are used as tokens



Enter this verification code if prompted during account sign-in:

alice@gmail.com
929165

alice.work@company.com
838610

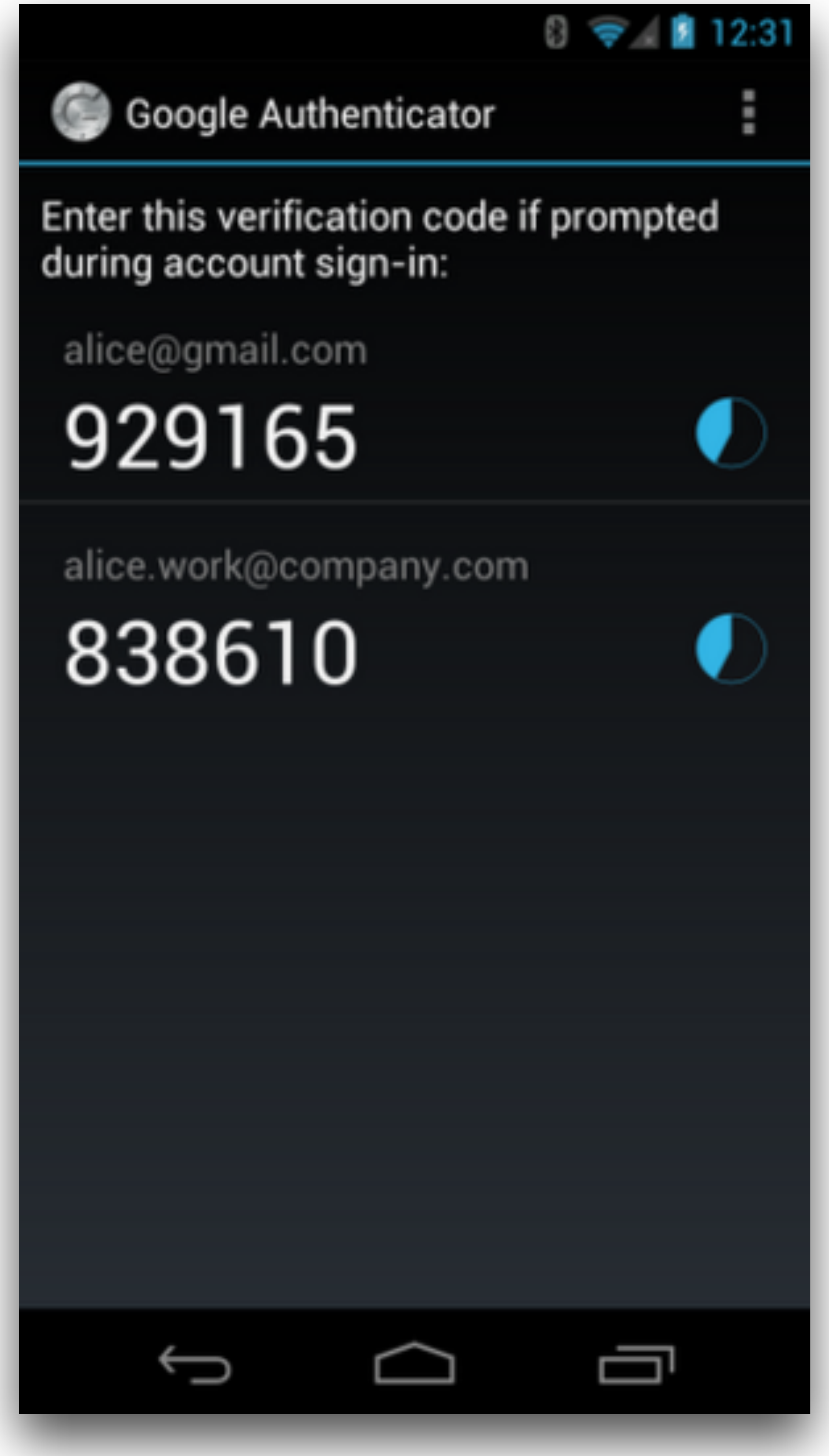
Web 2FA Adoption

Is 2FA used in practice on the web?

Web 2FA Adoption

Is 2FA used in practice on the web?

- Most popular 2FA: Code-based (App or SMS)
  - Google, Facebook, Apple, Microsoft, Twitter…



Enter this verification code if prompted during account sign-in:

alice@gmail.com
929165

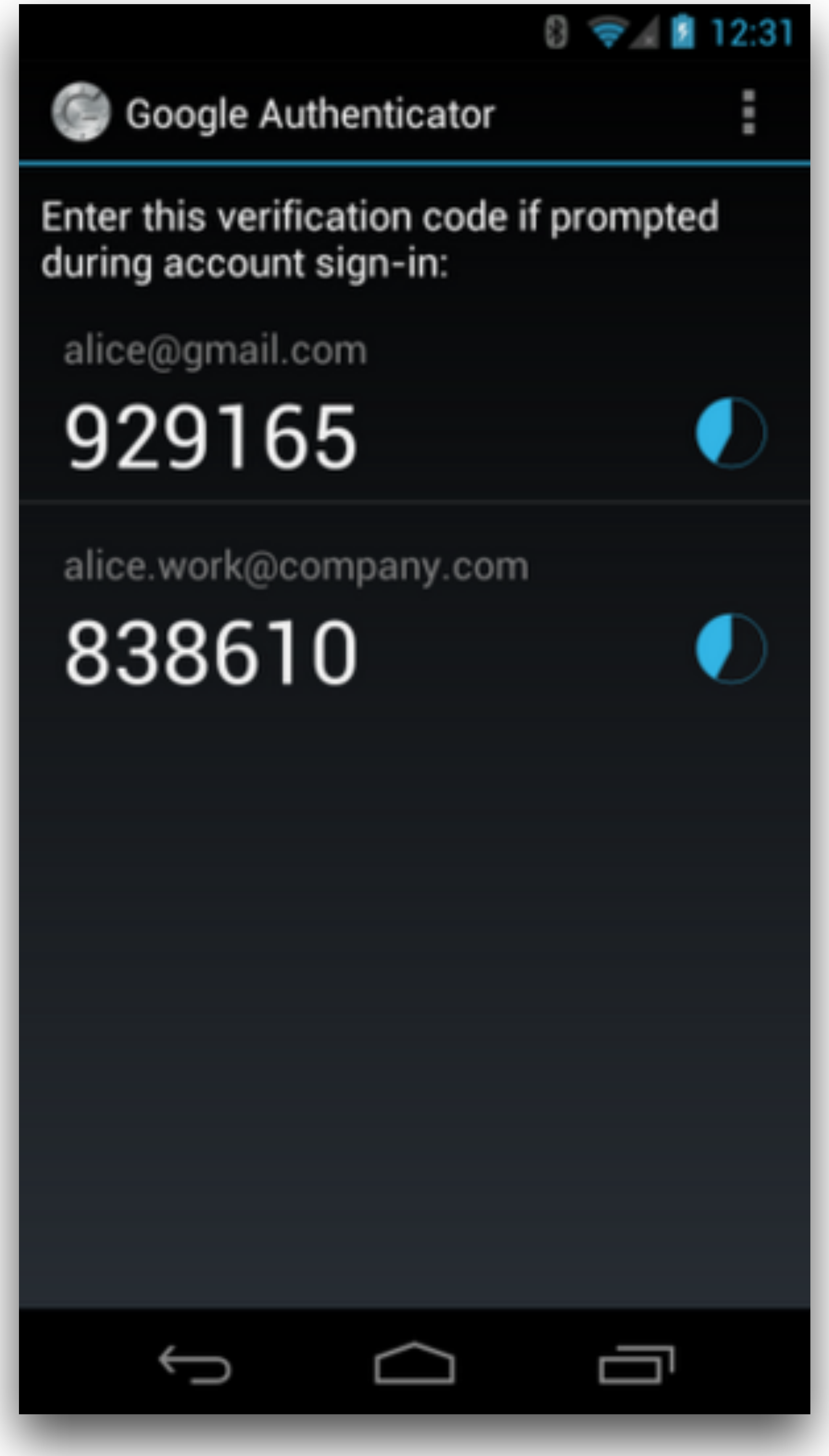
alice.work@company.com
838610

Web 2FA Adoption

Is 2FA used in practice on the web?

- Most popular 2FA: Code-based (App or SMS)
  - Google, Facebook, Apple, Microsoft, Twitter…

- **Small** user adoption (**if 2FA optional**)
  - Only 25% of Americans use 2FA[1]
  - Only 6% of 100k Gmail accounts have 2FA enabled[2]



Enter this verification code if prompted during account sign-in:

alice@gmail.com
929165

alice.work@company.com
838610

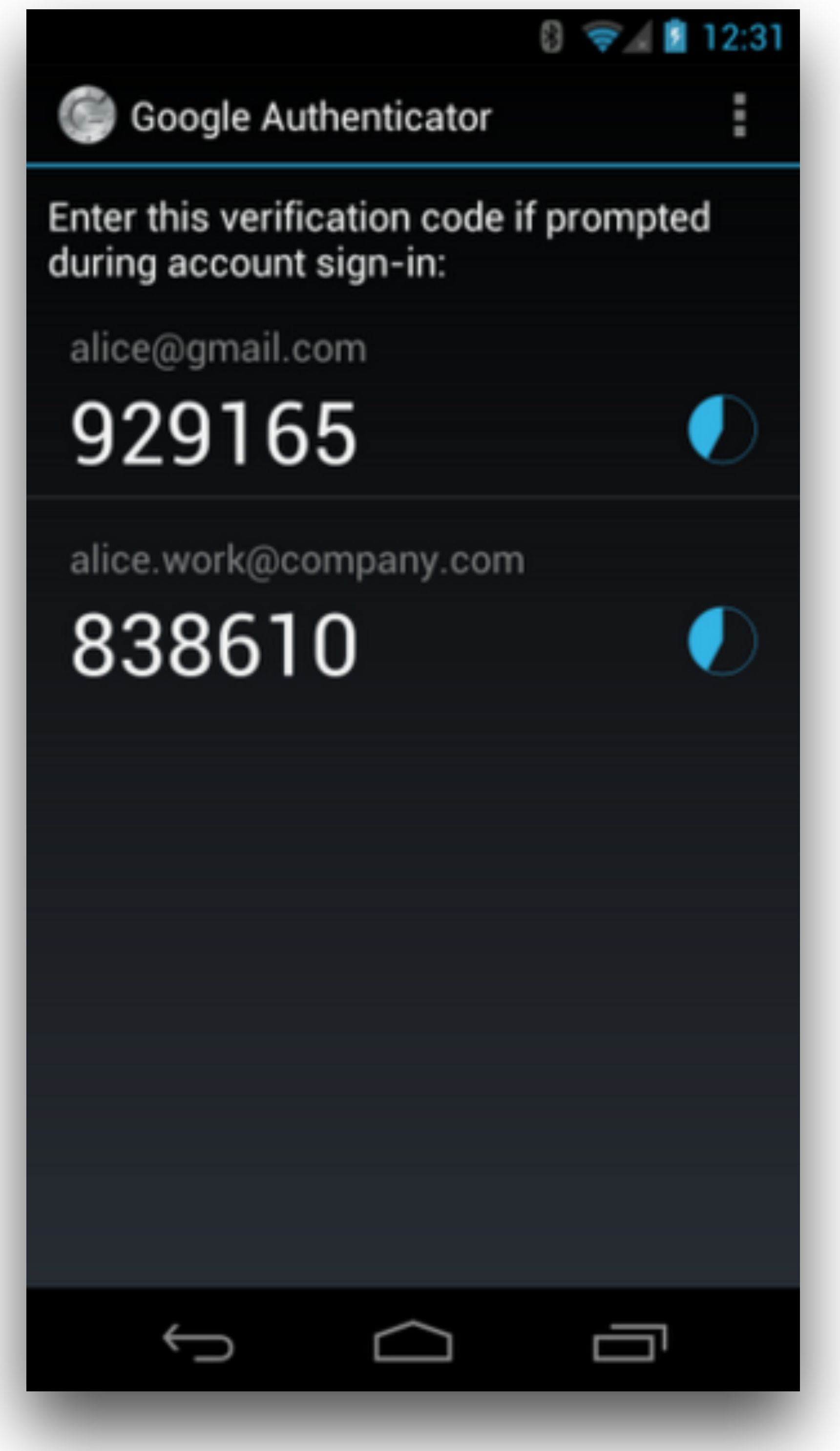
[1] Study by Impermium, 2013 (BusinessWire article, http://goo.gl/NsUCL7)
[2] Petsas et al., EuroSec 2015

Improving 2FA Usability

Reduce user actions

Improving 2FA Usability

Reduce user actions



12:31

Google Authenticator

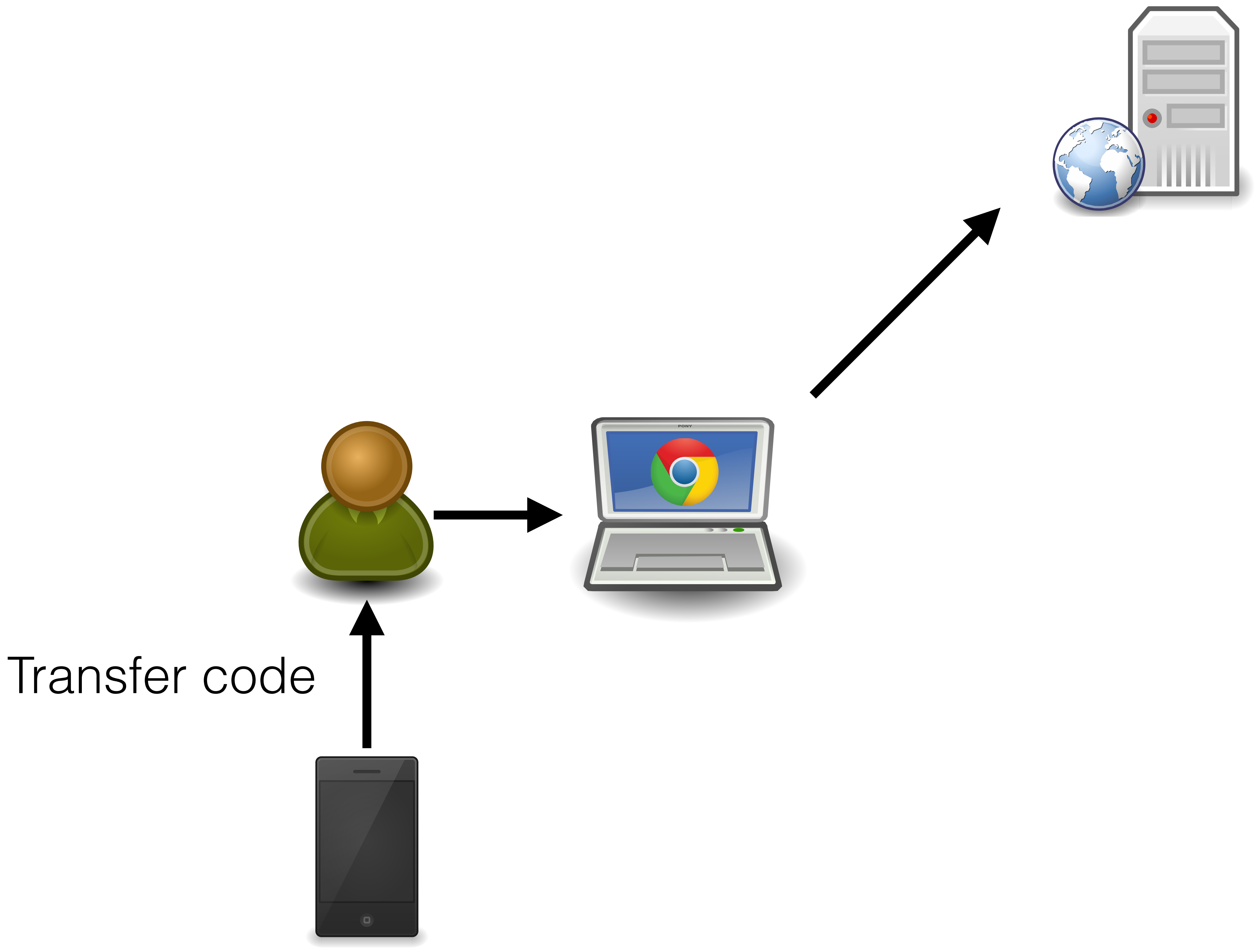
Enter this verification code if prompted during account sign-in:

alice@gmail.com

929165

alice.work@company.com

838610



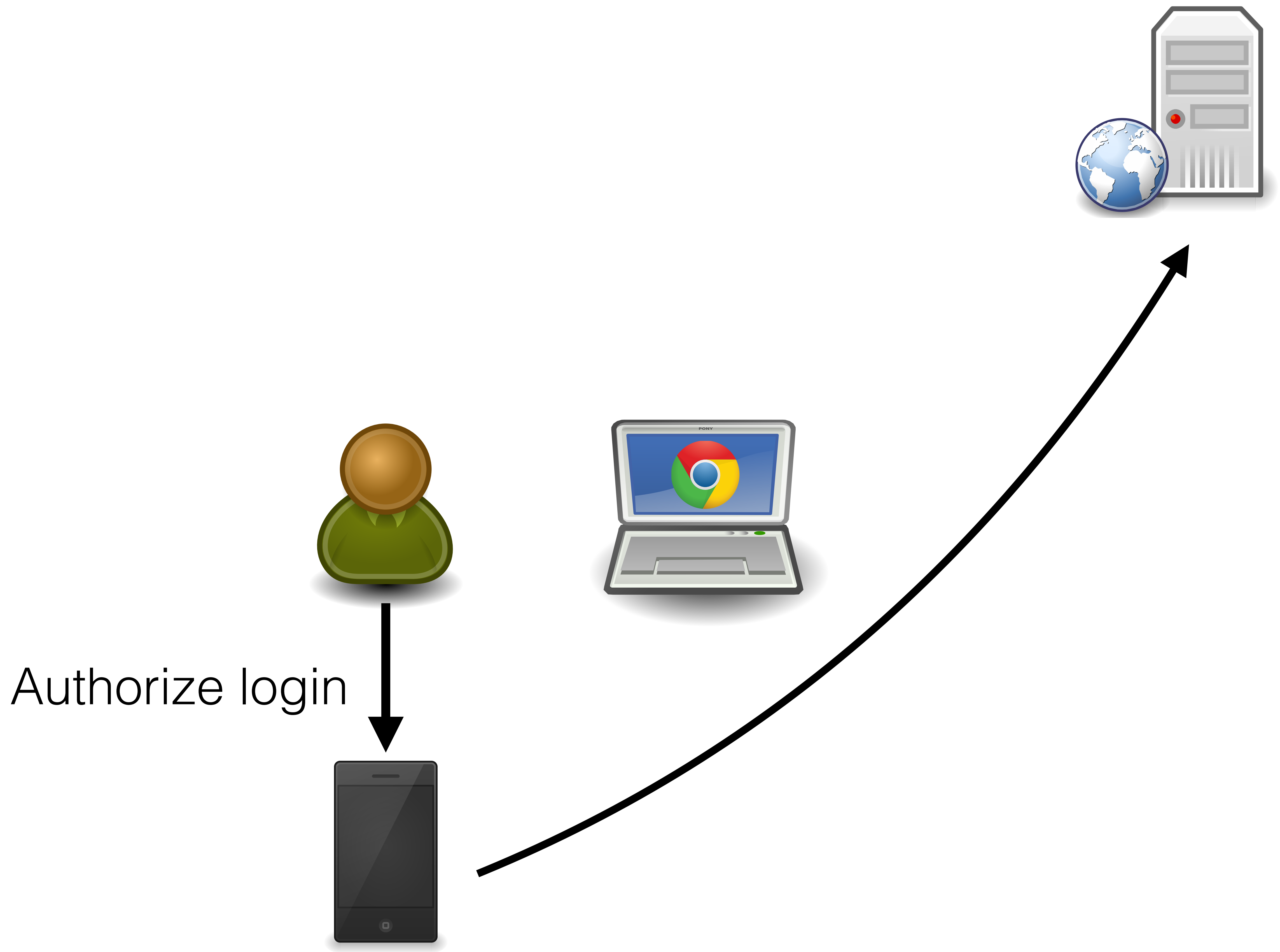
Improving 2FA Usability

Reduce user actions

- Minimize user-phone interaction
  - Just tap a button instead of copying a code

ENCAP® SECURITY

DUO



Authorize login

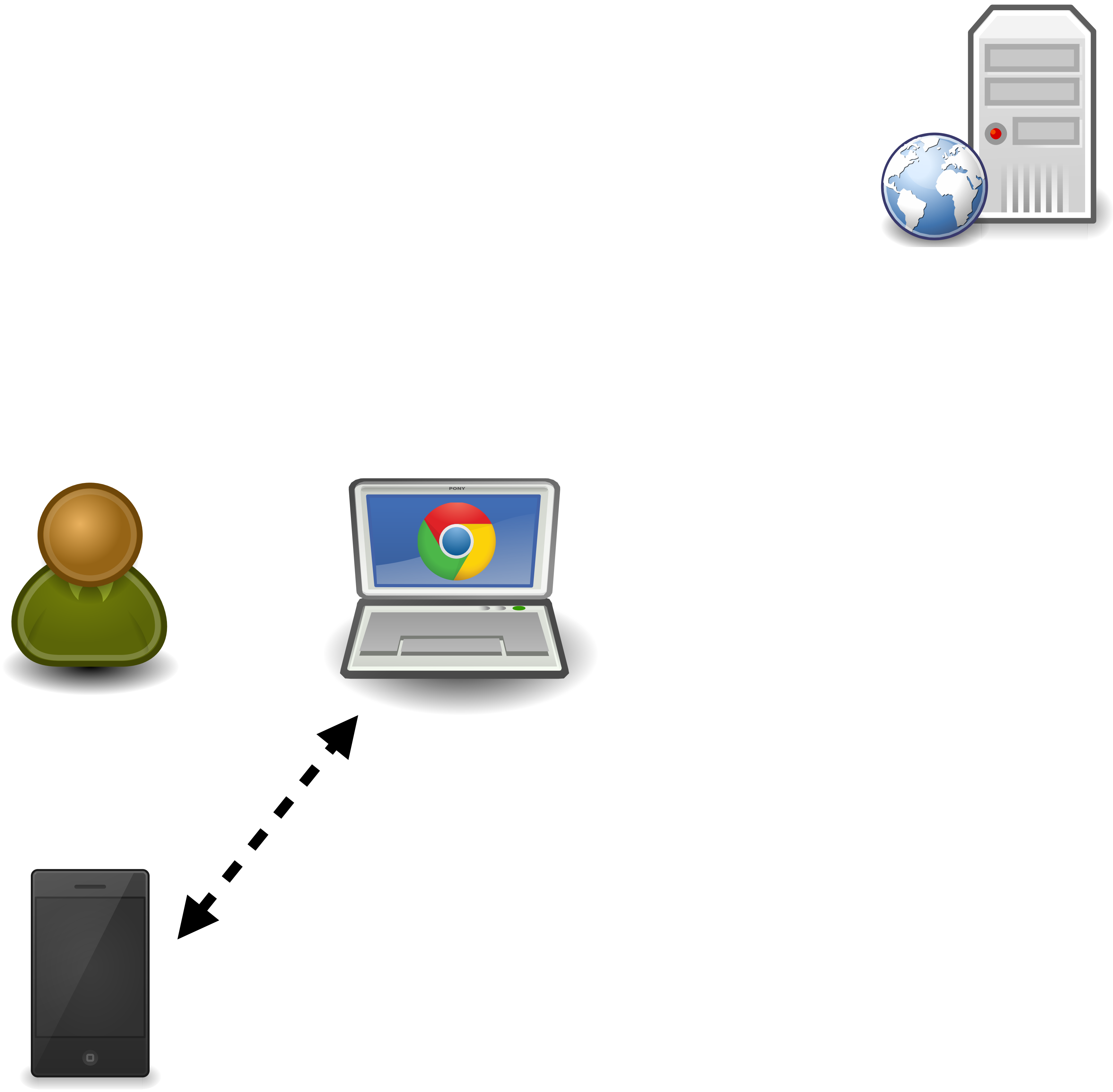
Eliminate user-phone interaction

How can it be achieved?

Eliminate user-phone interaction

How can it be achieved?

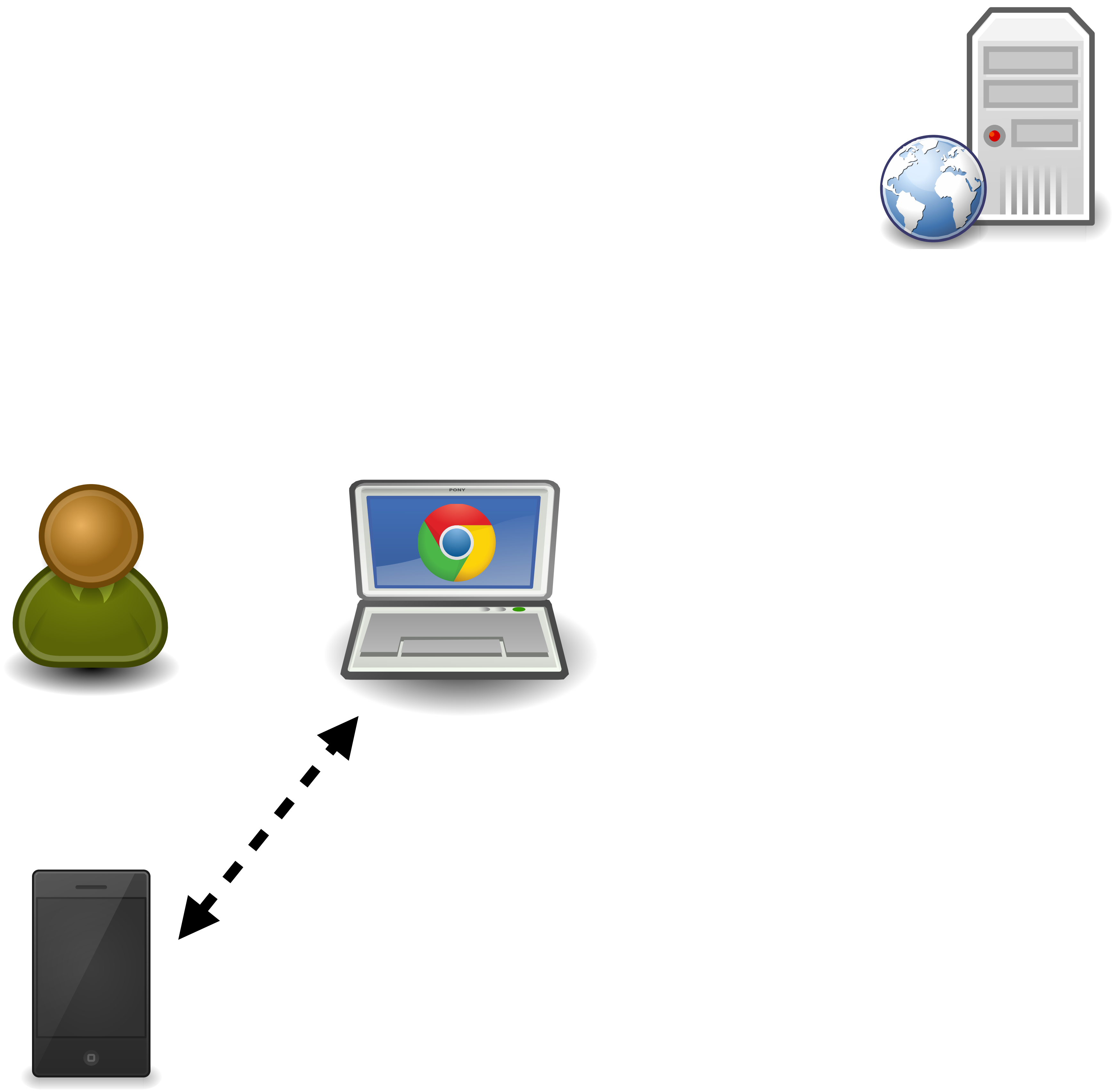
- Leverage the **proximity** between user's phone and computer as the **second factor**



Eliminate user-phone interaction

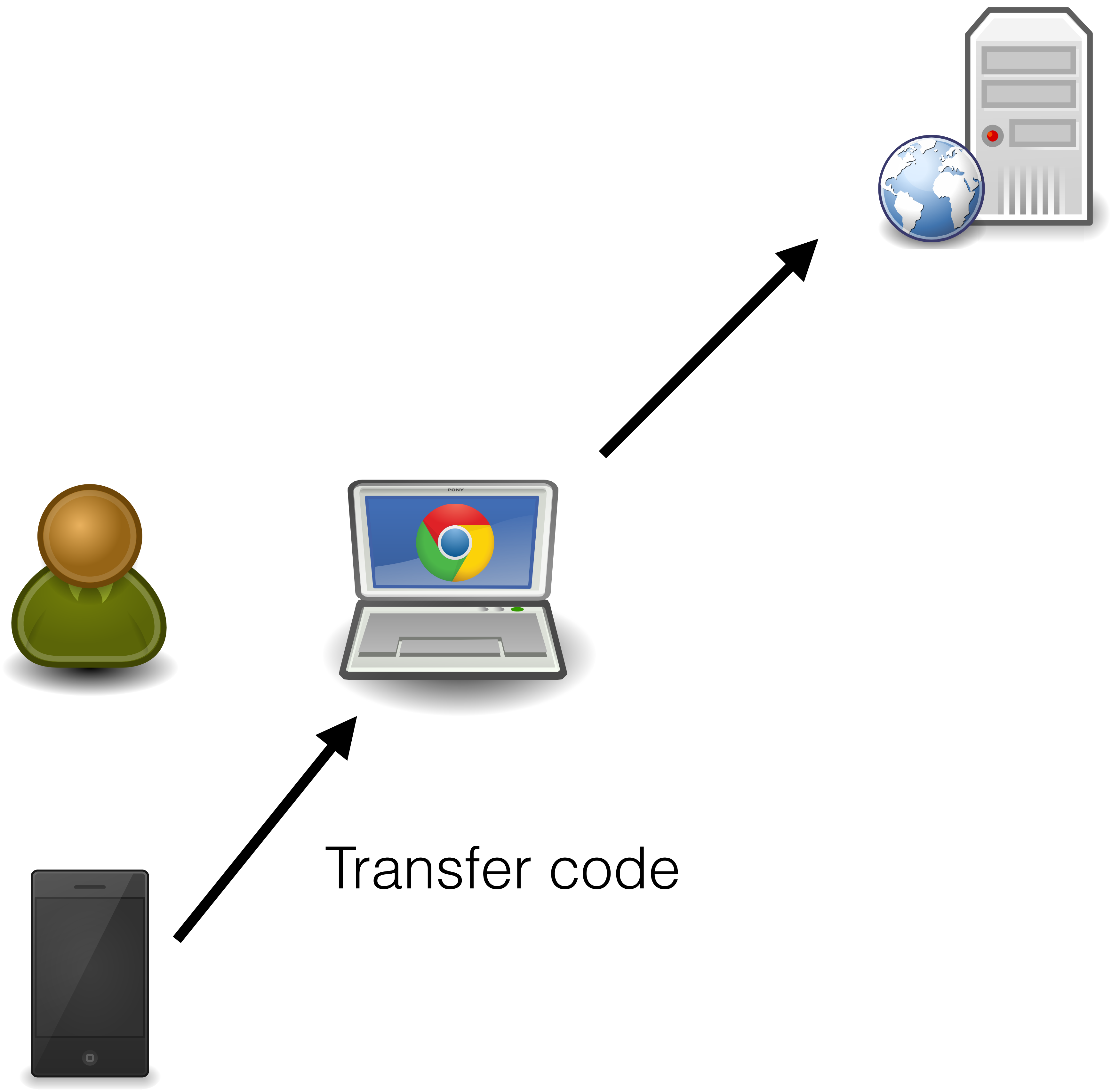
How can it be achieved?

- Leverage the **proximity** between user’s phone and computer as the **second factor**
- Proximity can be verified by:



How can it be achieved?

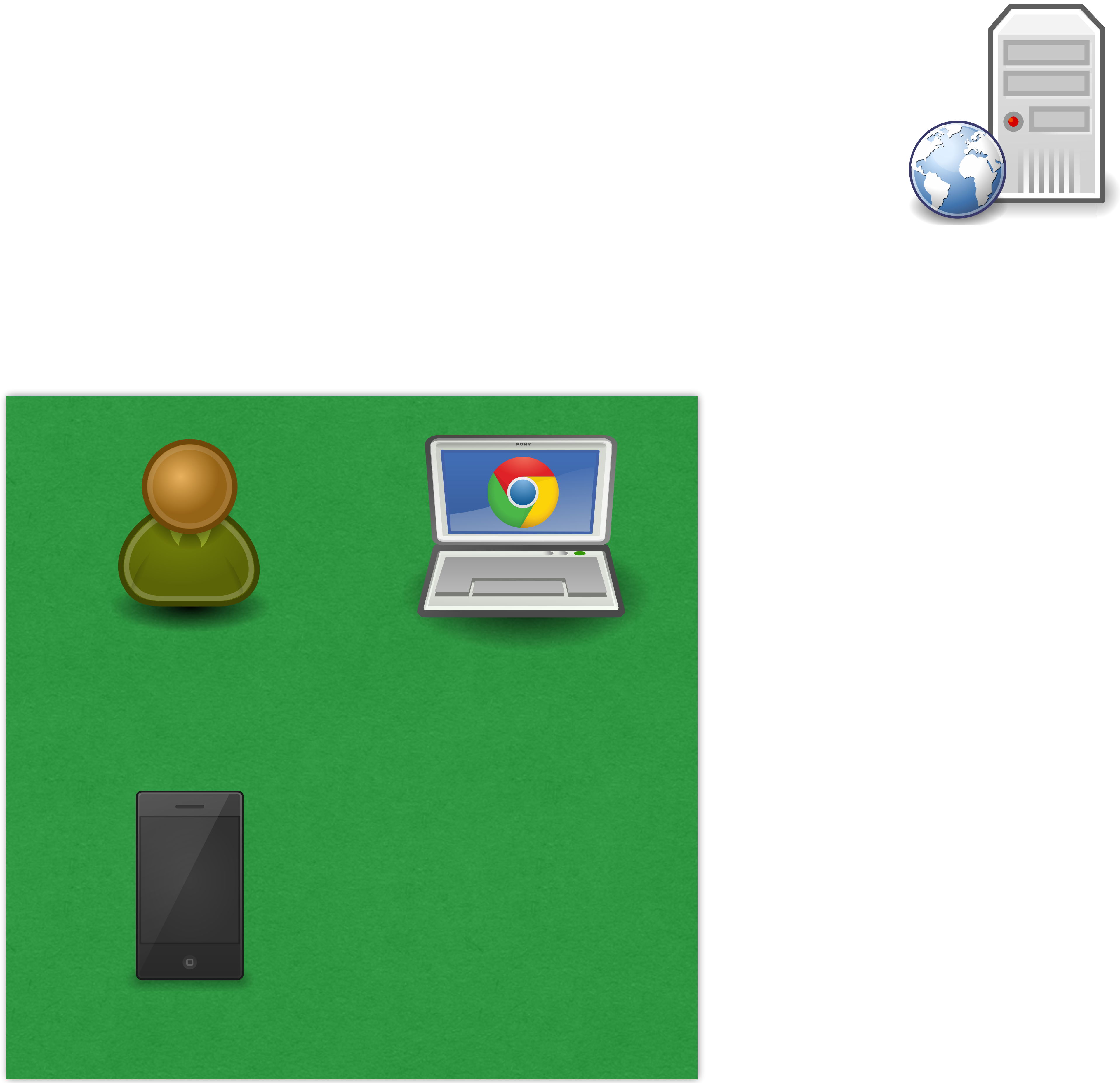
- Leverage the **proximity** between user's phone and computer as the **second factor**
- Proximity can be verified by:
  - Using local communication channels (phone-computer communication)



Eliminate user-phone interaction

How can it be achieved?

- Leverage the **proximity** between user’s phone and computer as the **second factor**
- Proximity can be verified by:
  - Using local communication channels (phone-computer communication)
  - Sensing the environment



Eliminate user-phone interaction

What are the available options?

Eliminate user-phone interaction

What are the available options?

Phone-computer communication

Eliminate user-phone interaction

What are the available options?

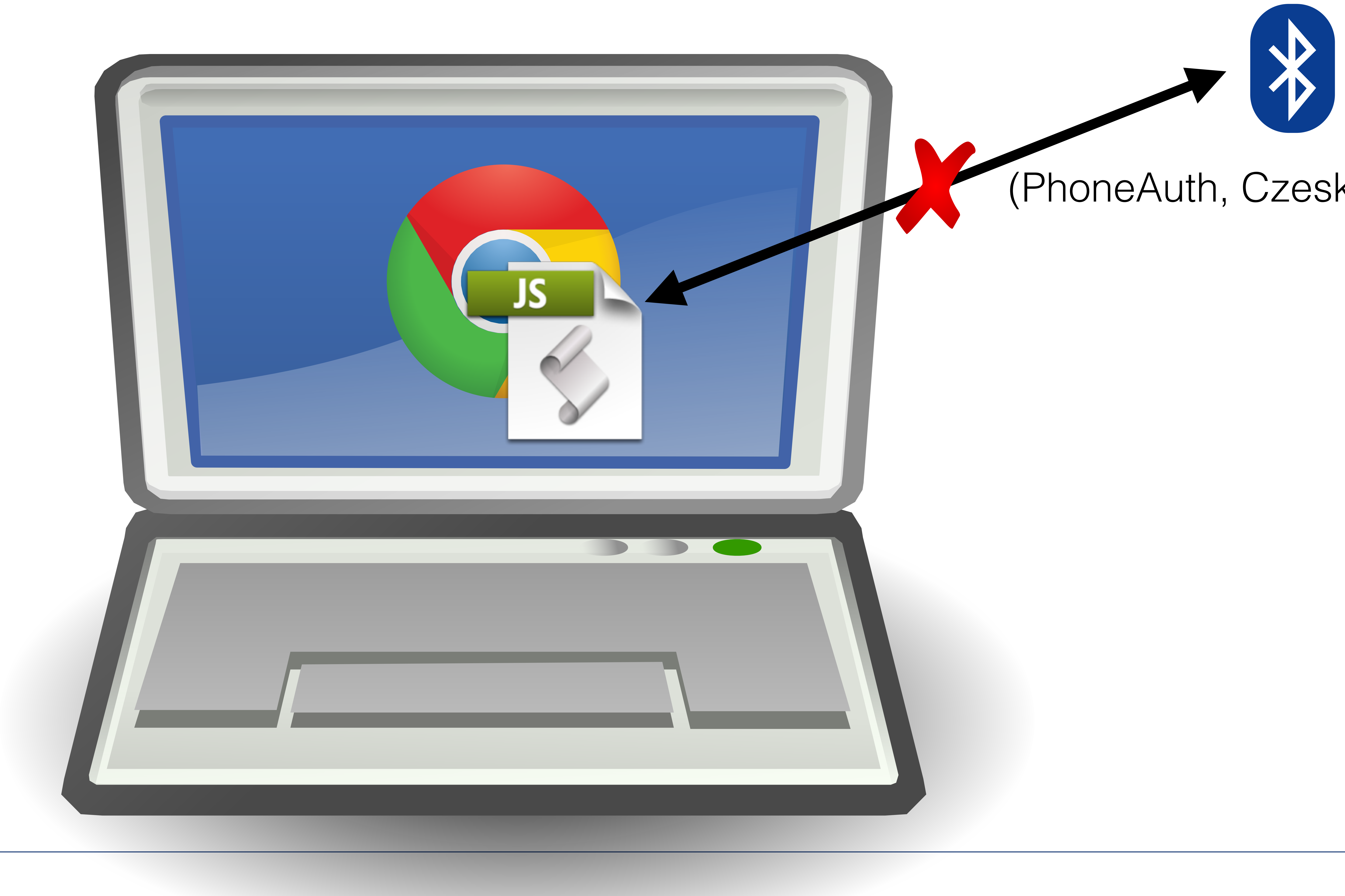
Phone-computer communication

(PhoneAuth, Czeskis et al., CCS '12)

Eliminate user-phone interaction

What are the available options?

Phone-computer communication



(PhoneAuth, Czeskis et al., CCS ’12)

Eliminate user-phone interaction

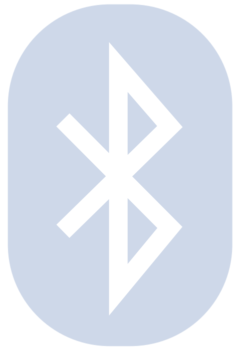
What are the available options?

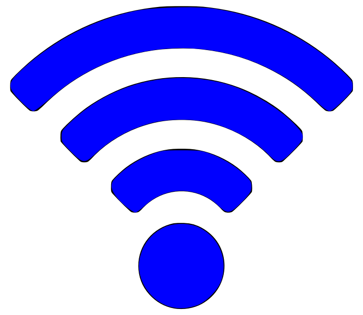
Phone-computer communication

Eliminate user-phone interaction

What are the available options?

Phone-computer communication





(Shirvanian et al., NDSS ’14)

Eliminate user-phone interaction

What are the available options?

Phone-computer communication

What are the available options?

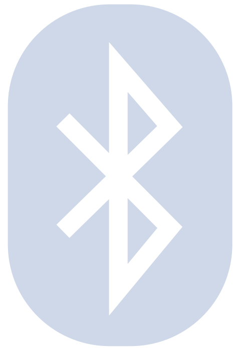
Phone-computer communication

Sense the environment

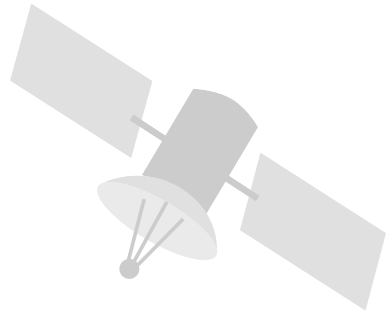
Eliminate user-phone interaction

What are the available options?

Phone-computer communication



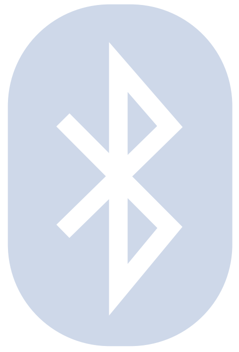
Sense the environment



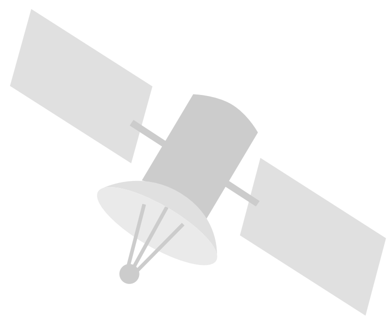
Eliminate user-phone interaction

What are the available options?

Phone-computer communication



Sense the environment

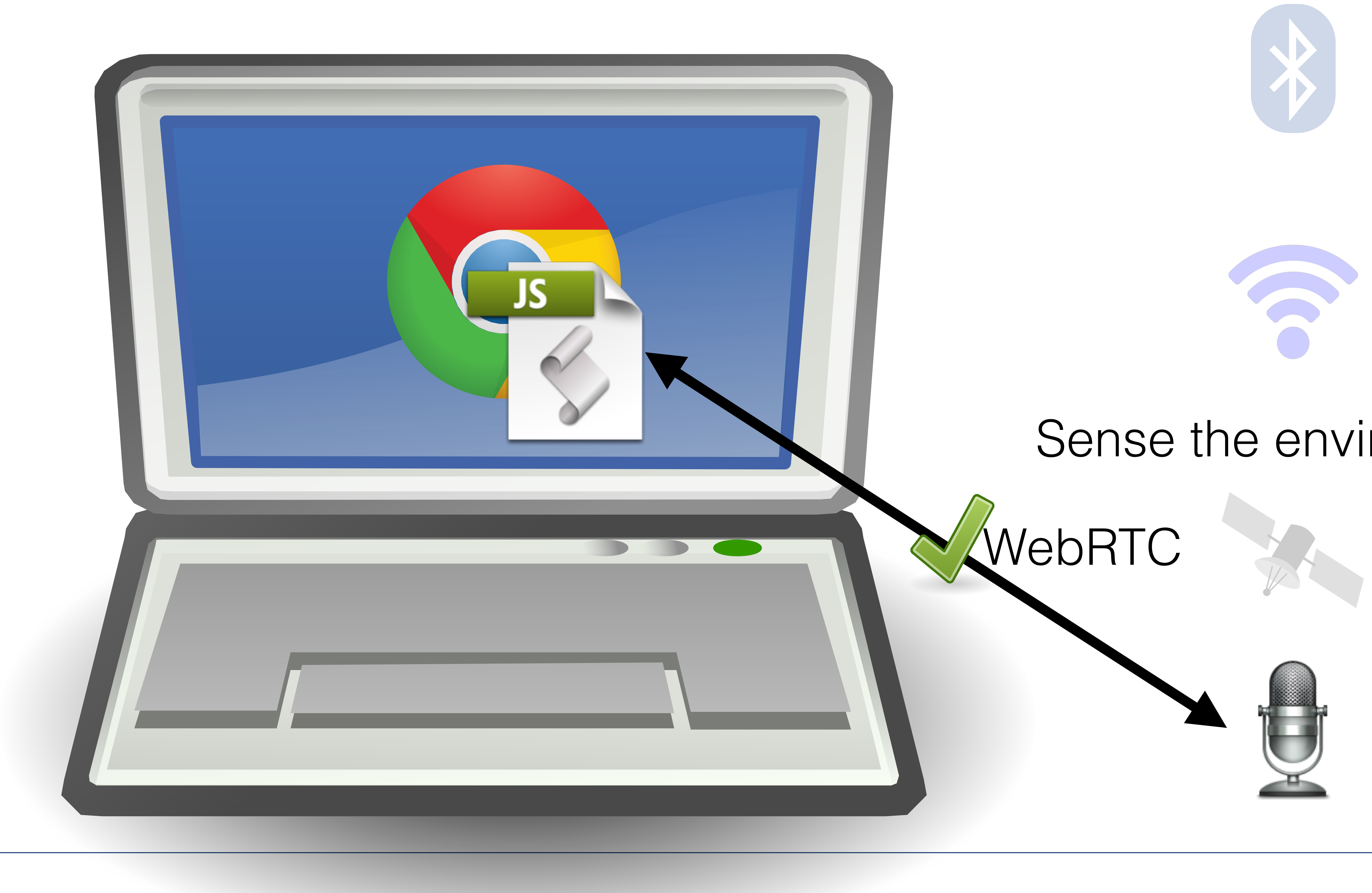


Eliminate user-phone interaction

What are the available options?

Phone-computer communication

Sense the environment



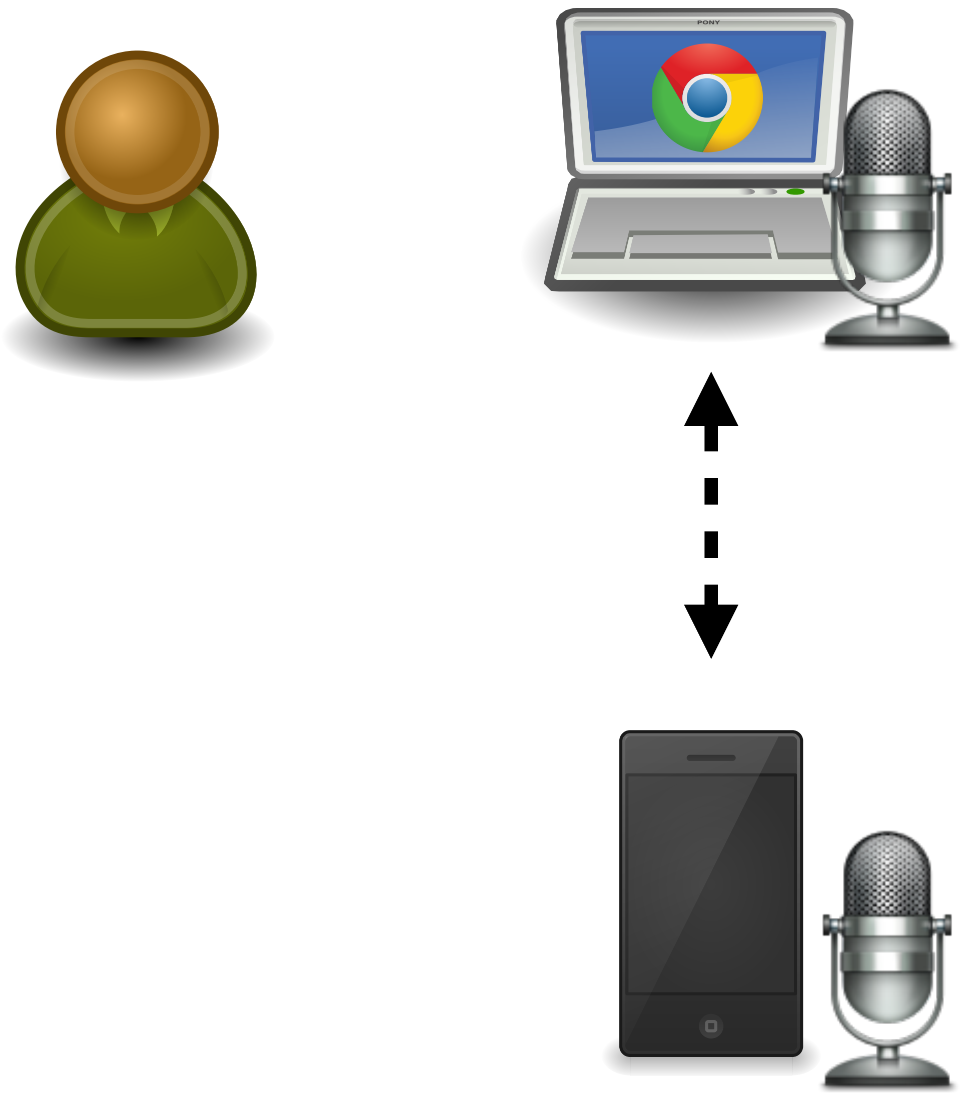
✓ WebRTC

Contributions

Sound-Proof

Sound-Proof

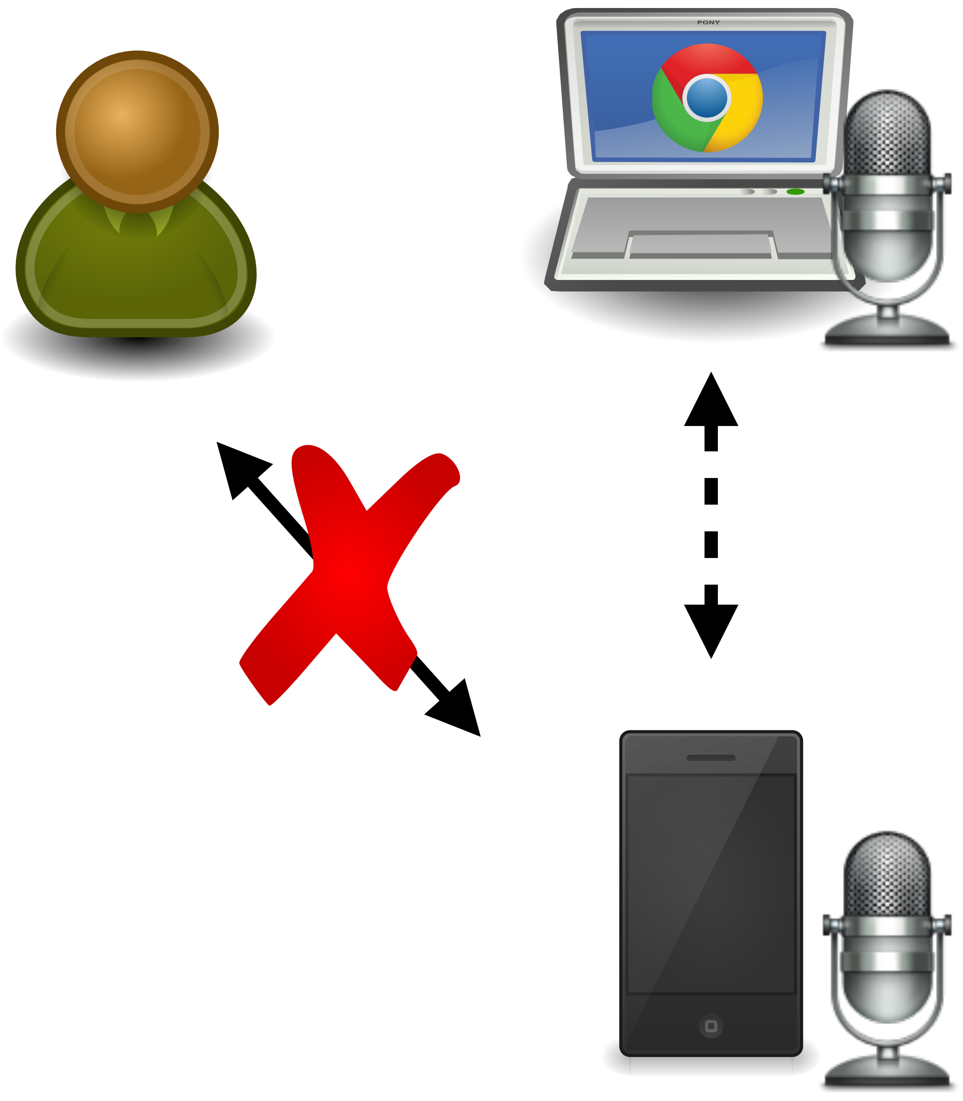
- Novel 2FA mechanism
  - Sense ambient audio to verify proximity



Contributions

Sound-Proof

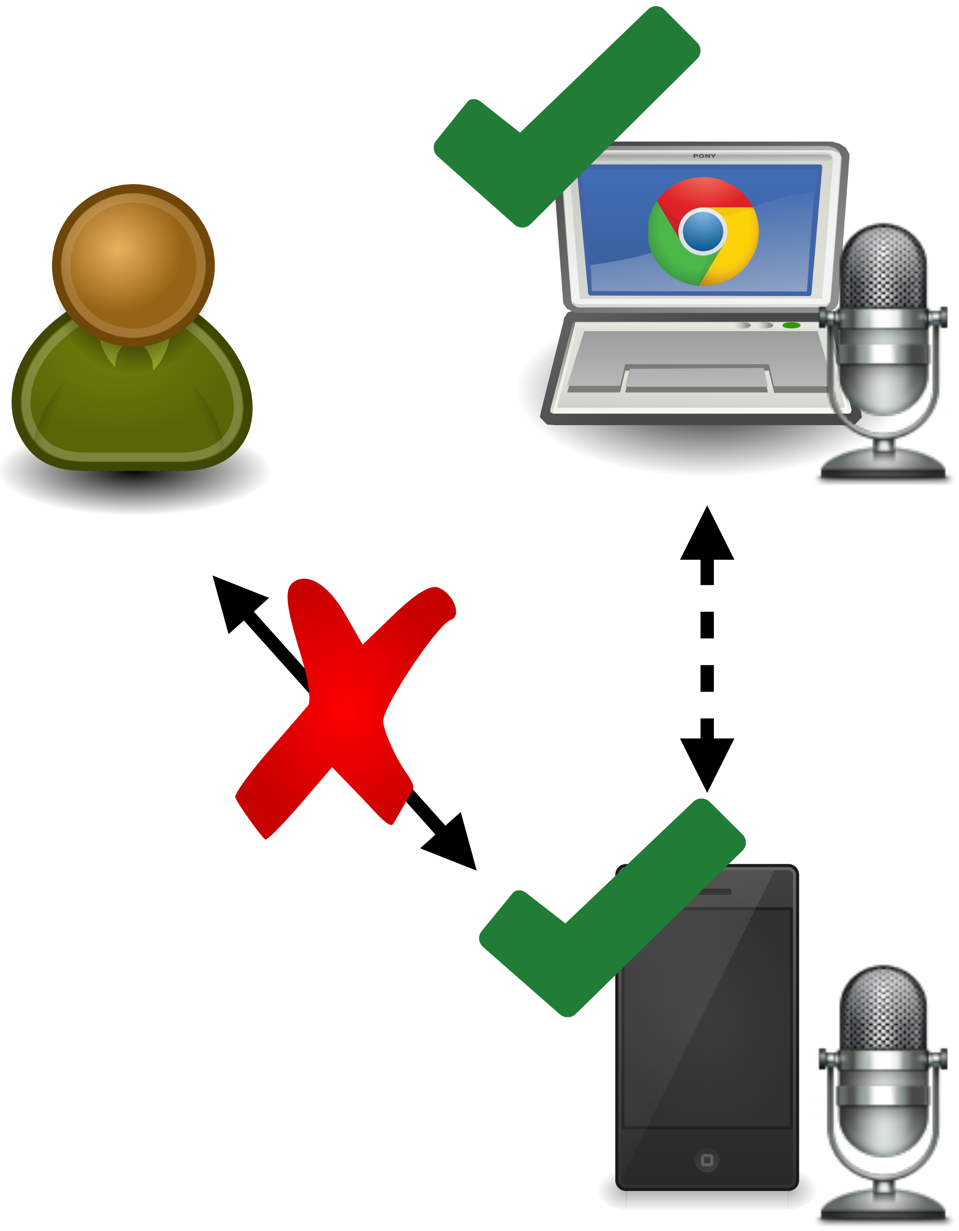
- Novel 2FA mechanism
  - Sense ambient audio to verify proximity
  - **Usable**: No user-phone interaction



Contributions

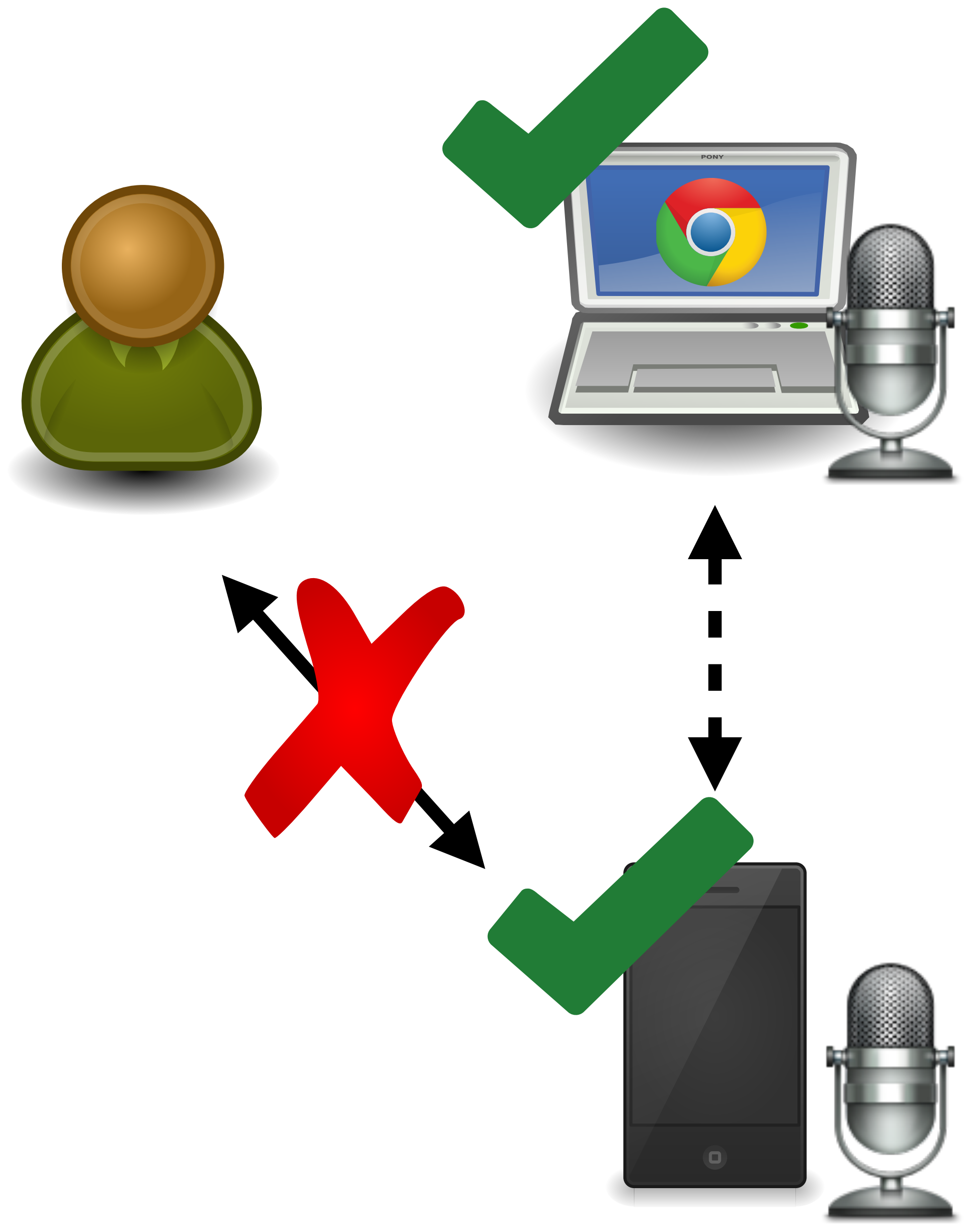
Sound-Proof

- Novel 2FA mechanism
  - Sense ambient audio to verify proximity
  - **Usable**: No user-phone interaction
  - **Deployable**: Compatible with smartphones and major browsers without plugins



Sound-Proof

- Novel 2FA mechanism
  - Sense ambient audio to verify proximity
  - **Usable**: No user-phone interaction
  - **Deployable**: Compatible with smartphones and major browsers without plugins

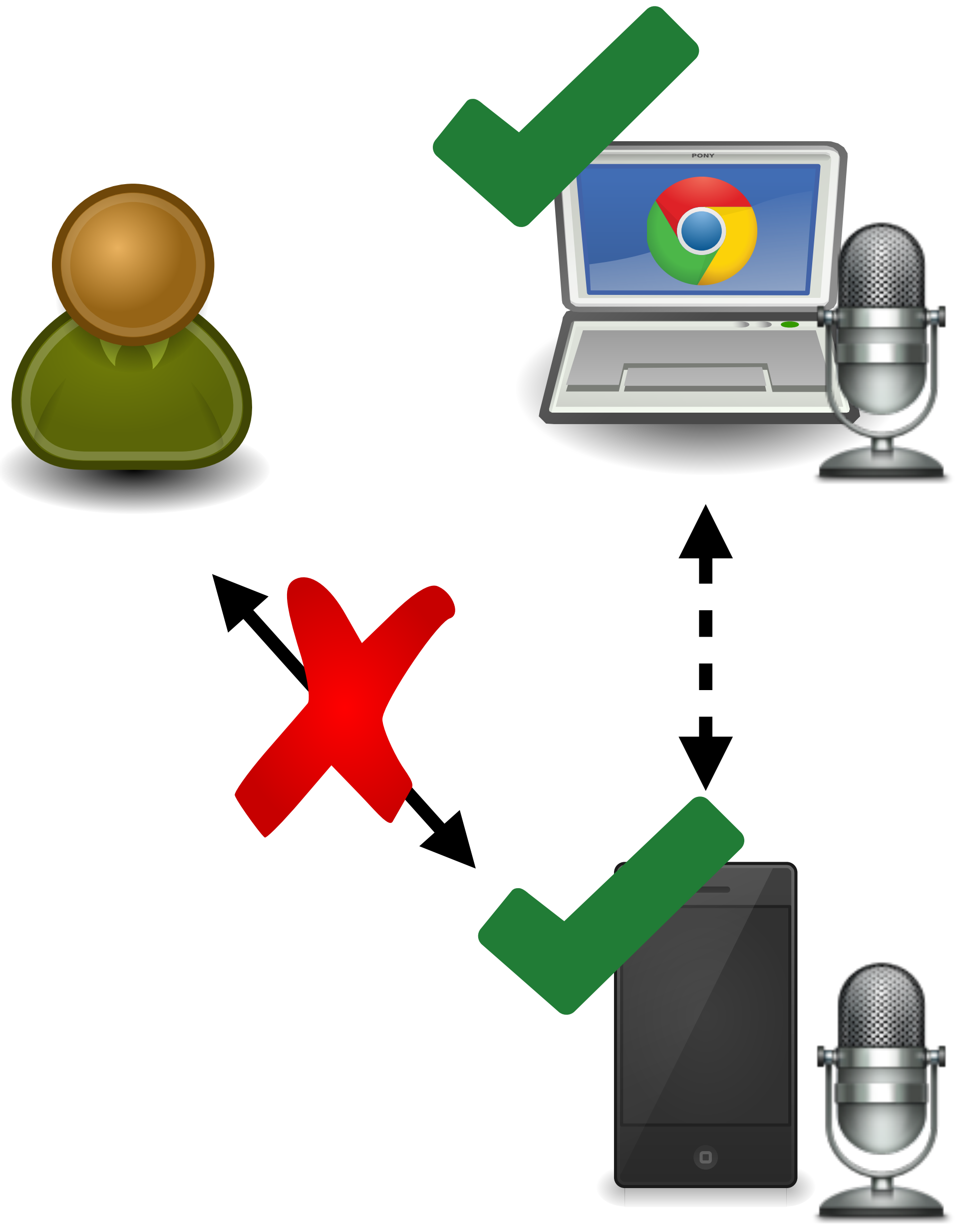


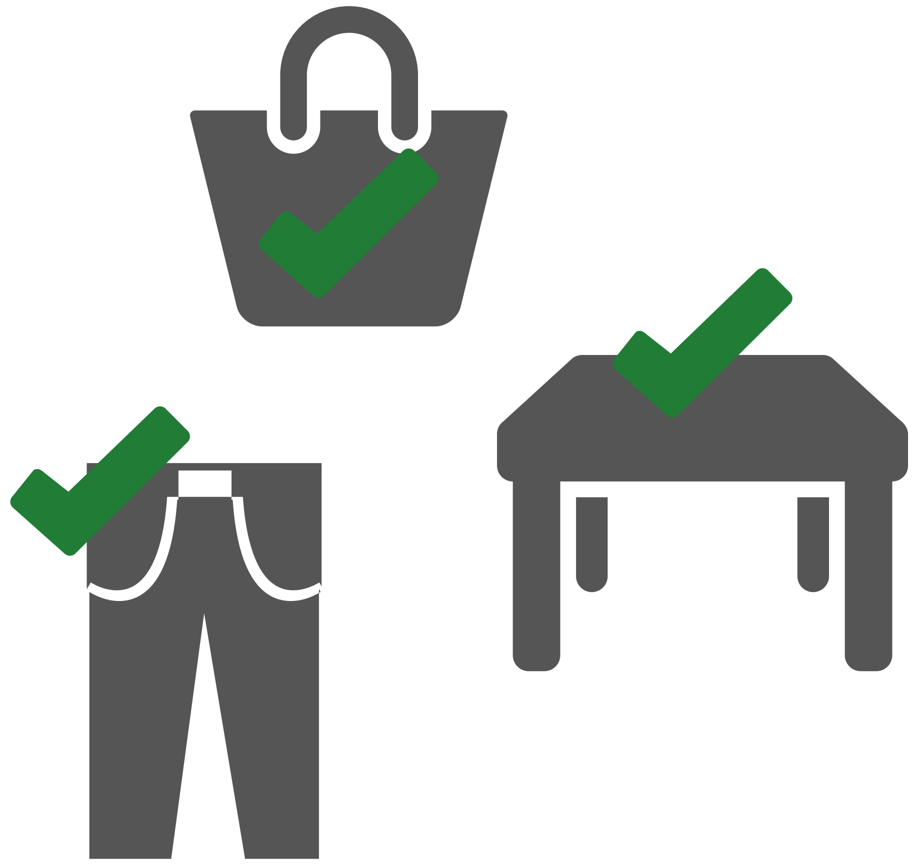
- Prototype implementation on Android and iOS

Contributions

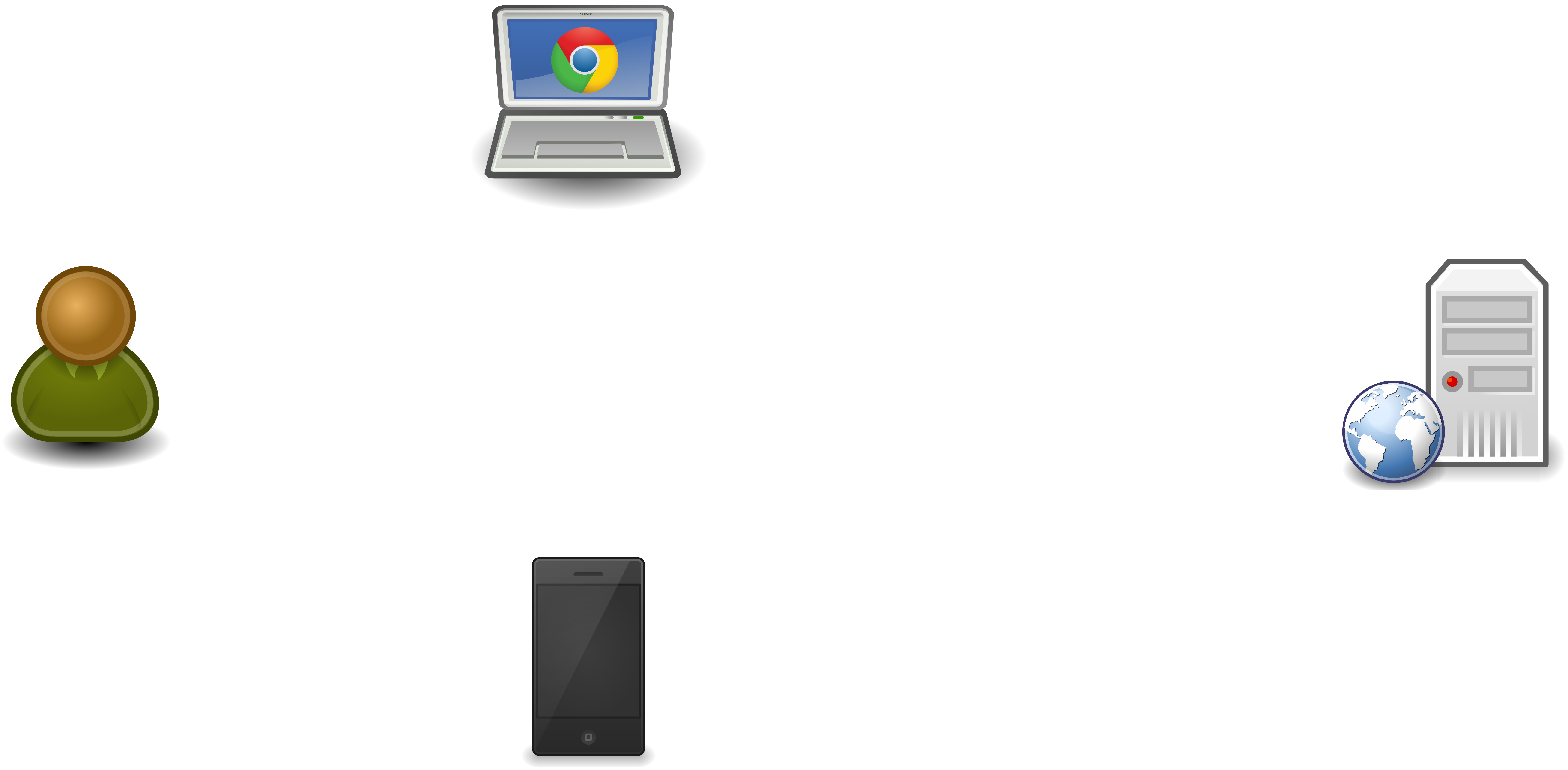
Sound-Proof

- Novel 2FA mechanism
  - Sense ambient audio to verify proximity
  - **Usable**: No user-phone interaction
  - **Deployable**: Compatible with smartphones and major browsers without plugins
- Prototype implementation on Android and iOS
- Evaluation
  - Sound-Proof works in a **variety of environments**, even if the phone is in a pocket or purse

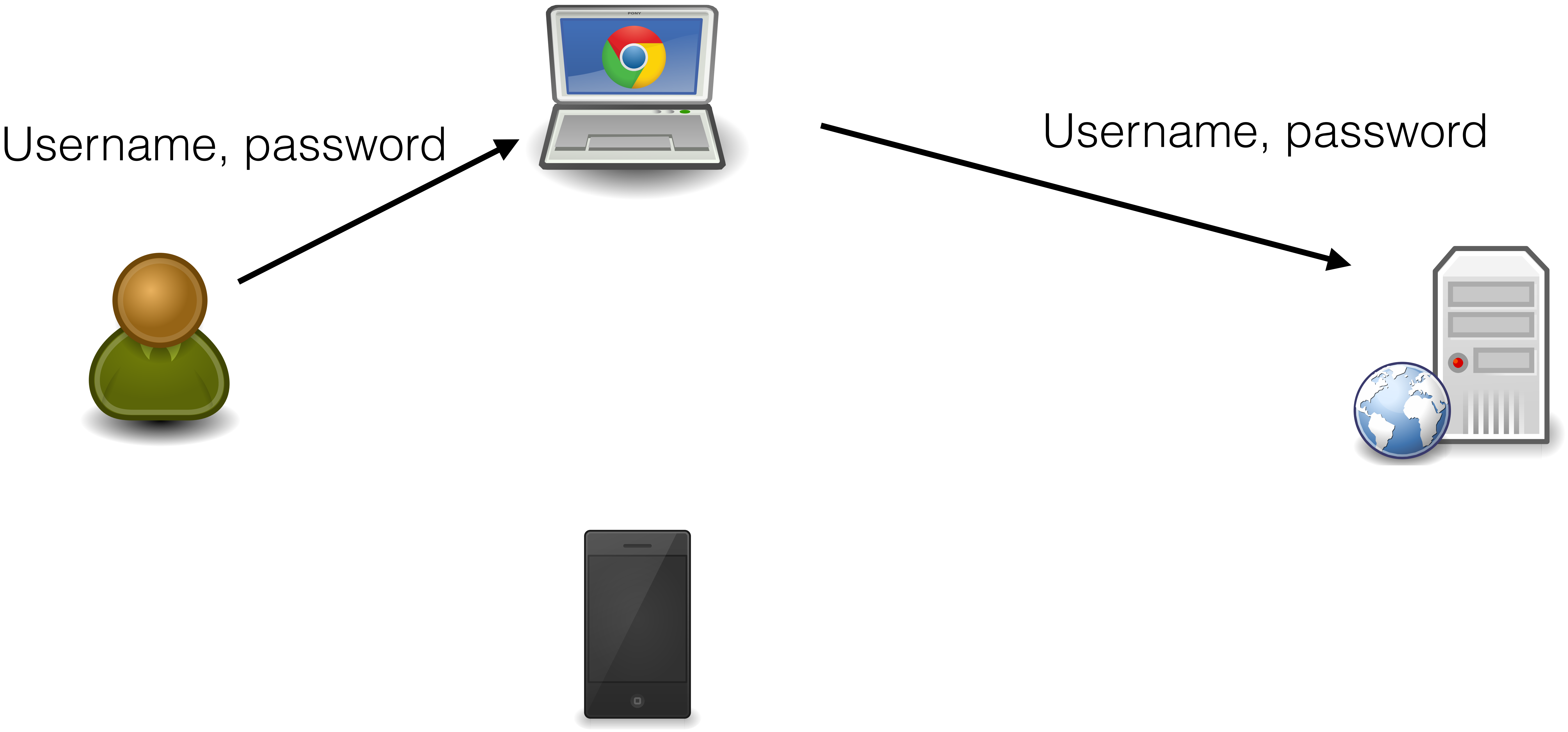




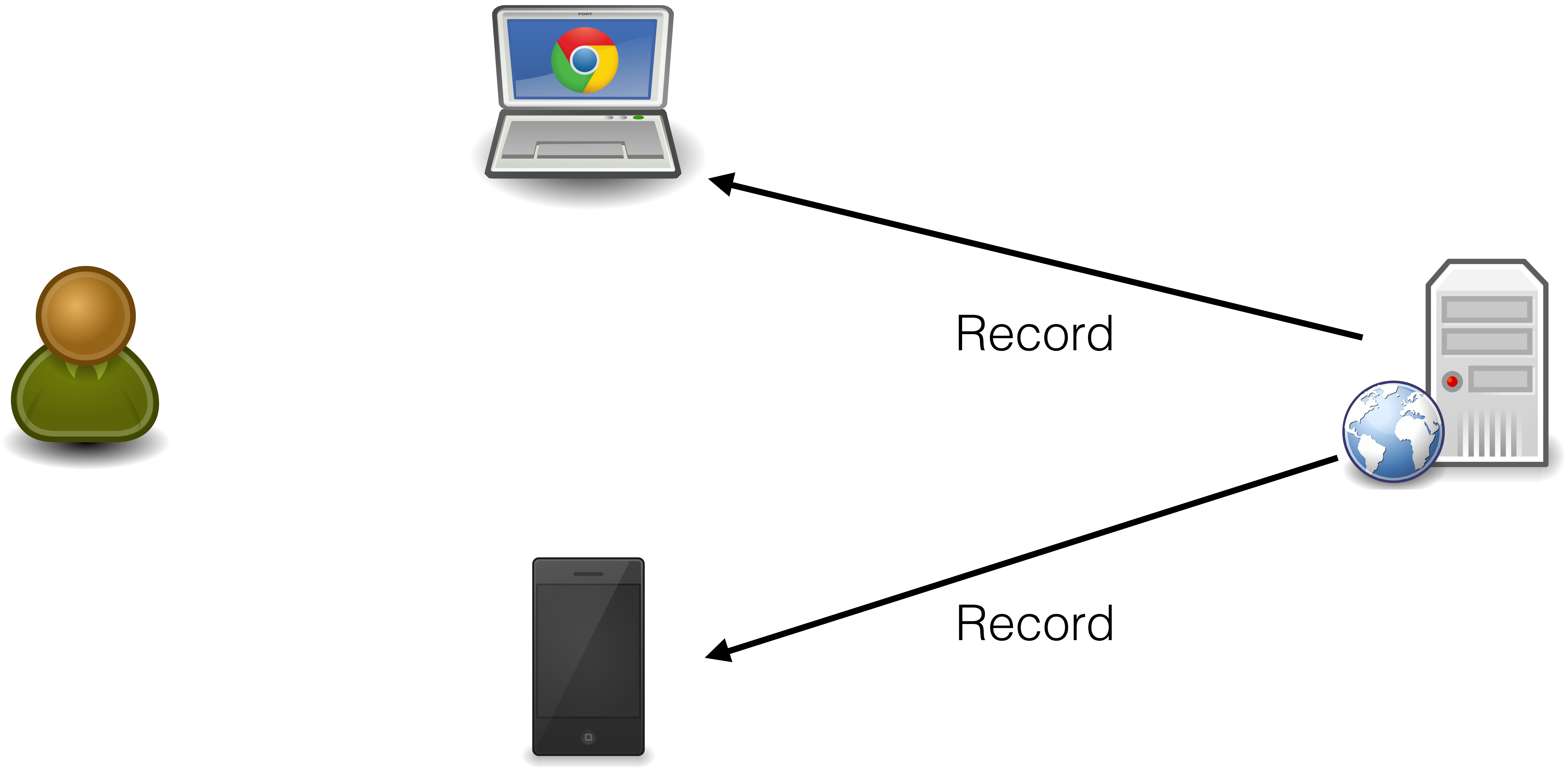
Architecture overview



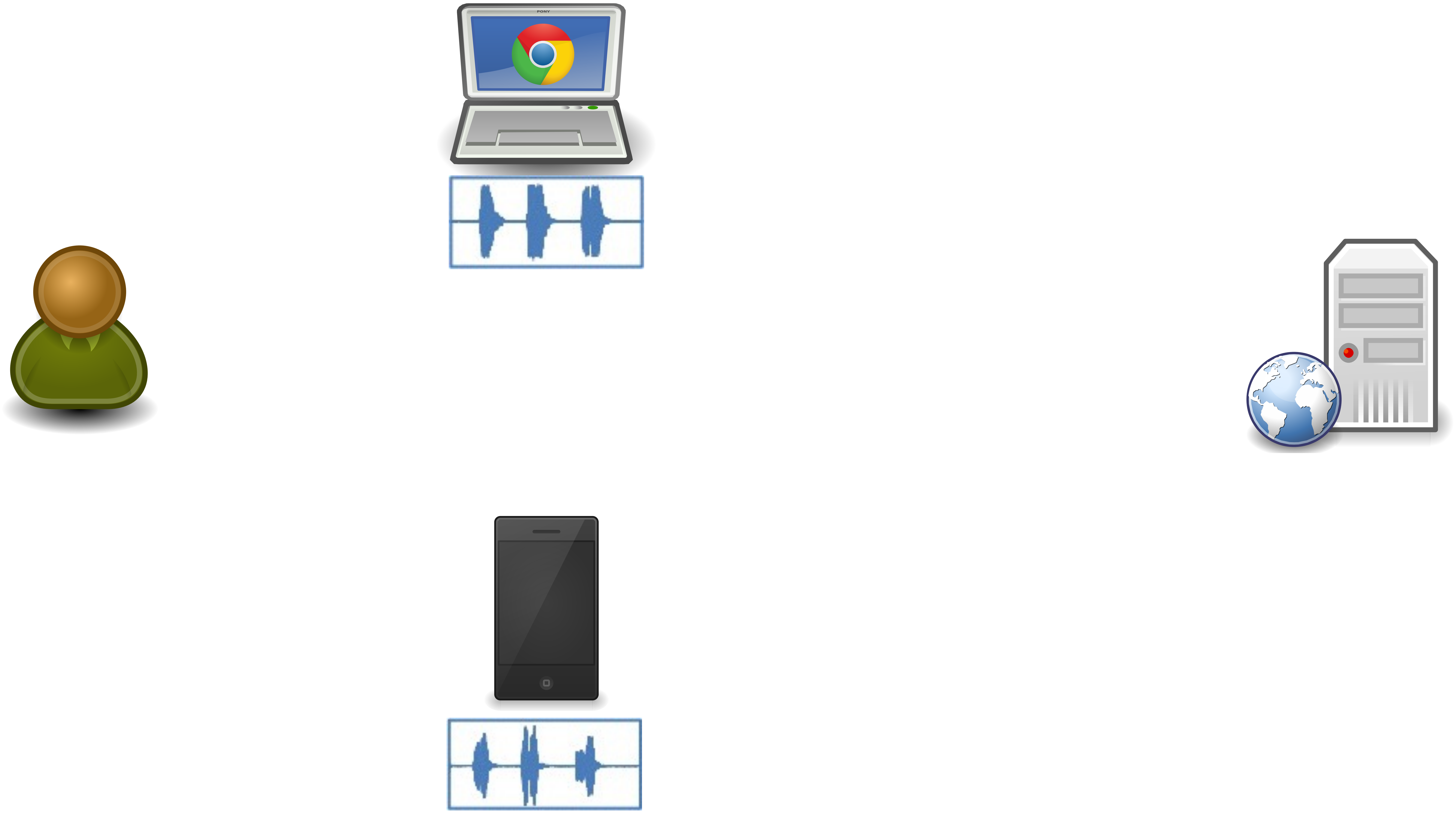
Architecture overview



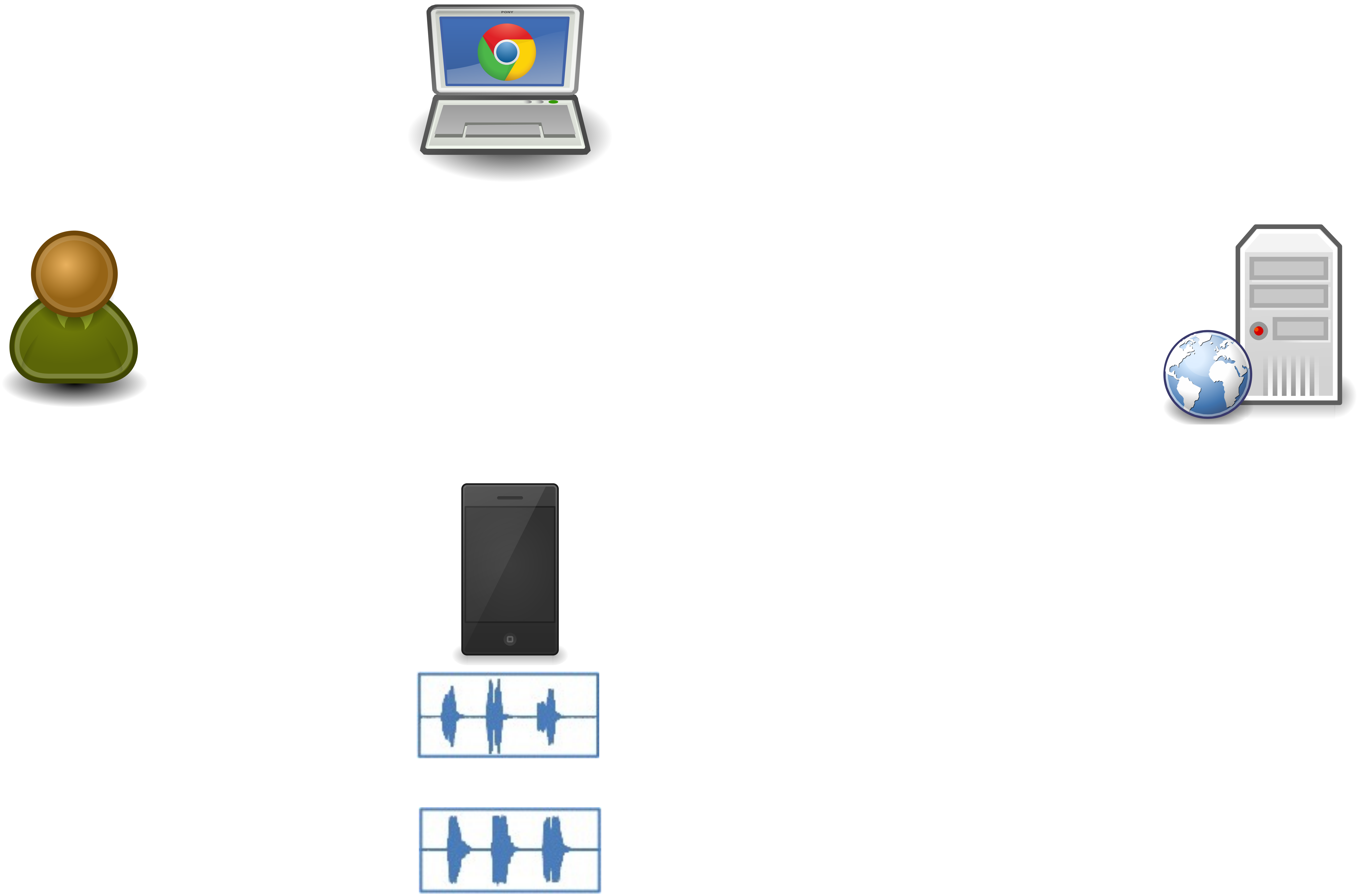
Architecture overview



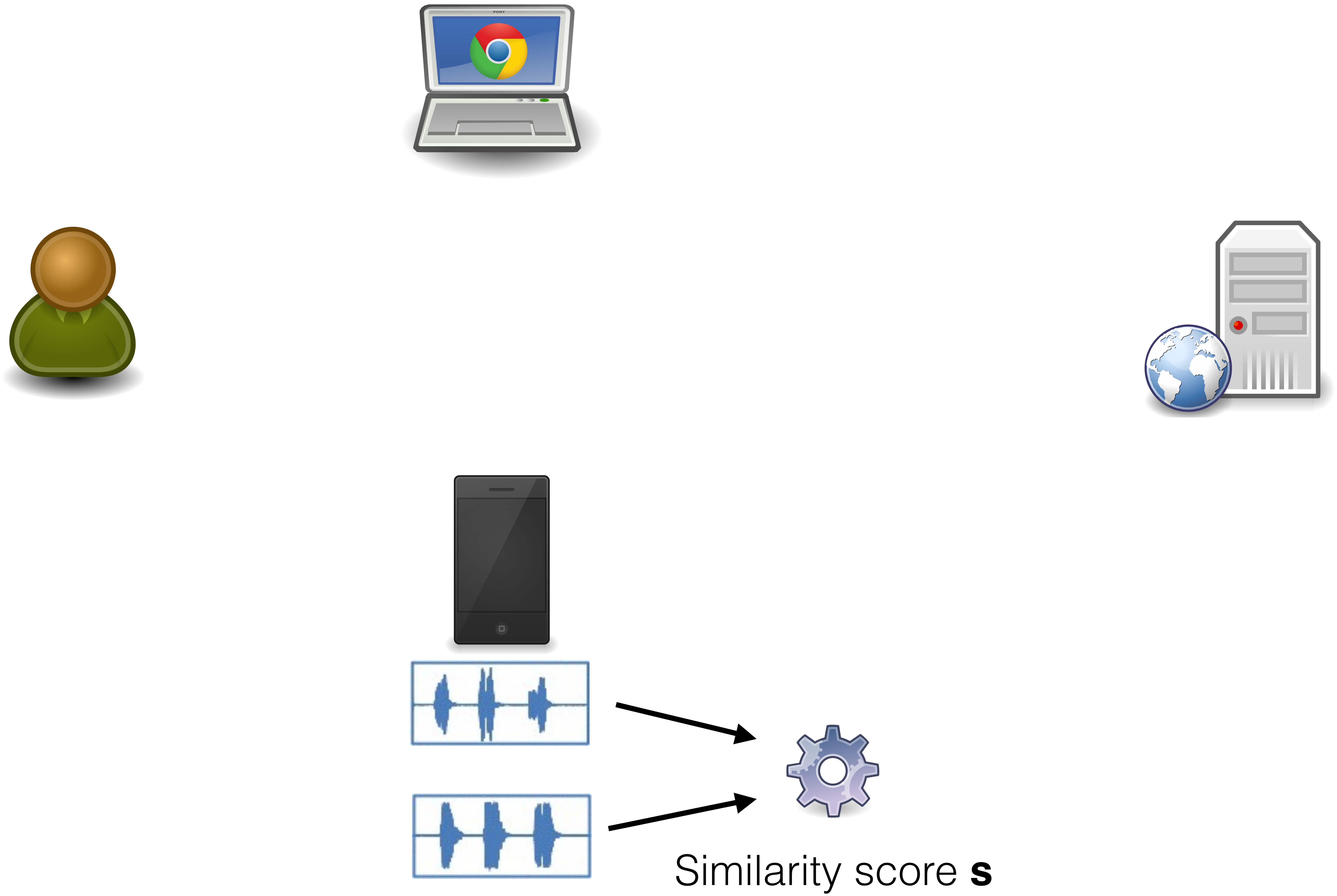
Architecture overview



Architecture overview

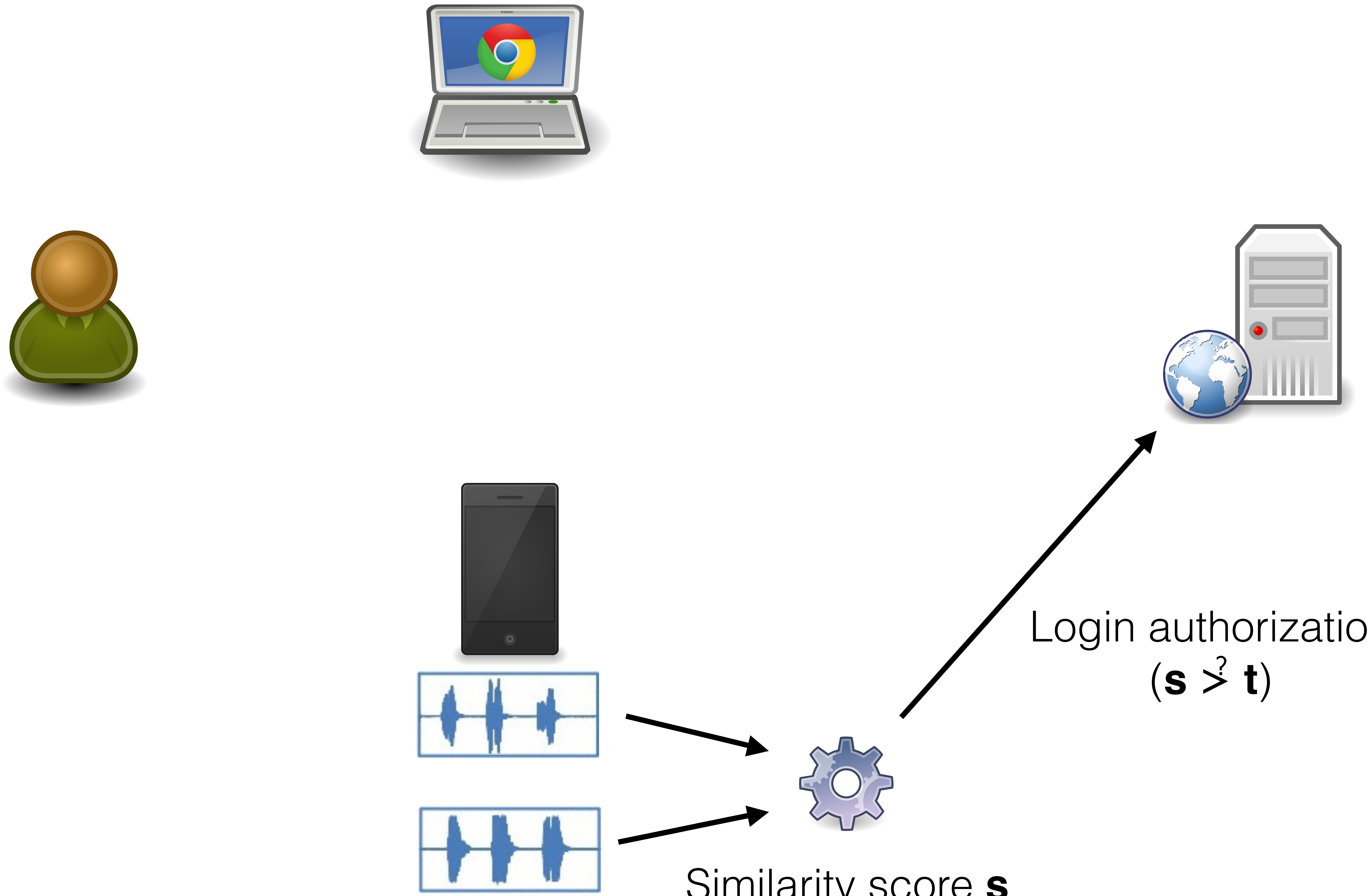


Architecture overview



Similarity score **s**

Architecture overview

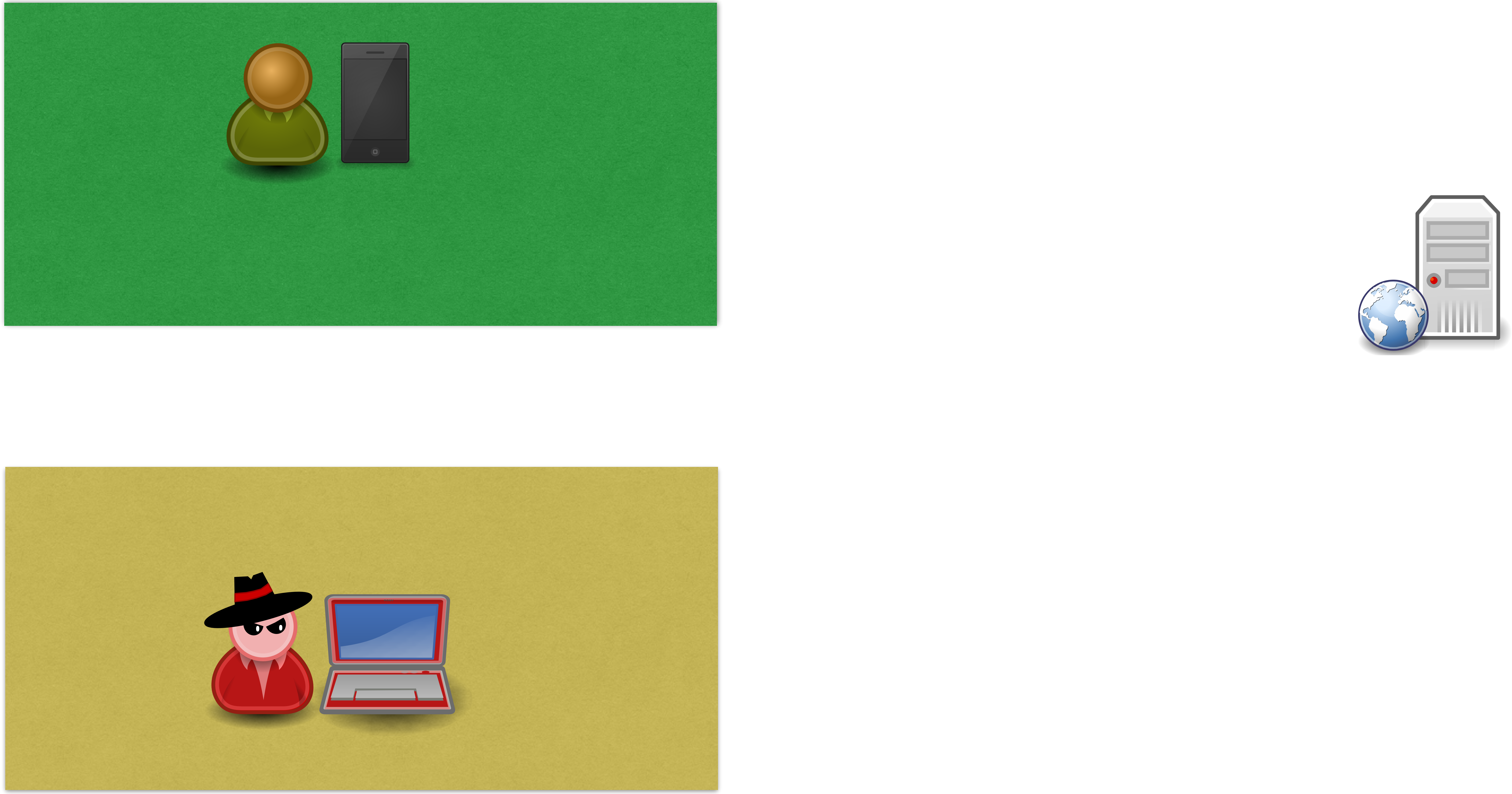


Login authorization
$(\mathbf{s} \overset{?}{>} \mathbf{t})$

Similarity score **s**

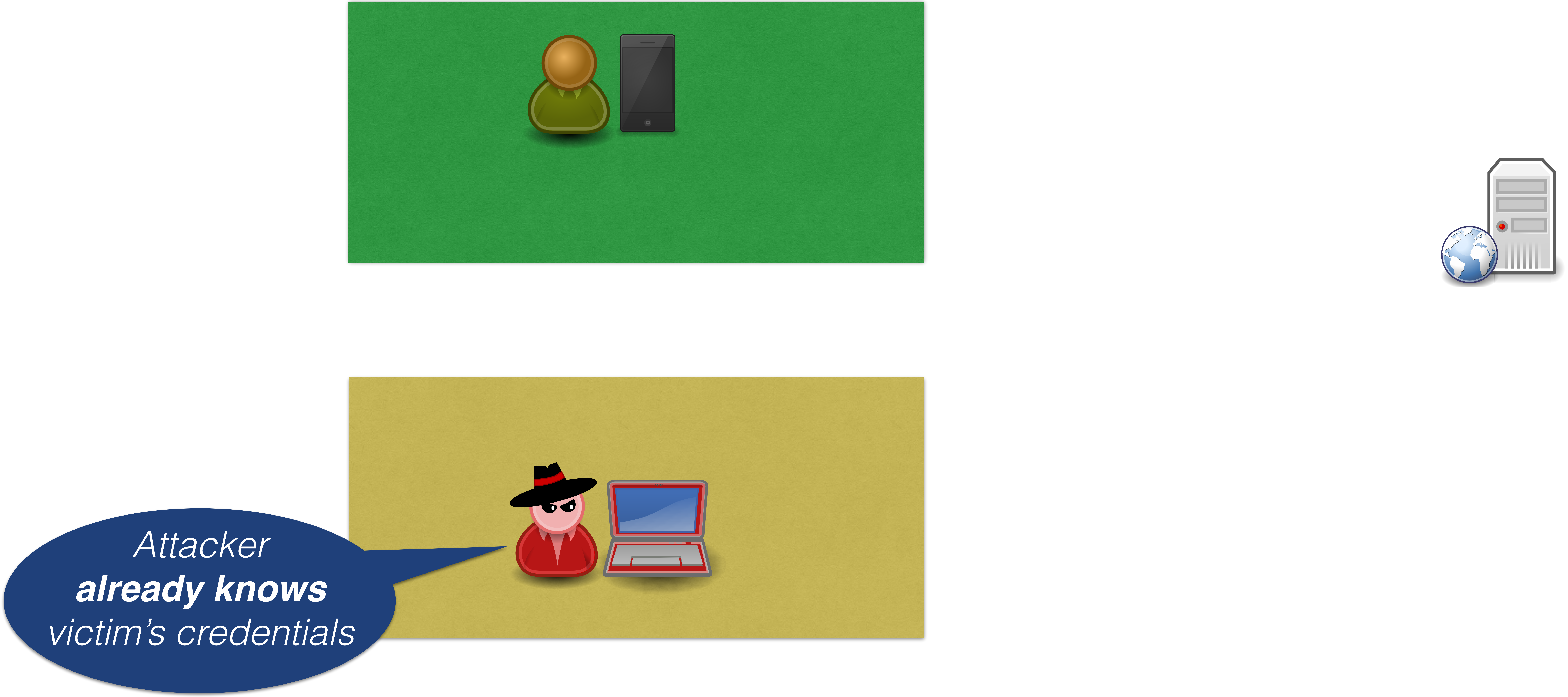
Attacker Model

Remote attacker



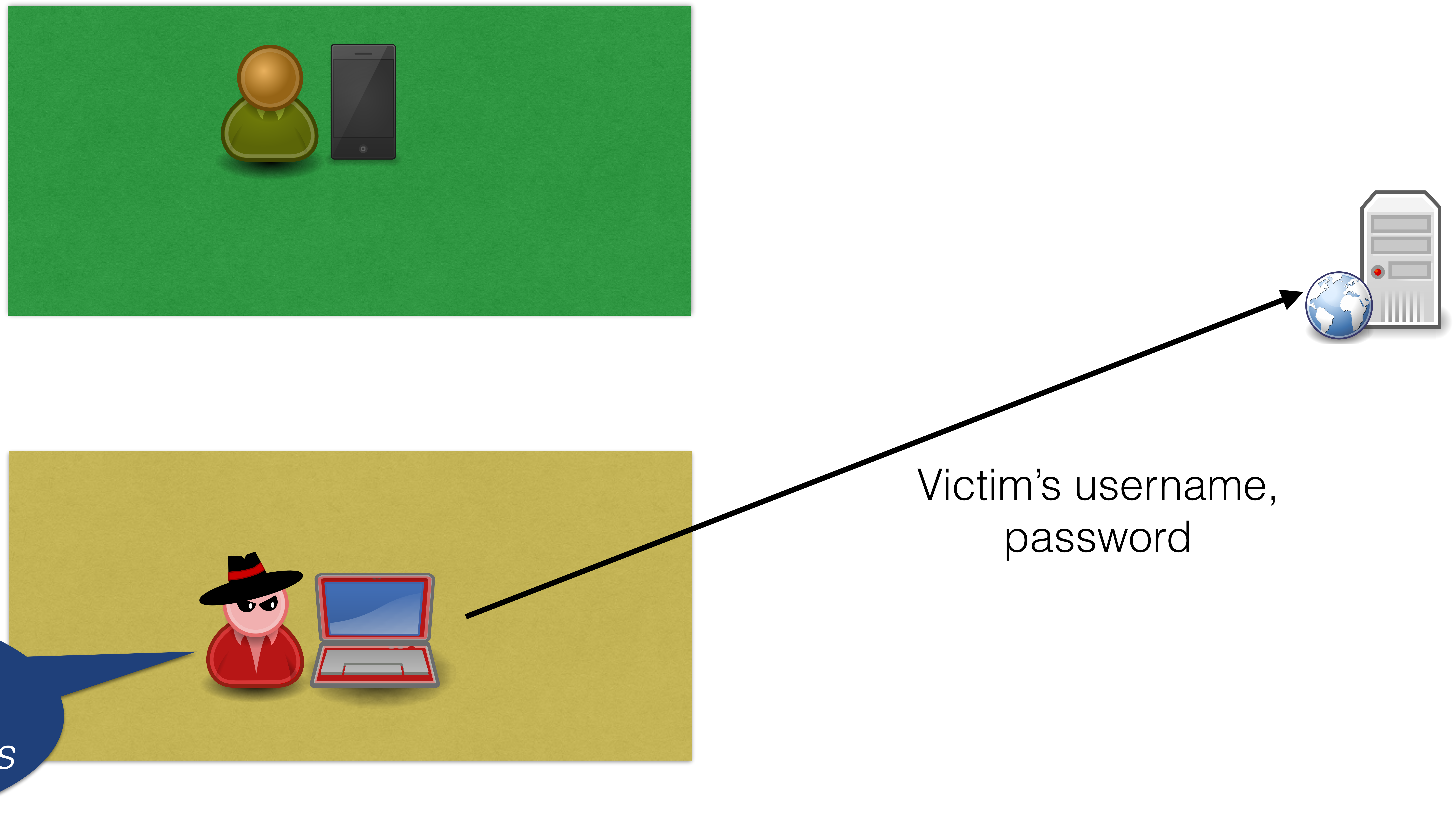
Attacker Model

Remote attacker

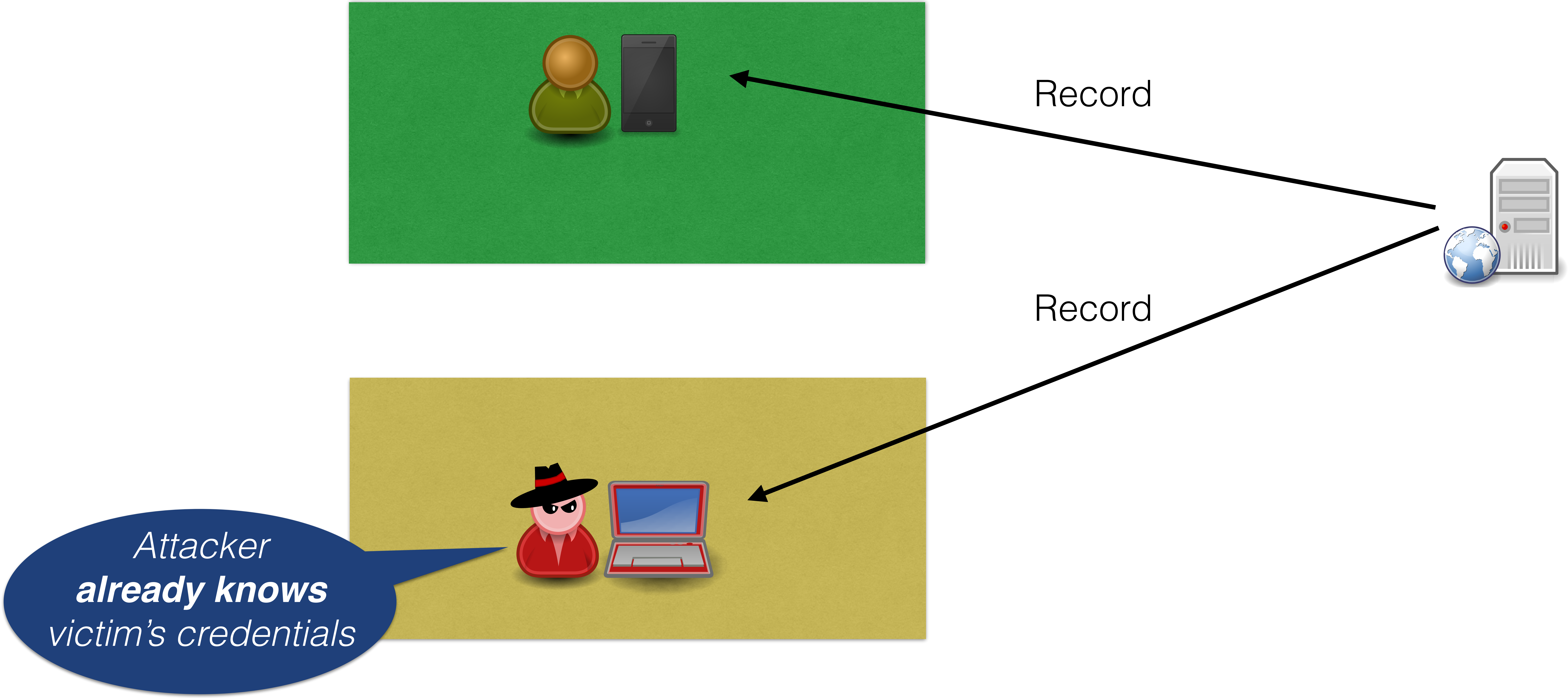


Attacker *already knows* victim's credentials

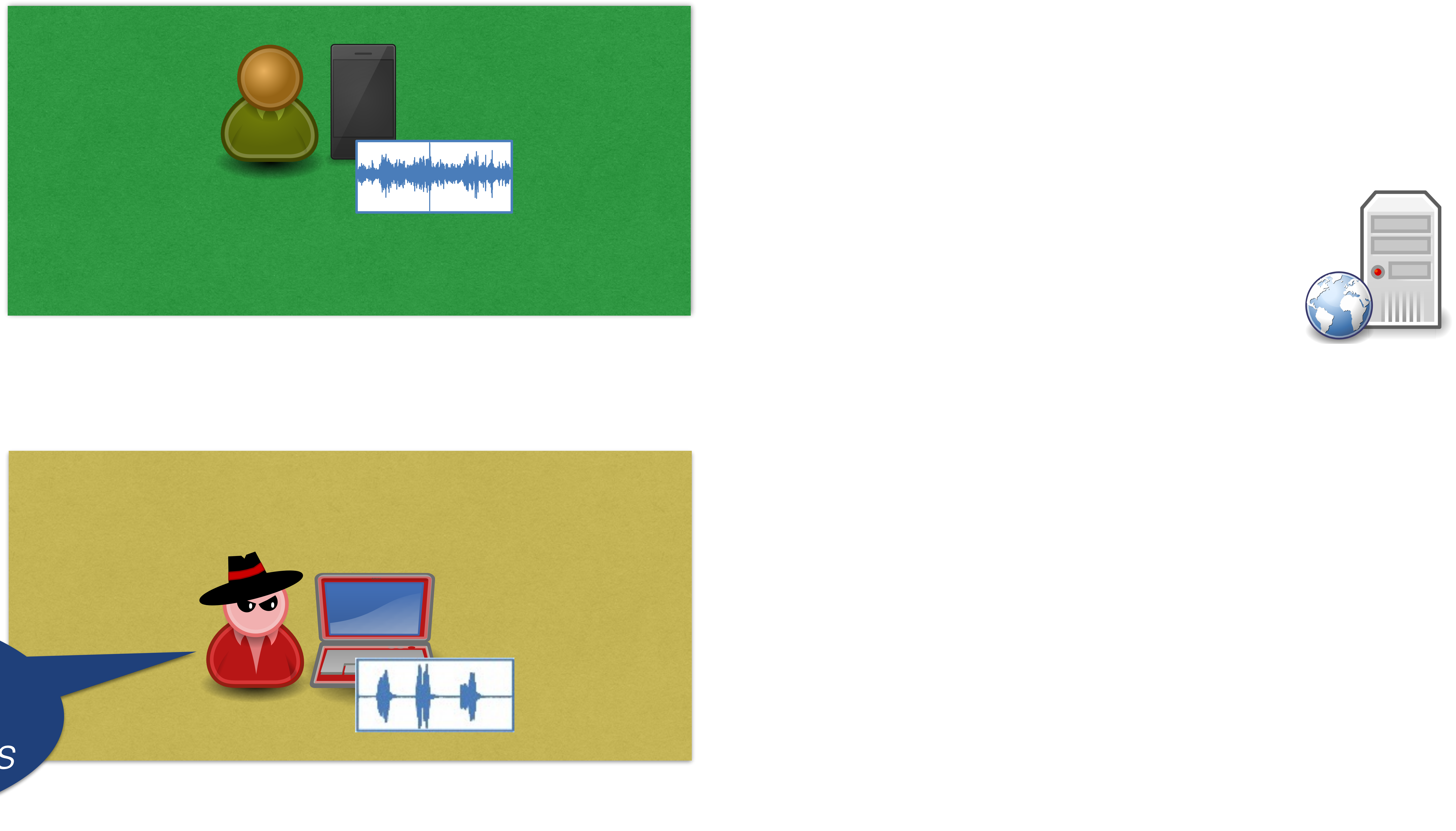
Remote attacker


Victim's username, password
Attacker *already knows* victim's credentials

Remote attacker



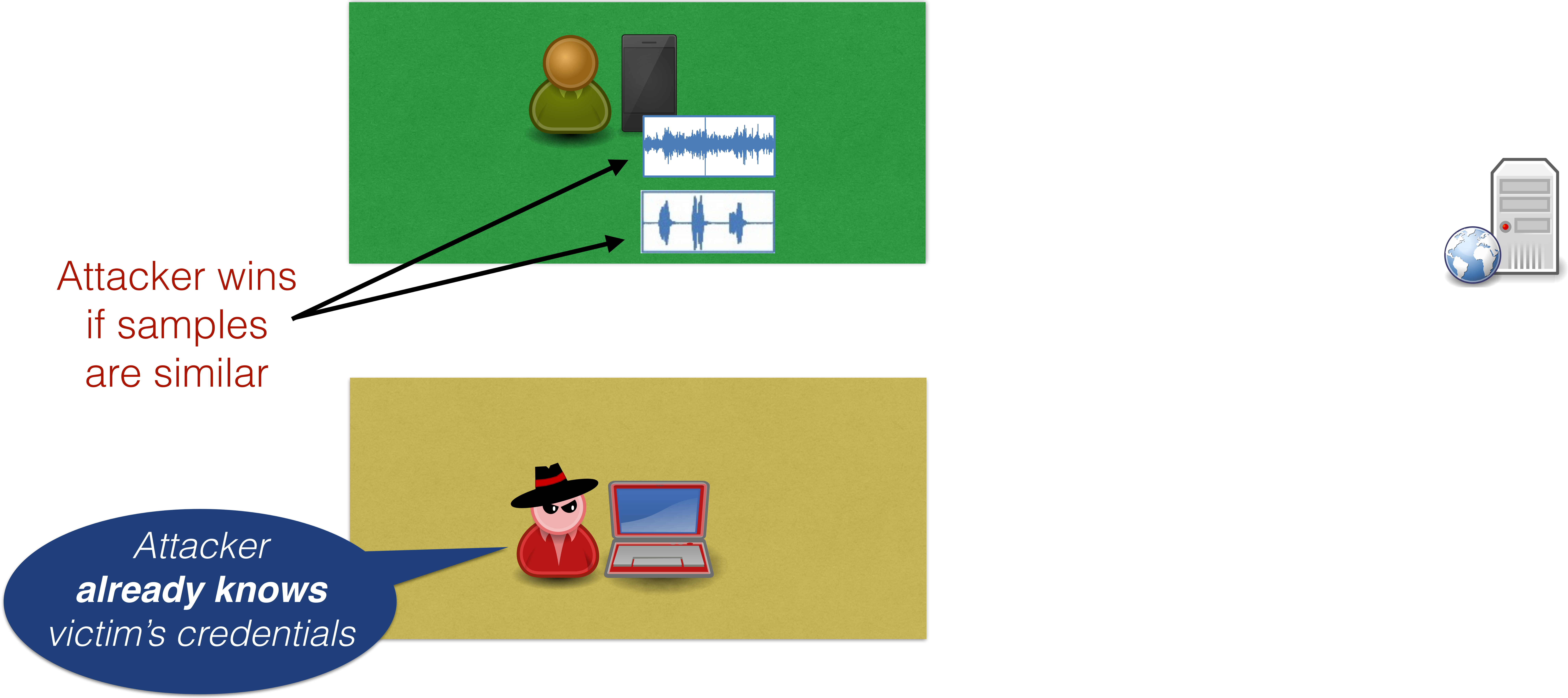
Remote attacker



Attacker **already knows** victim's credentials

Attacker Model

Remote attacker

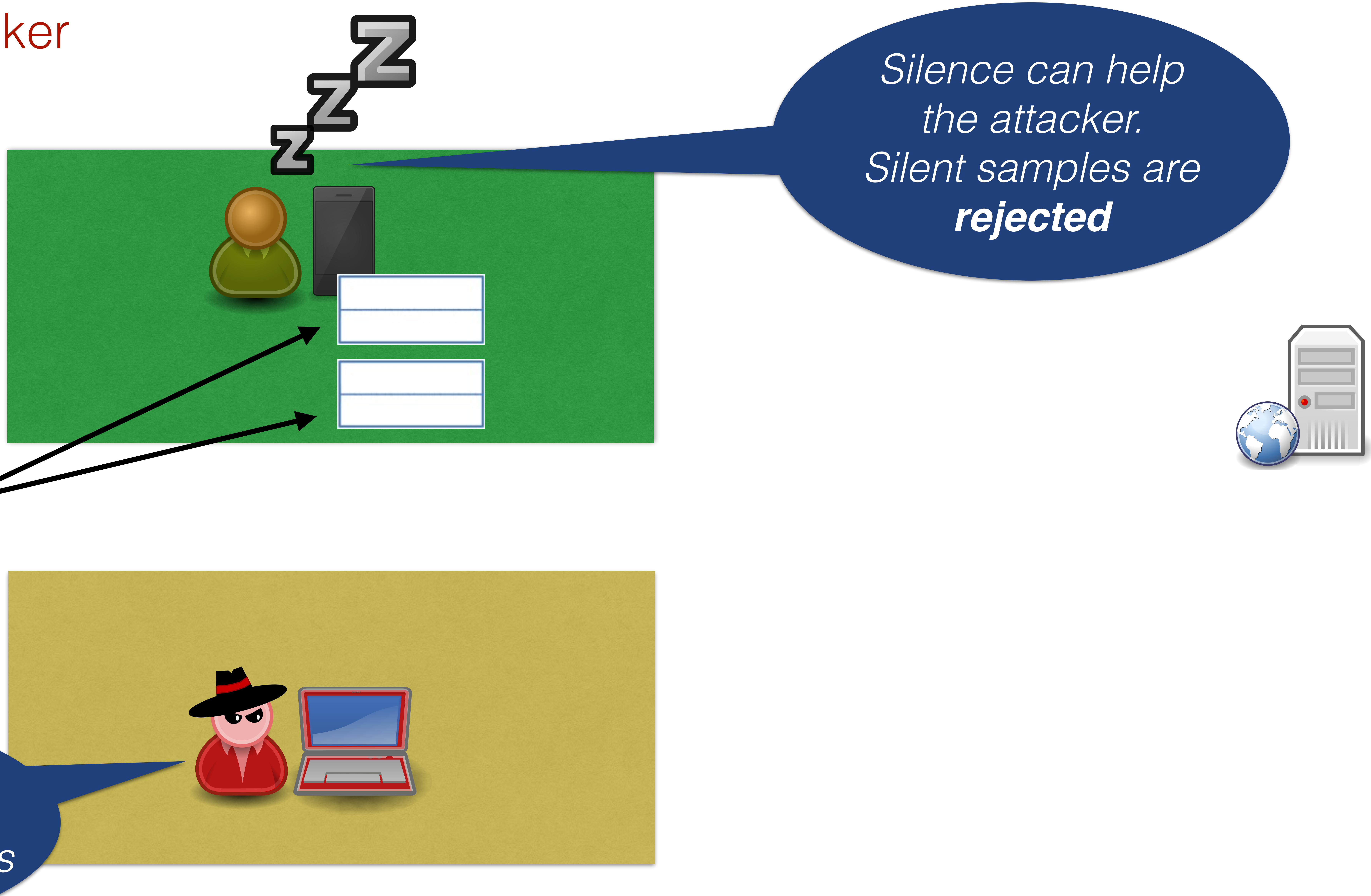


Attacker wins if samples are similar

Attacker ***already knows*** *victim's credentials*

Attacker Model

Remote attacker



*Silence can help the attacker. Silent samples are **rejected***

Attacker wins if samples are similar

*Attacker **already knows** victim's credentials*

Sound-Proof Evaluation

ETHzürich

Performance

Sound-Proof Evaluation

Performance

- Total time: User clicks “login” —> browser refresh to log the user in
  - Recording time: 3 seconds

Sound-Proof Evaluation

Performance

- Total time: User clicks “login” —> browser refresh to log the user in
  - Recording time: 3 seconds

	Total Time (mean)
WiFi	4677ms (±181ms)
Cellular	4944ms (±233ms)

Phone network connectivity

Sound-Proof Evaluation

Performance

- Total time: User clicks “login” —> browser refresh to log the user in
  - Recording time: 3 seconds
- Room for **improvement**
  - Compress and/or stream browser recording

	Total Time (mean)
WiFi	4677ms (±181ms)
Cellular	4944ms (±233ms)

Phone network connectivity

Audio Collection Campaign (2 subjects over 4 weeks)

- **Environment**
  - office, office-music, home-TV, lecture room, train station, café
- **Laptop**
  - MacBook Pro Mid 2012, Dell E6510 (using Google Chrome)
- **Phone**
  - iPhone 5, Google Nexus 4
- **Phone position**
  - outside, in pocket, in purse
- **User activity**
  - being silent, talking, coughing, whistling

4014 audio samples (2007 login attempts)

Sound-Proof Evaluation

Parameter Tuning

Parameter Tuning

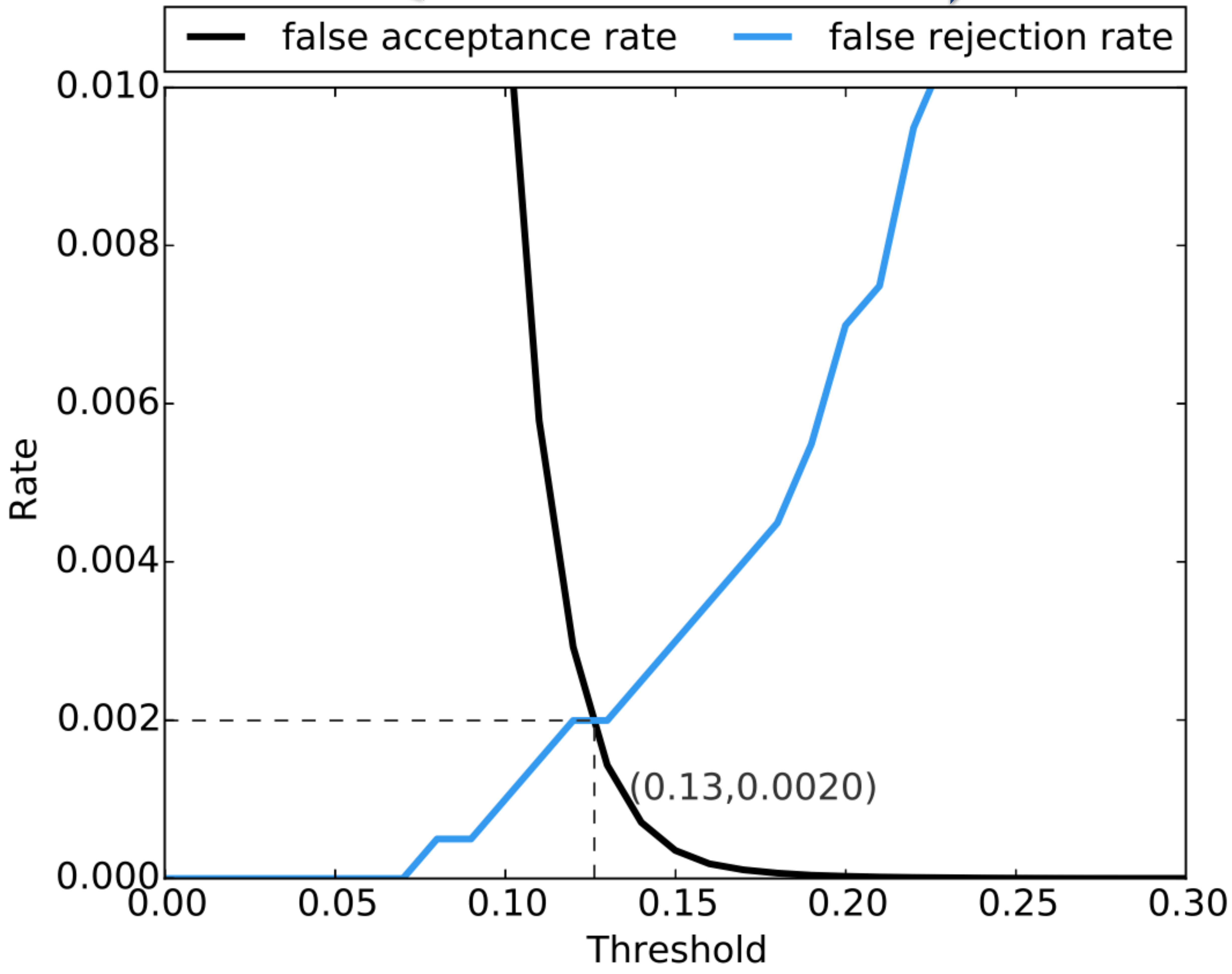
- Frequency bands
  - ≥ 50Hz (low frequency noise)
  - ≤ 4kHz (fading, directionality)

Parameter Tuning

- Frequency bands
  - ≥ 50Hz (low frequency noise)
  - ≤ 4kHz (fading, directionality)

Fraudulent logins not detected

Legitimate logins rejected



Sound-Proof Evaluation

Parameter Tuning

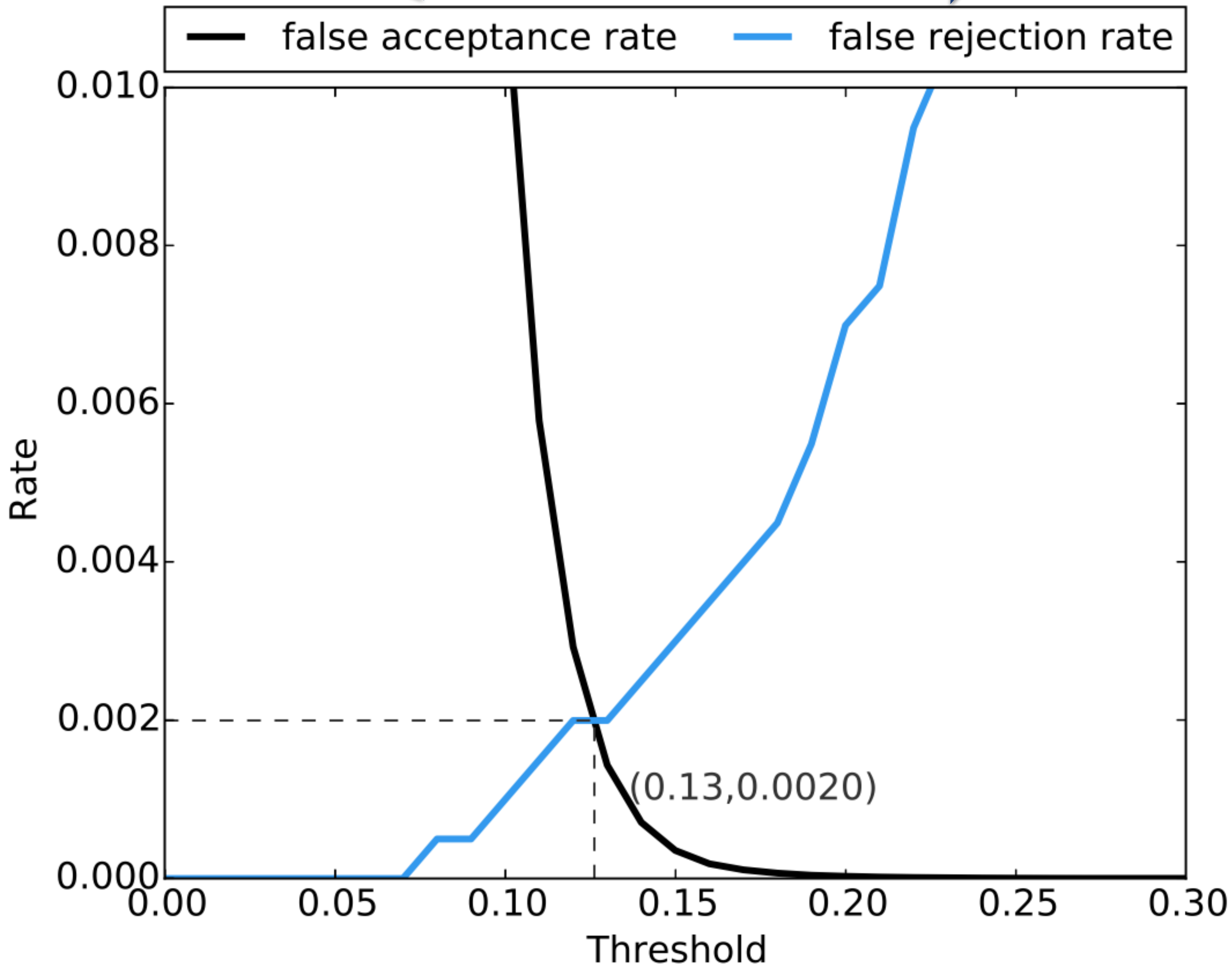
- Frequency bands
  - ≥ 50Hz (low frequency noise)
  - ≤ 4kHz (fading, directionality)

- Similarity score threshold t = 0.13
  - **Equal Error Rate = 0.002**

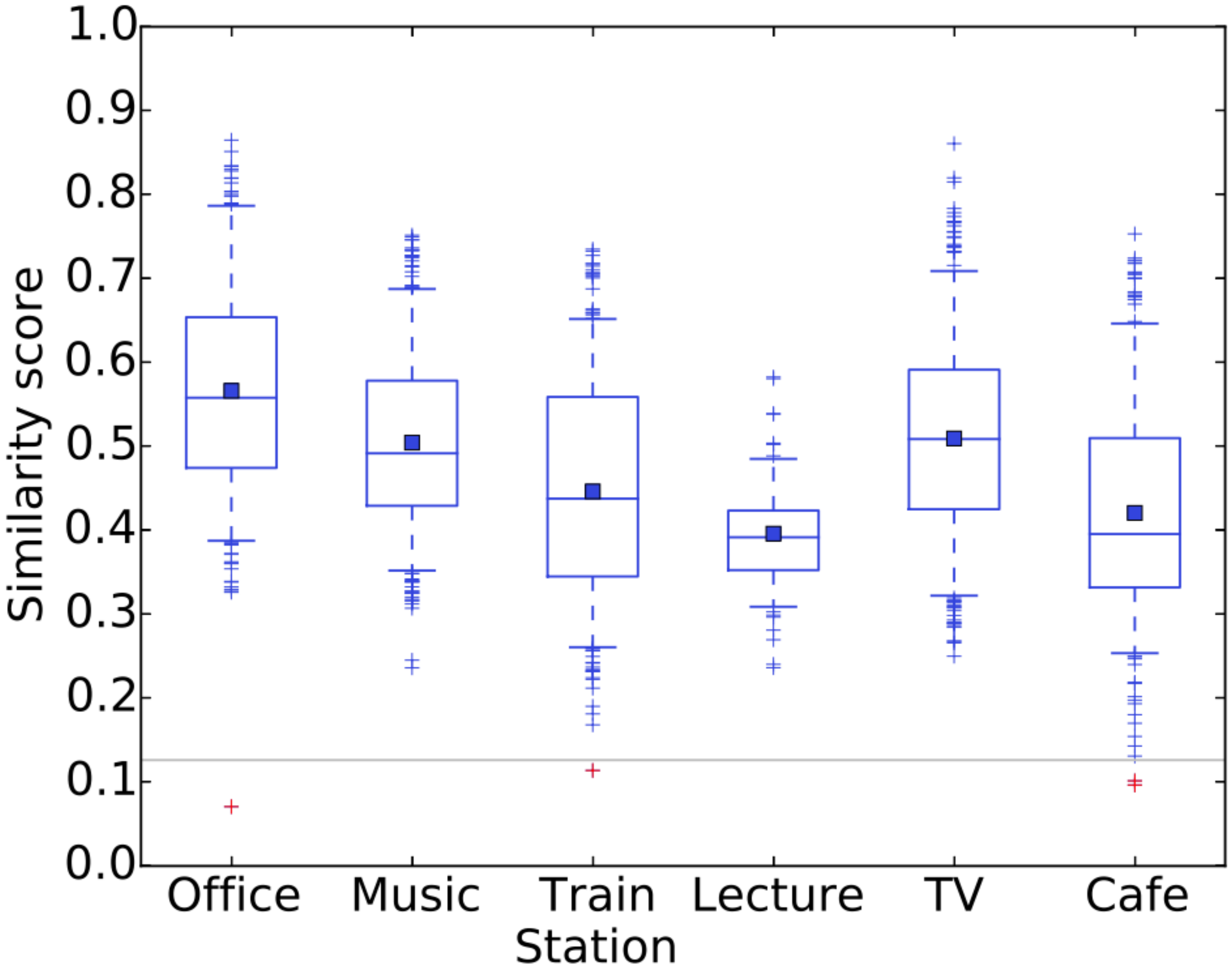
0.2%

Fraudulent logins not detected

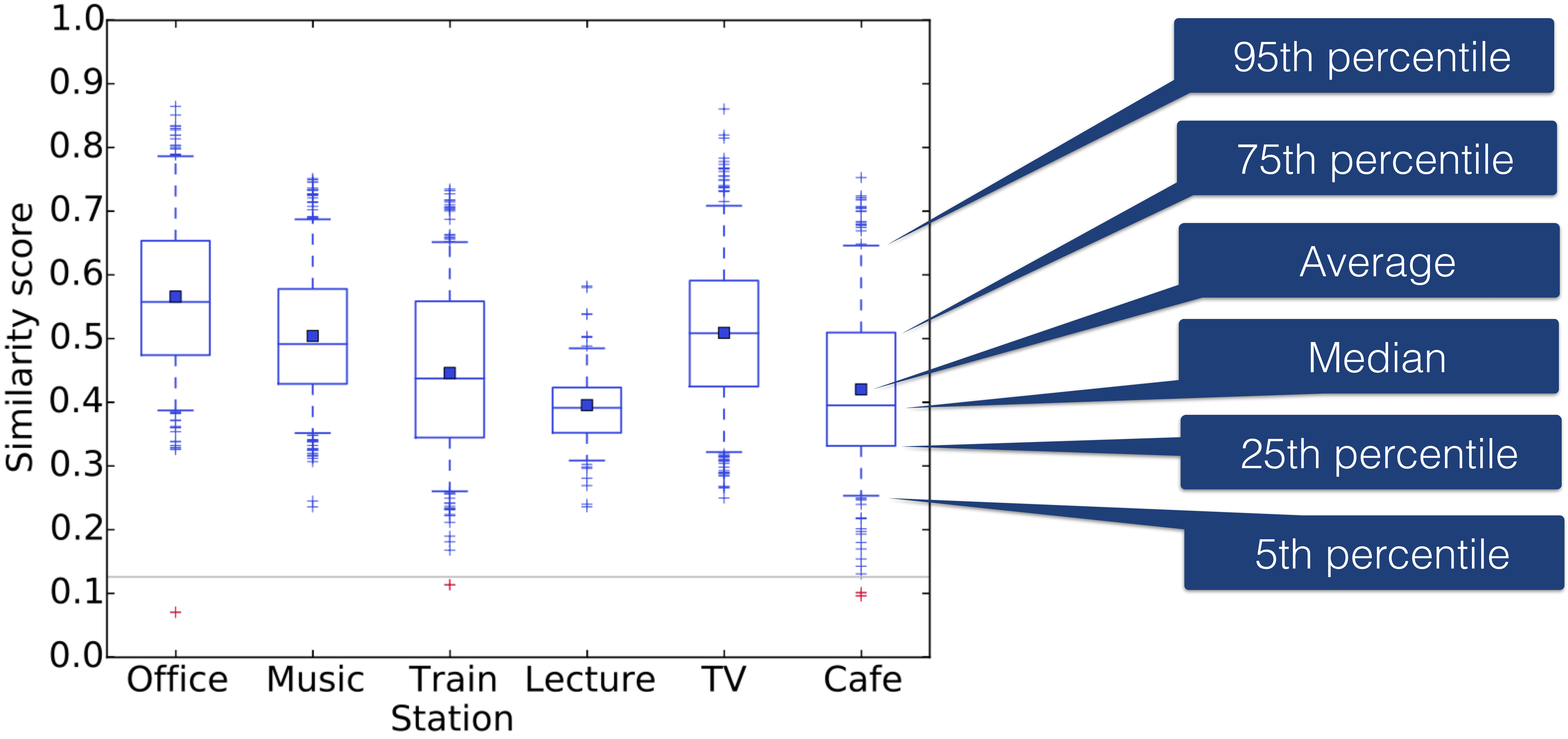
Legitimate logins rejected



Impact of environment



Impact of environment



95th percentile

75th percentile

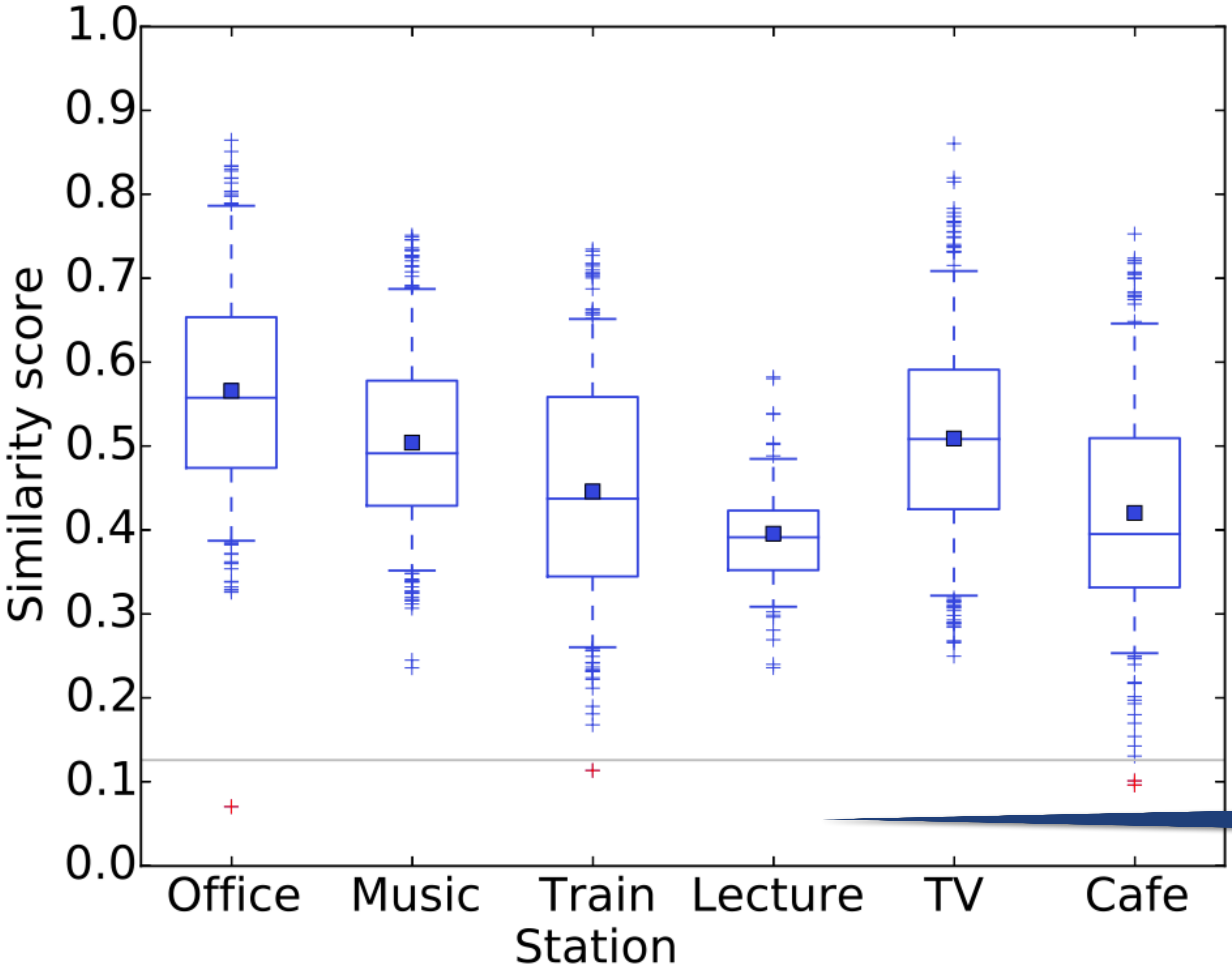
Average

Median

25th percentile

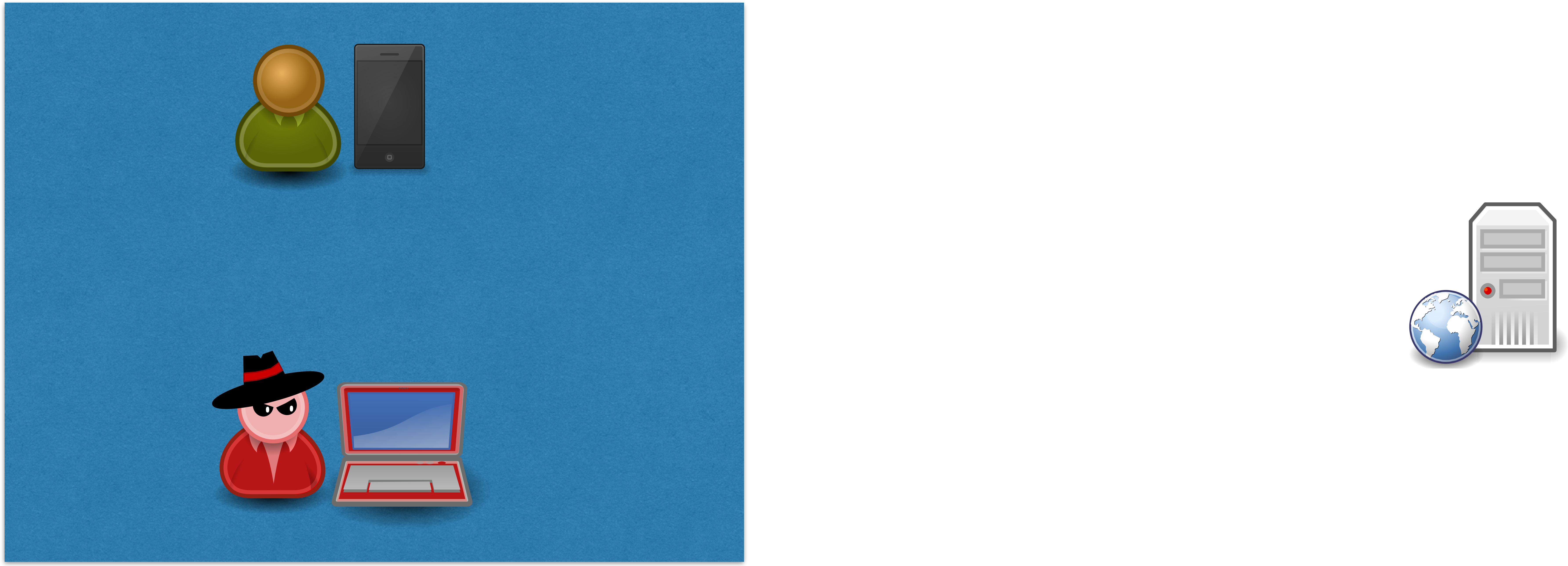
5th percentile

Impact of environment



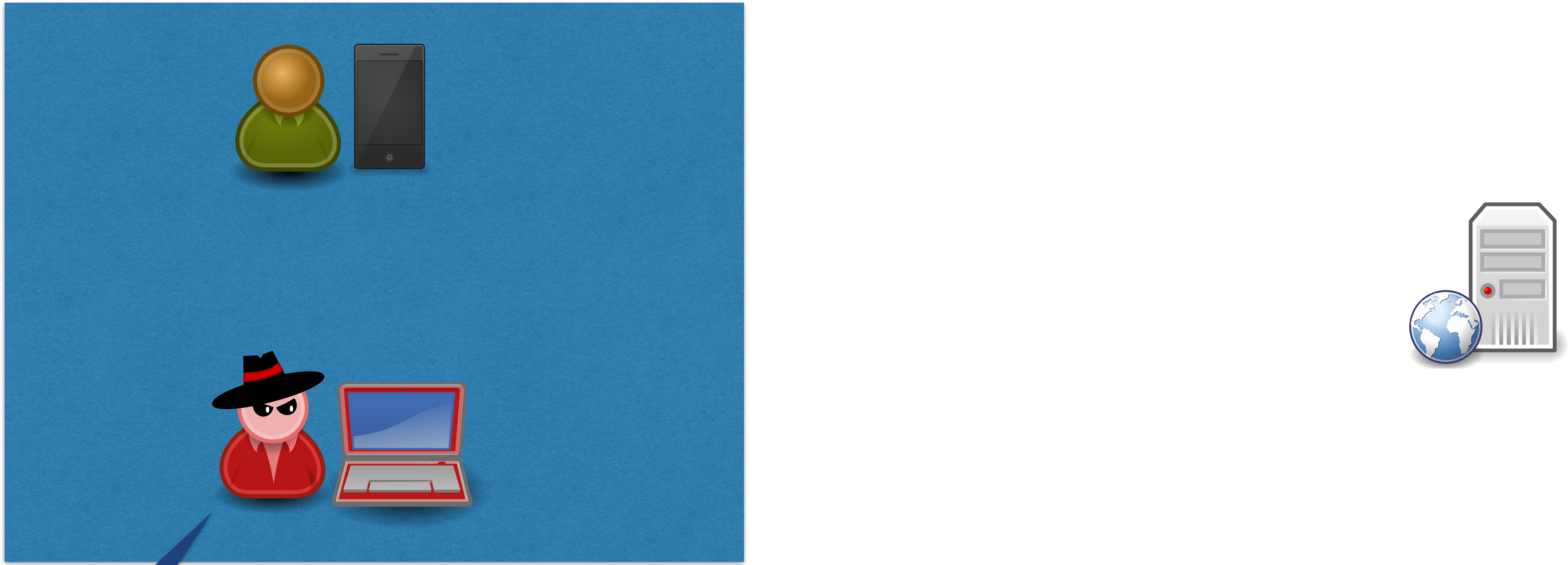
4 false rejections out of **2007**

Co-located attackers



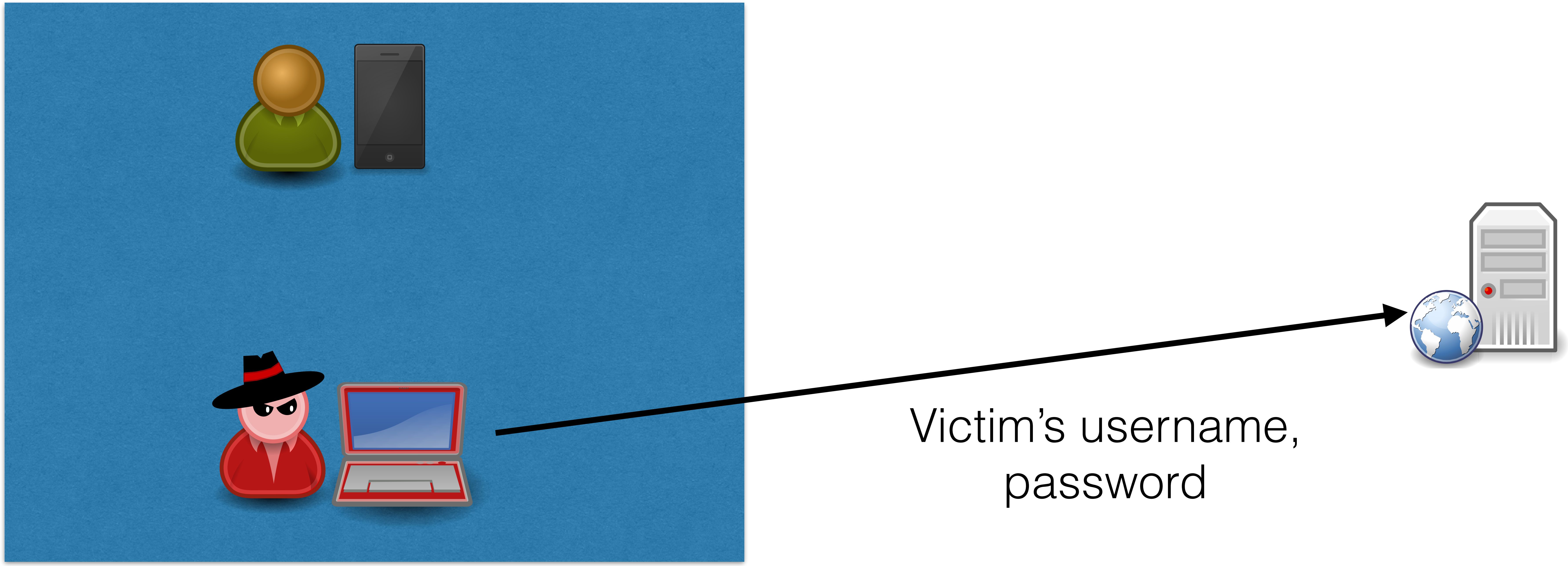
Security Evaluation

Co-located attackers



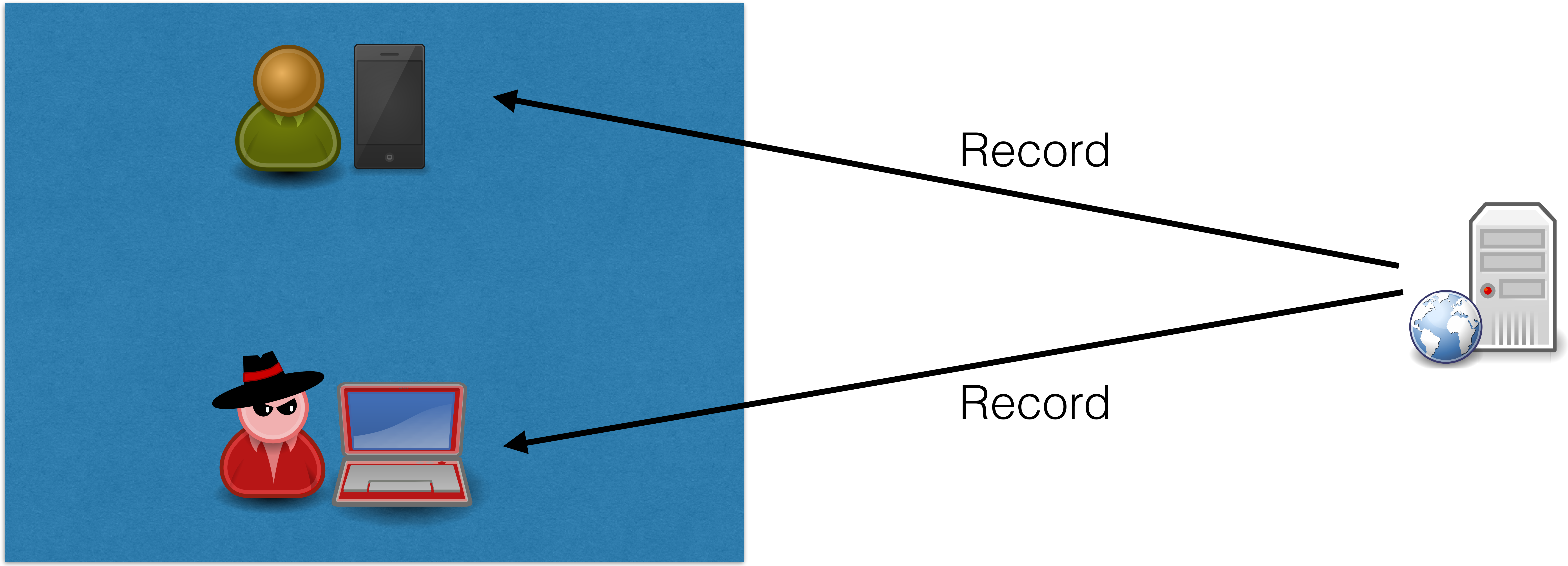
Attacker already knows victim's credentials

Co-located attackers

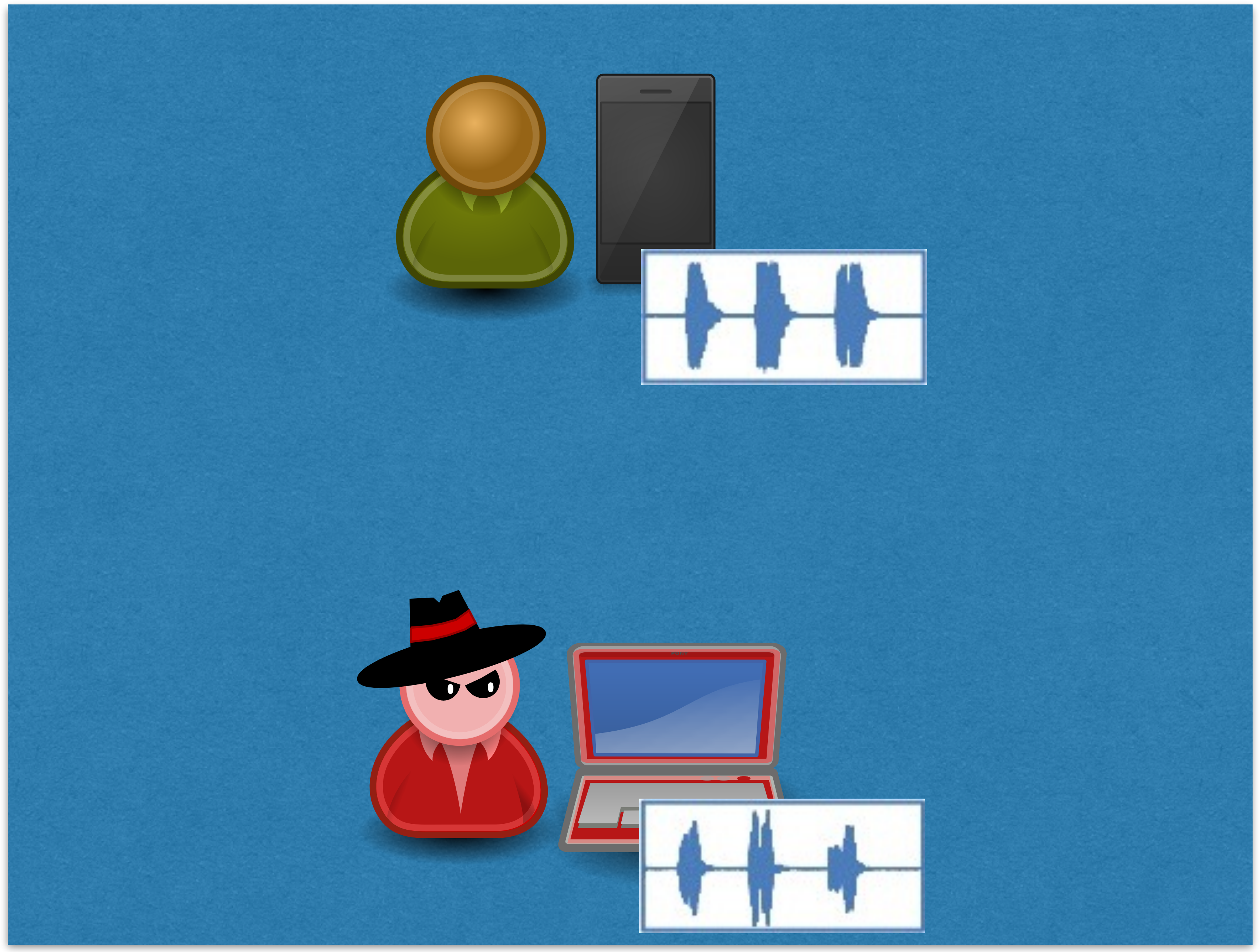


Victim’s username, password

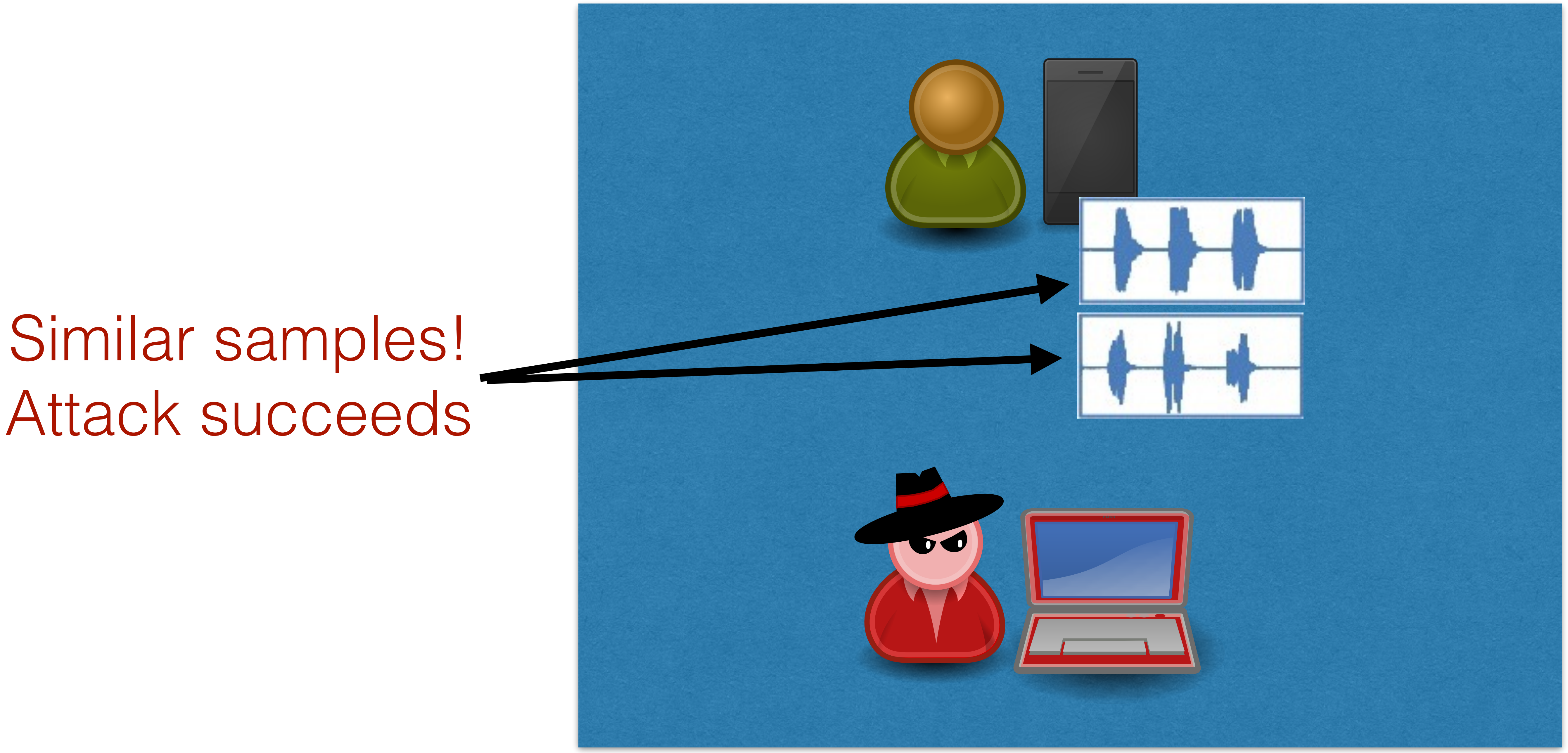
Co-located attackers



Co-located attackers

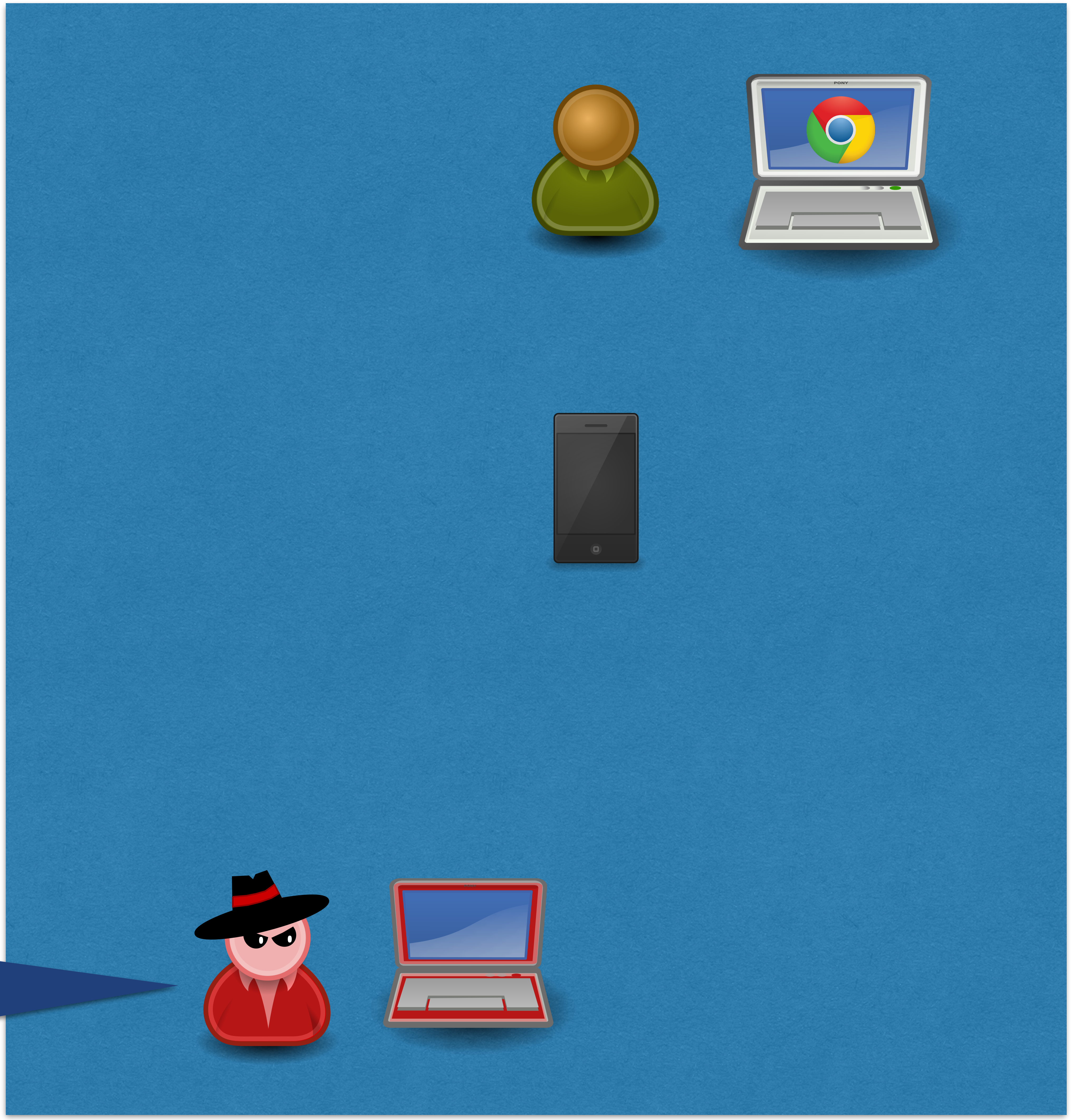


Co-located attackers



Co-located Attacks

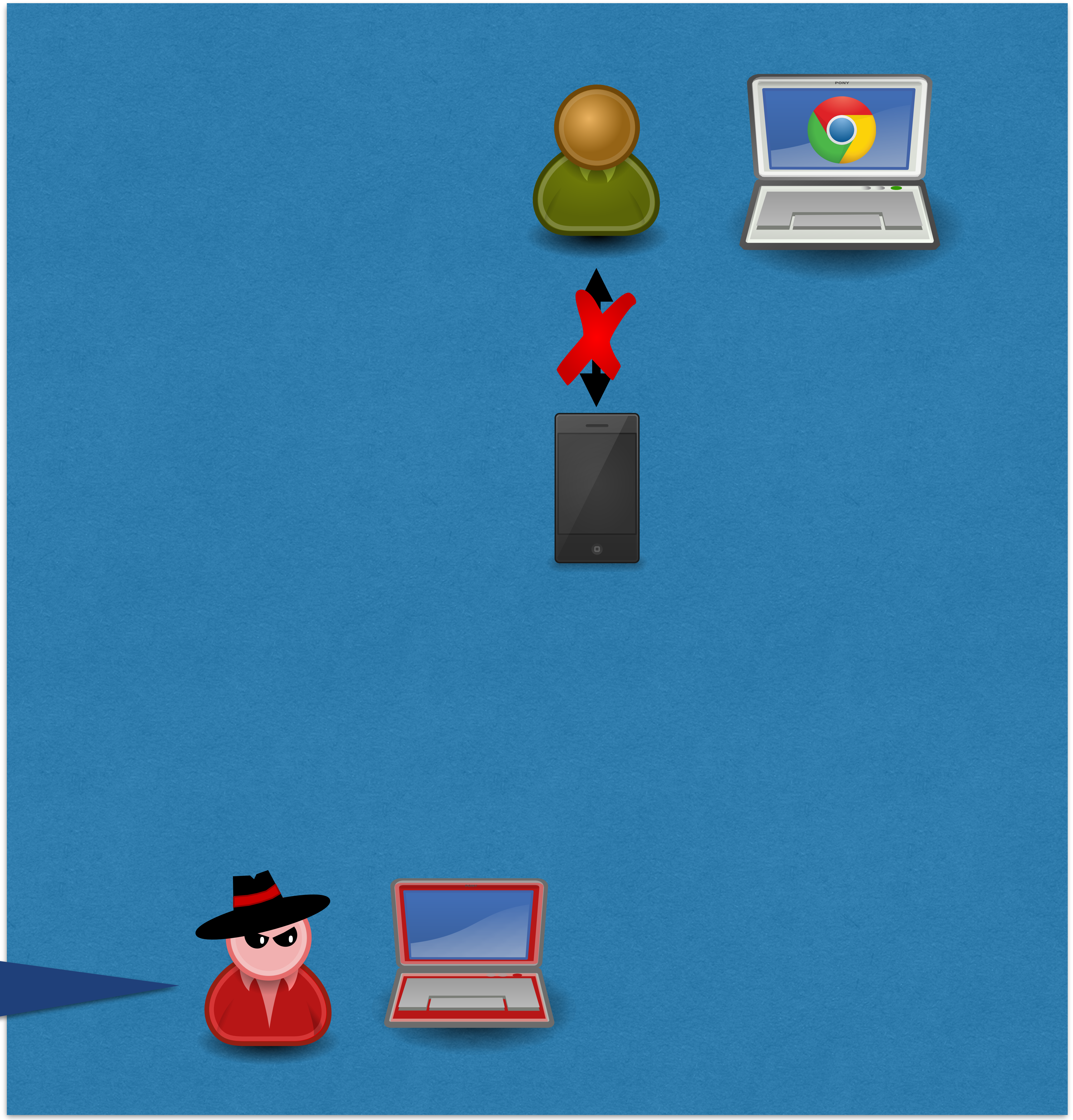
Hard to defeat



Attacker already knows victim's credentials

Hard to defeat

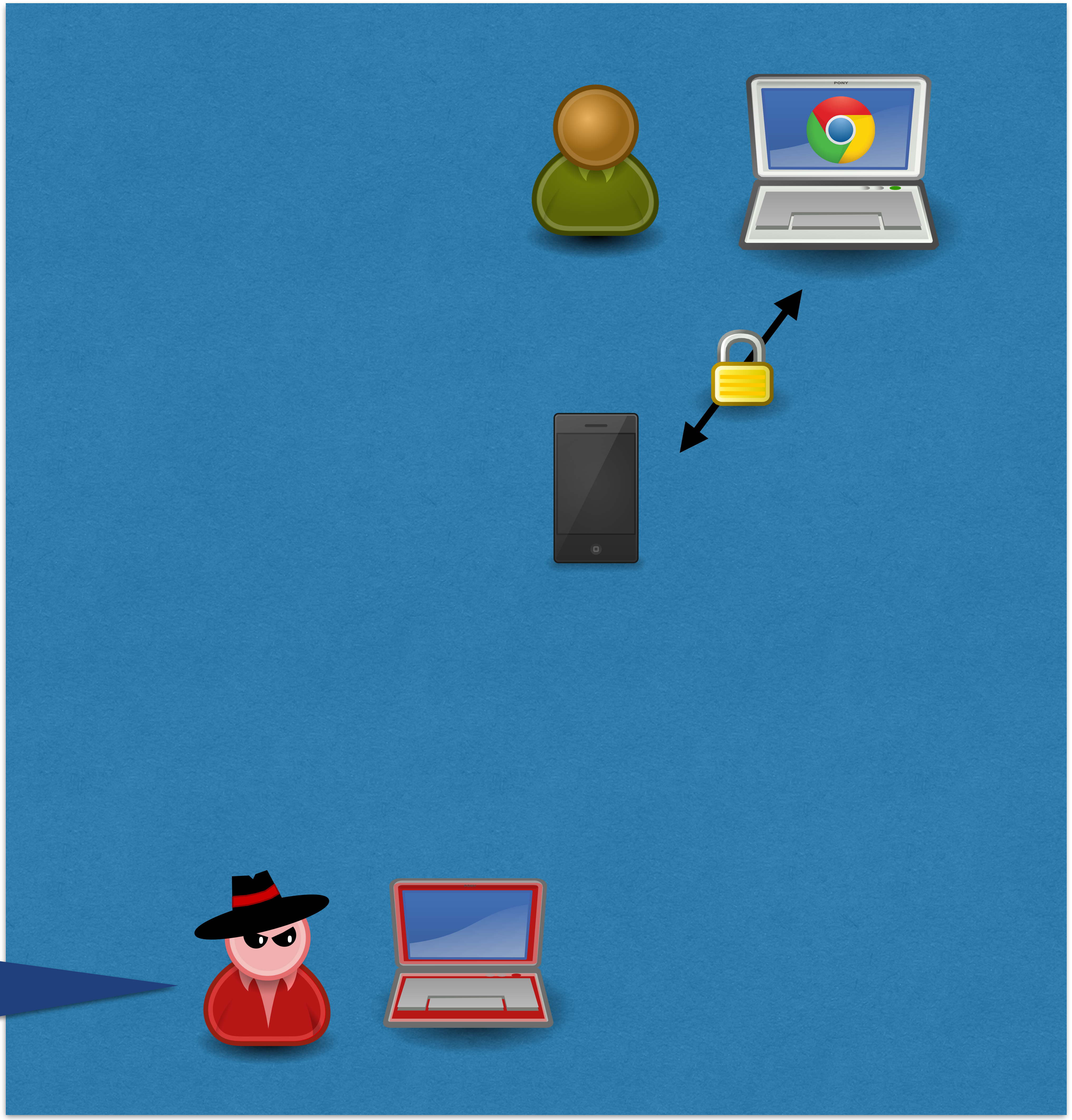
- Attack trivial if no user-phone interaction



Attacker already knows victim's credentials

Hard to defeat

- Attack trivial if no user-phone interaction
  - Unless phone-computer pairing is required (affects usability)

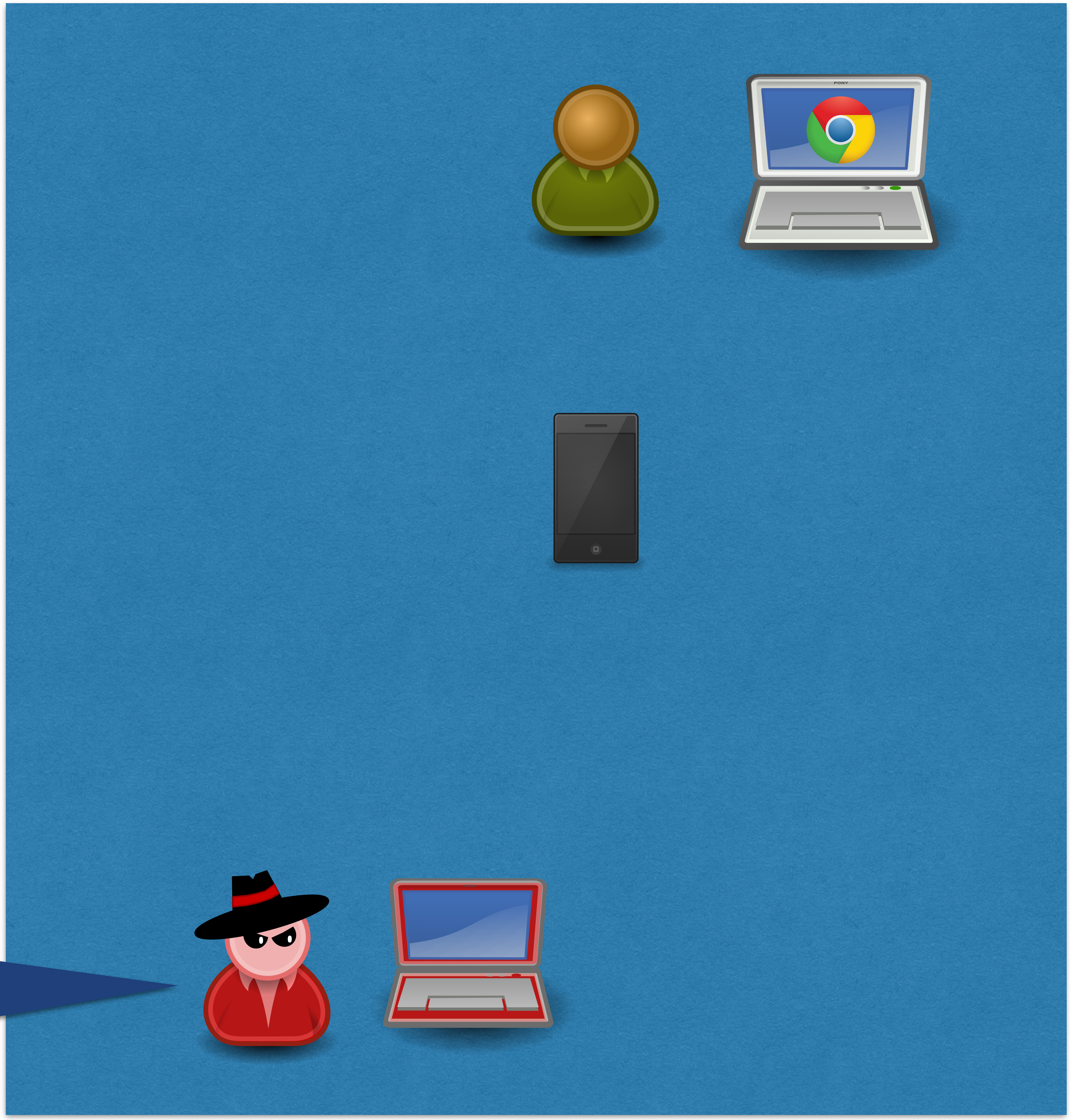


Attacker already knows victim's credentials

Hard to defeat

- Attack trivial if no user-phone interaction
  - Unless phone-computer pairing is required (affects usability)

- Even when 2FA requires user-phone interaction, a determined, co-located attacker might be hard to defeat...



Attacker already knows victim's credentials

User Study

Do people find Sound-Proof usable?

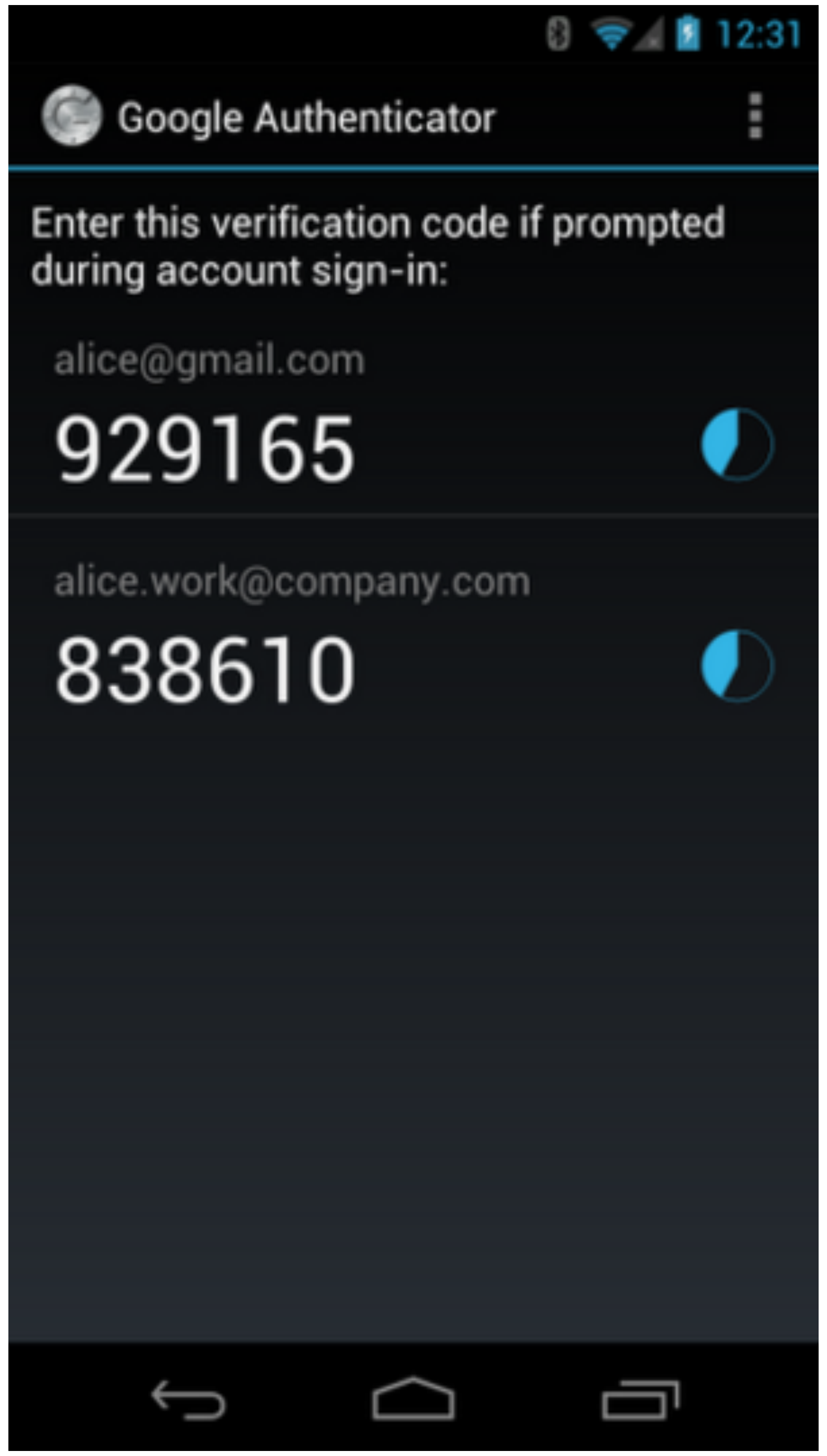
User Study

Do people find Sound-Proof usable?

32 participants (no security experts) in a controlled environment

Do people find Sound-Proof usable?

32 participants (no security experts) in a controlled environment



Enter this verification code if prompted during account sign-in:

alice@gmail.com
929165

alice.work@company.com
838610

Google 2SV

Do people find Sound-Proof usable?

32 participants (no security experts) in a controlled environment

Google 2SV **vs** **Sound-Proof**

User Study

Do people find Sound-Proof usable?

32 participants (no security experts) in a controlled environment

Google 2SV **vs** **Sound-Proof**

Preferred method ✓

User Study

Do people find Sound-Proof usable?

32 participants (no security experts) in a controlled environment

Google 2SV	vs	Sound-Proof
		Preferred method ✓
> 10s		< 5s ✓

User Study

Do people find Sound-Proof usable?

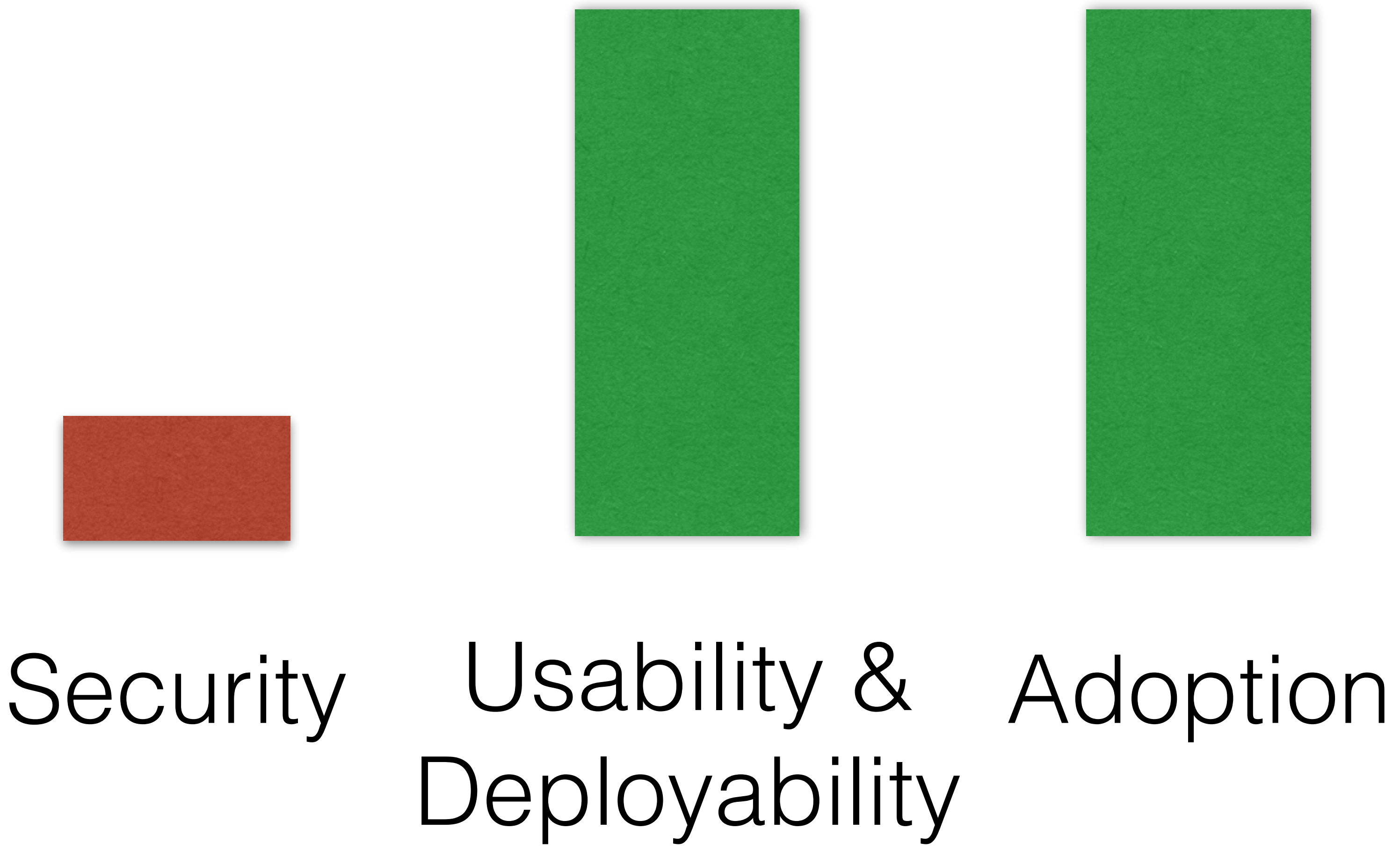
32 participants (no security experts) in a controlled environment

Google 2SV	vs	Sound-Proof
		Preferred method ✓
> 10s		< 5s ✓
		More likely to opt-in ✓

Takeaway

Attempt to foster 2FA adoption on the web

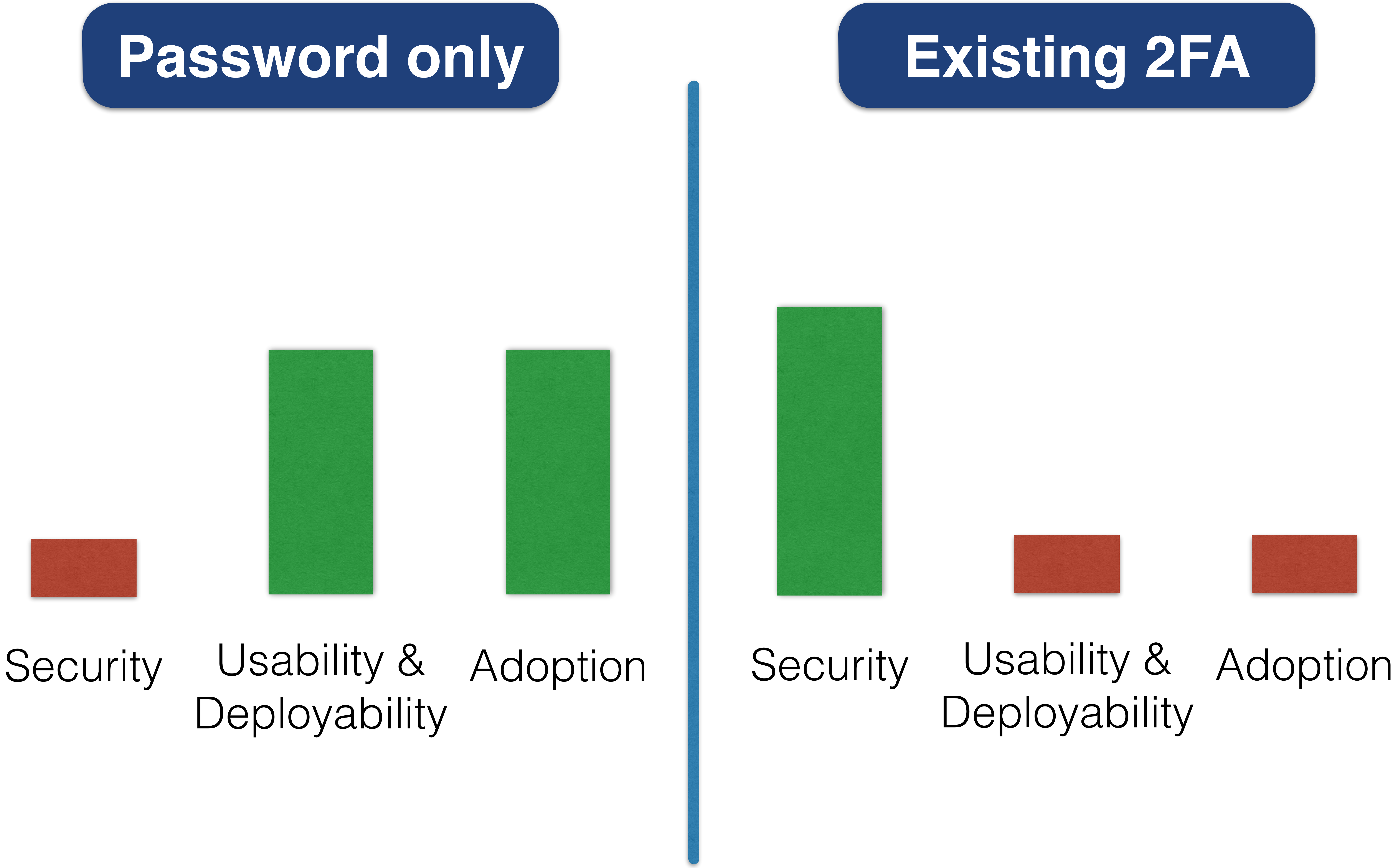
Password only



Sizes are purely qualitative!

Takeaway

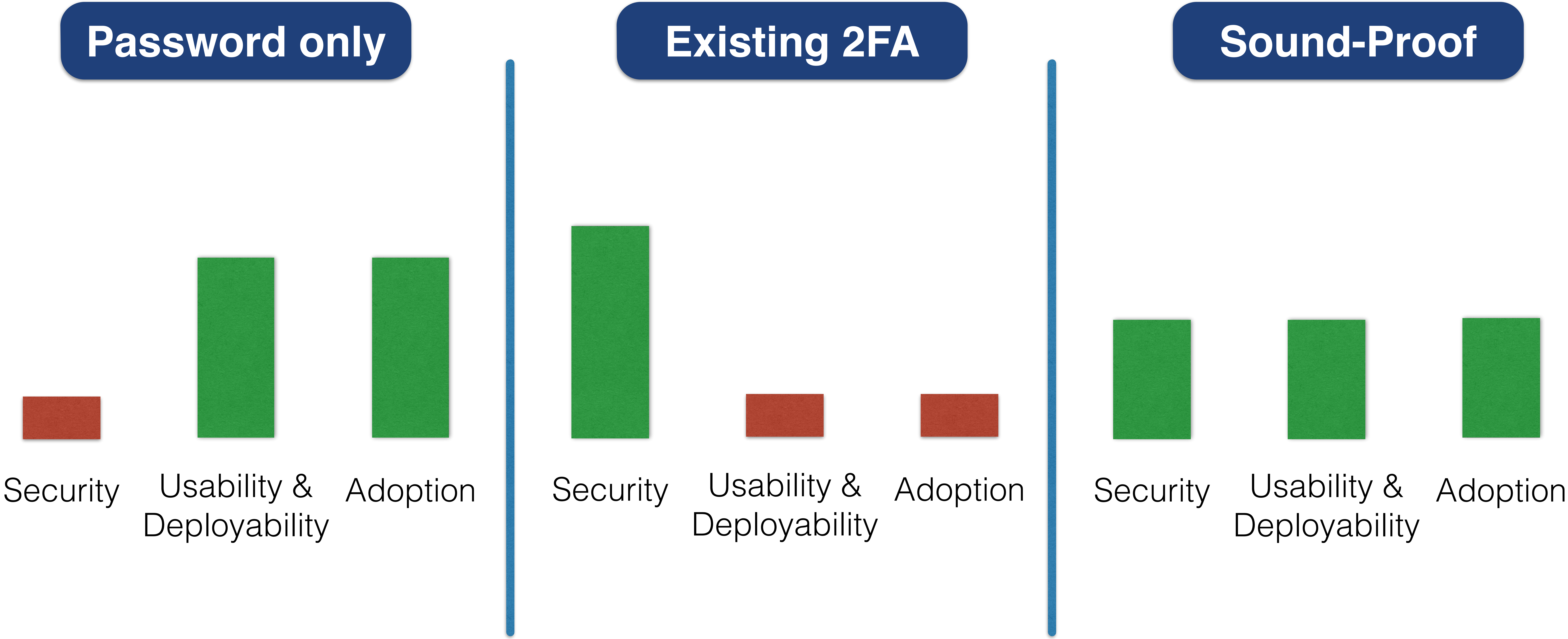
Attempt to foster 2FA adoption on the web



Sizes are purely qualitative!

Takeaway

Attempt to foster 2FA adoption on the web



Sizes are purely qualitative!

Thank you for your attention!
Any Questions?

http://sound-proof.ch/

knikos@inf.ethz.ch

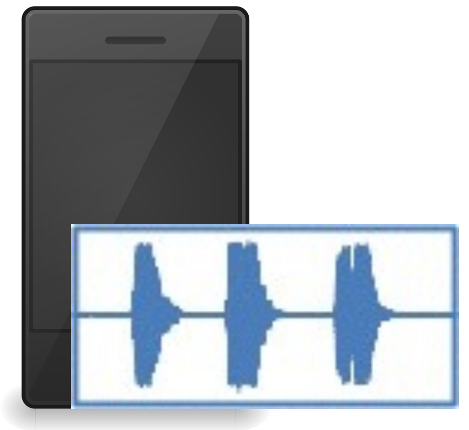
Some of the icons used in this presentation were taken and adapted from opensecurityarchitecture.org

User Privacy

Prying service provider has to actively cheat

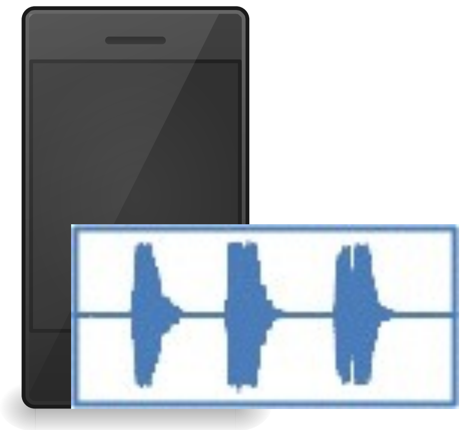
Prying service provider has to actively cheat

- Phone sample never leaves the phone
  - Service provider cannot use phone to spy on user



Prying service provider has to actively cheat

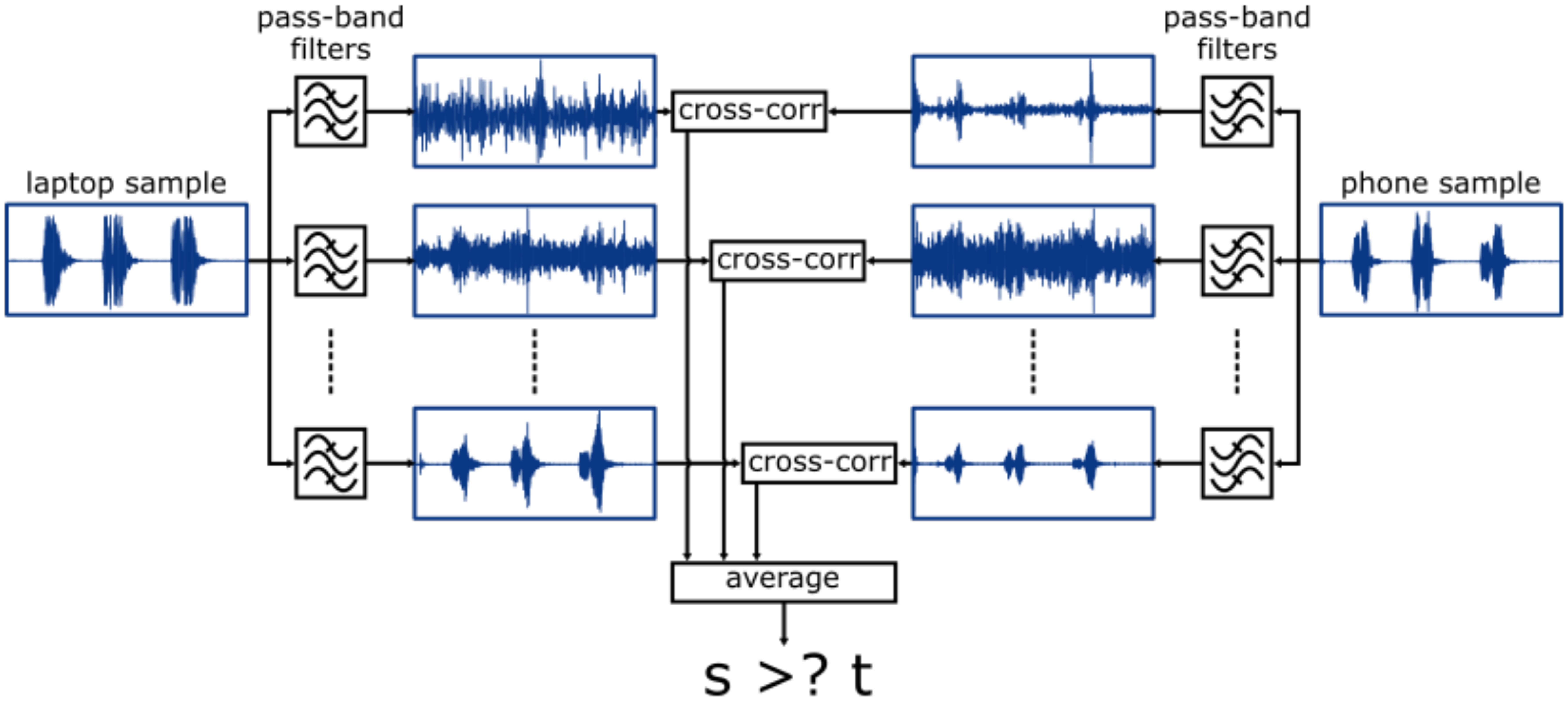
- Phone sample never leaves the phone
  - Service provider cannot use phone to spy on user



- Browser sample encrypted under phone's public key
  - Service provider has to actively play Man-In-The-Middle or supply malicious Javascript
  - Can only be abused, while the user is browsing the site

- Browser indicators whenever web site is recording
- Service provider risks detection —> reputation

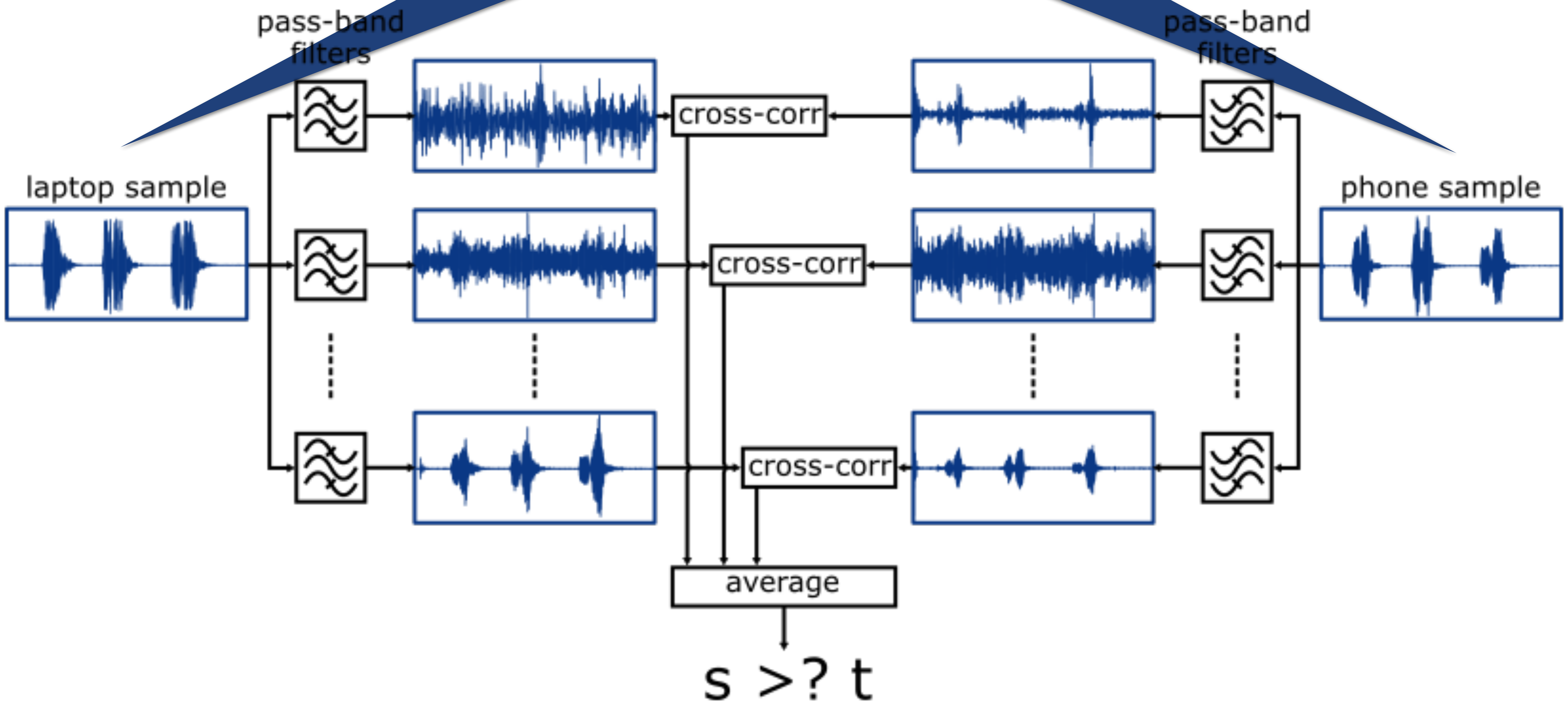
Similarity score computation



Audio Comparison

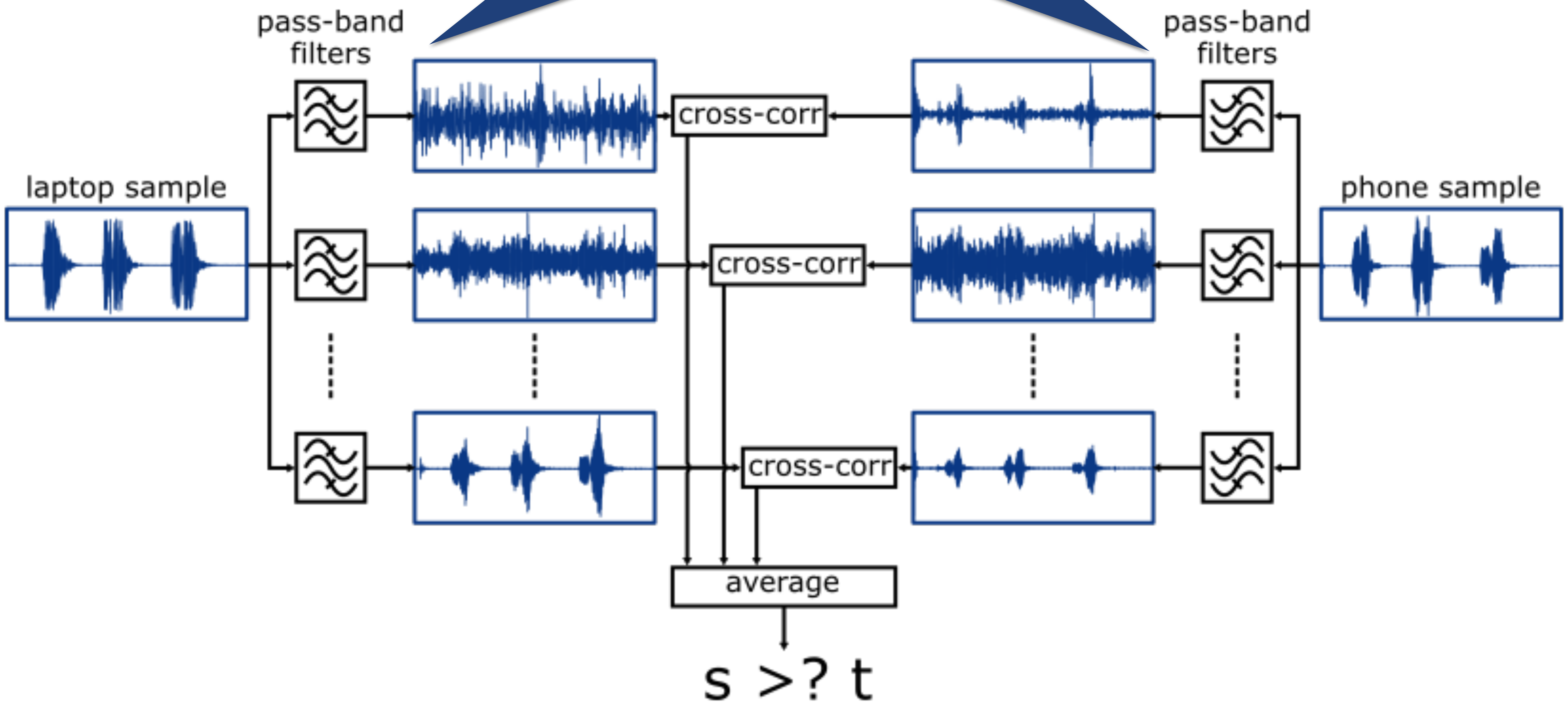
Similarity score computation

Reject silent recordings



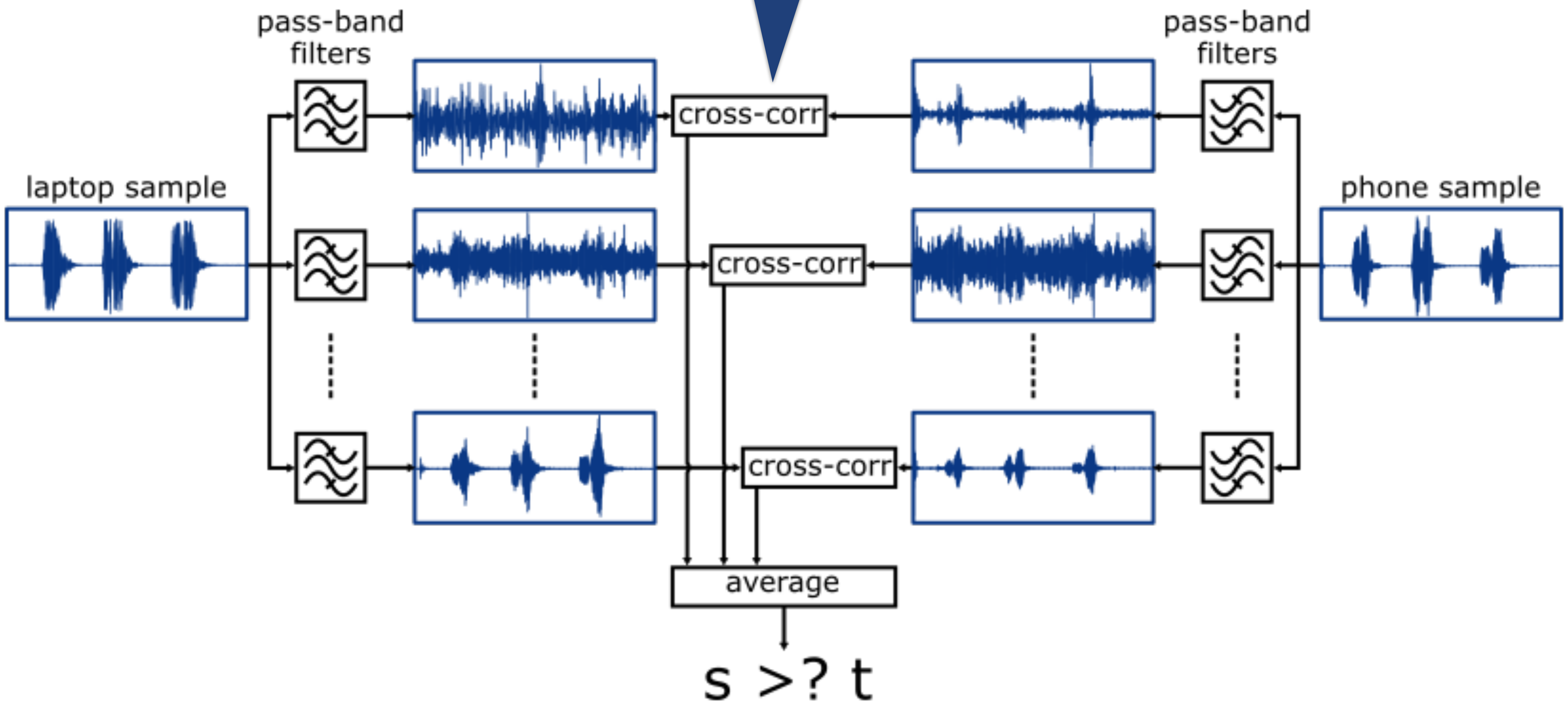
Similarity score computation

Split signal in 1/3 octave-bands

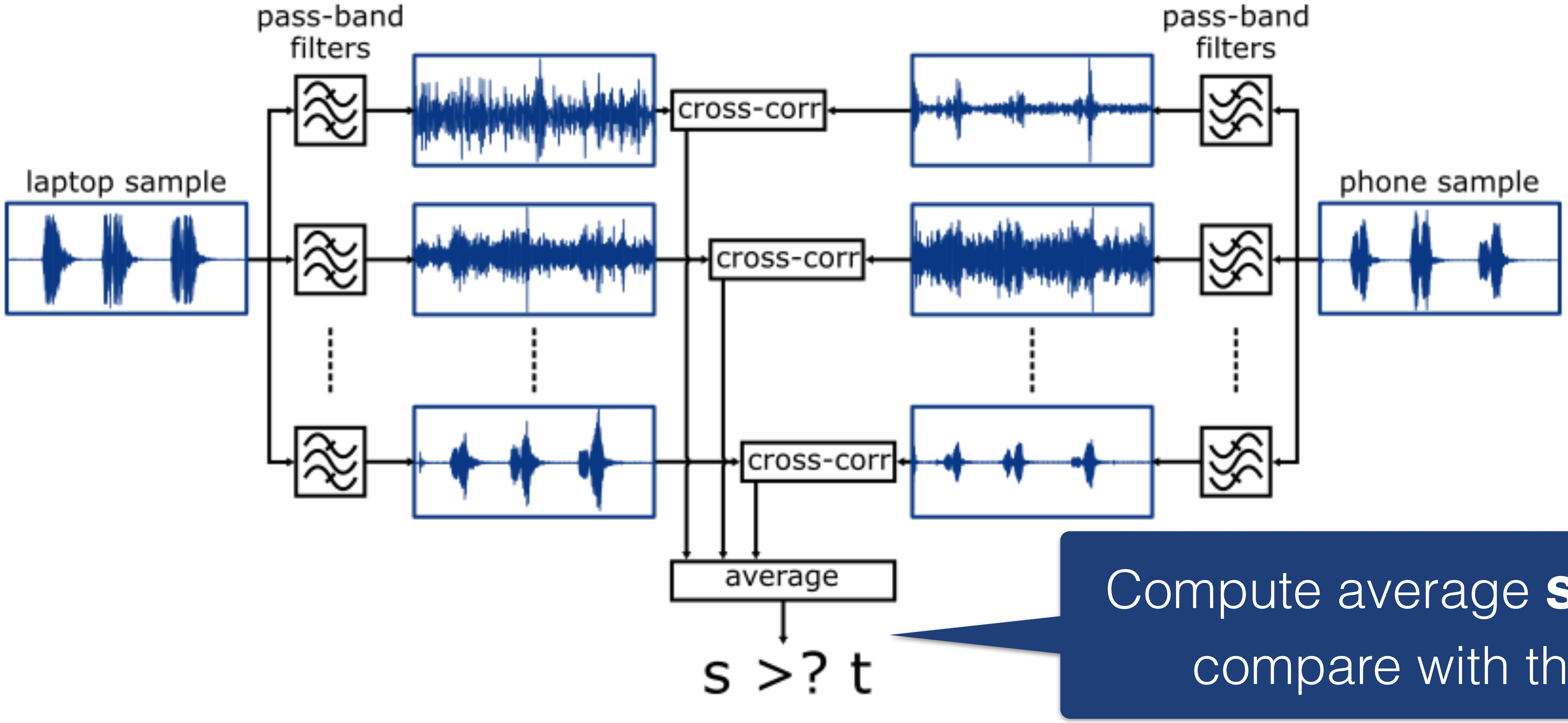


Similarity score computation

Pair-wise cross-correlation
(0 ≤ xcorr ≤ 1)



Similarity score computation



Compute average **s** (0 ≤ **s** ≤ 1), compare with threshold **t**