

Encrypted Access Logging for Online Accounts: Device Attributions without Device Tracking

Carolina Ortega Pérez*, Alaa Daffalla*, and Thomas Ristenpart

*Equal contribution by both authors.



Cornell University

**CORNELL
TECH**

Accounts



Importance of Account Security Interfaces (ASIs)



Importance of Account Security Interfaces (ASIs)



**Account compromise
is a frequent problem
for survivors**

- Abusers can often bypass authentication
- May not be safe to remove abuser
- Survivors often need to know whether access has occurred

Importance of Account Security Interfaces (ASIs)



Account compromise is a frequent problem for survivors

- Abusers can often bypass authentication
- May not be safe to remove abuser
- Survivors often need to know whether access has occurred

Importance of Account Security Interfaces (ASIs)

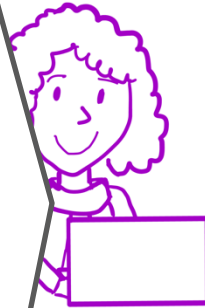
Account login activity

You're currently logged in on these devices:

- MacBook
New Brunswick, NJ, United States •
[This device](#)

Logins on other devices

- iPad 10.2 (2021)
New Brunswick, NJ, United States >
• 17 hours ago
- iPhone 7
New York, NY, United States • on >
April 20, 2023 at 6:46 PM



Account compromise is a frequent problem for survivors

- Abusers can often bypass authentication
- May not be safe to remove abuser
- Survivors often need to know whether access has occurred

Importance of Account Security Interfaces (ASIs)

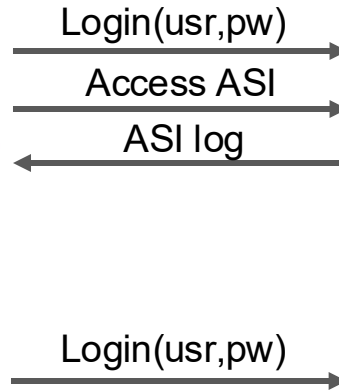
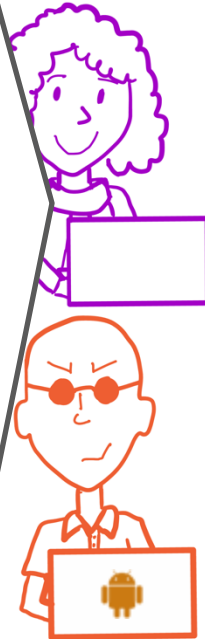
Account login activity

You're currently logged in on these devices:

- MacBook
New Brunswick, NJ, United States •
[This device](#)

Logins on other devices

- iPad 10.2 (2021)
New Brunswick, NJ, United States >
• 17 hours ago
- iPhone 7
New York, NY, United States • on >
April 20, 2023 at 6:46 PM



Account compromise is a frequent problem for survivors

- Abusers can often bypass authentication
- May not be safe to remove abuser
- Survivors often need to know whether access has occurred

Importance of Account Security Interfaces (ASIs)

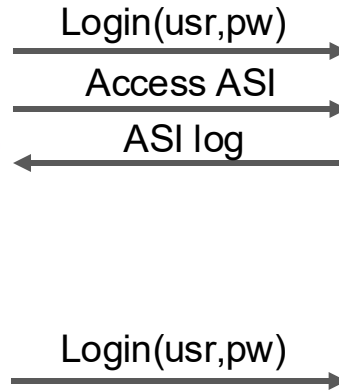
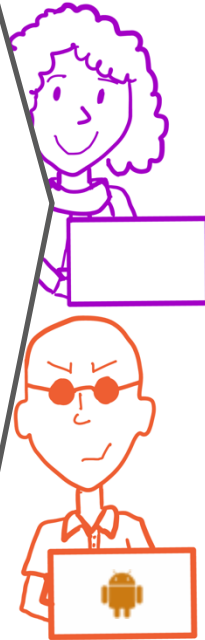
Account login activity

You're currently logged in on these devices:

- MacBook
New Brunswick, NJ, United States •
[This device](#)

Logins on other devices

- iPad 10.2 (2021)
New Brunswick, NJ, United States >
• 17 hours ago
- iPhone 7
New York, NY, United States • on >
April 20, 2023 at 6:46 PM
- Pixel
Exeter, NH, United States • 8 hours ago



Account compromise is a frequent problem for survivors

- Abusers can often bypass authentication
- May not be safe to remove abuser
- Survivors often need to know whether access has occurred

Importance of Account Security Interfaces (ASIs)

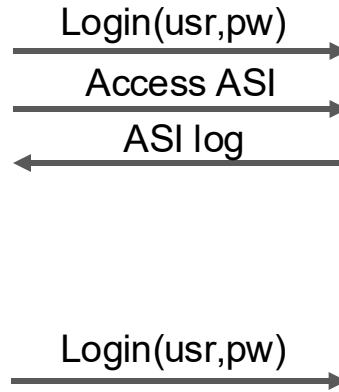
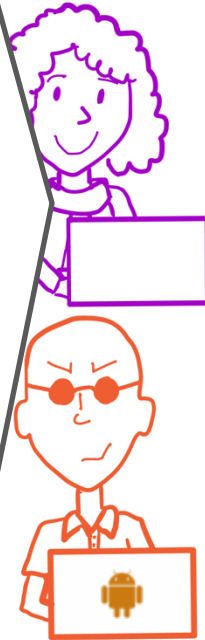
Account login activity

You're currently logged in on these devices:

- MacBook
New Brunswick, NJ, United States •
[This device](#)

Logins on other devices

- iPad 10.2 (2021)
New Brunswick, NJ, United States >
• 17 hours ago
- iPhone 7
New York, NY, United States • on >
April 20, 2023 at 6:46 PM
- Pixel
Exeter, NH, United States • 8 hours ago



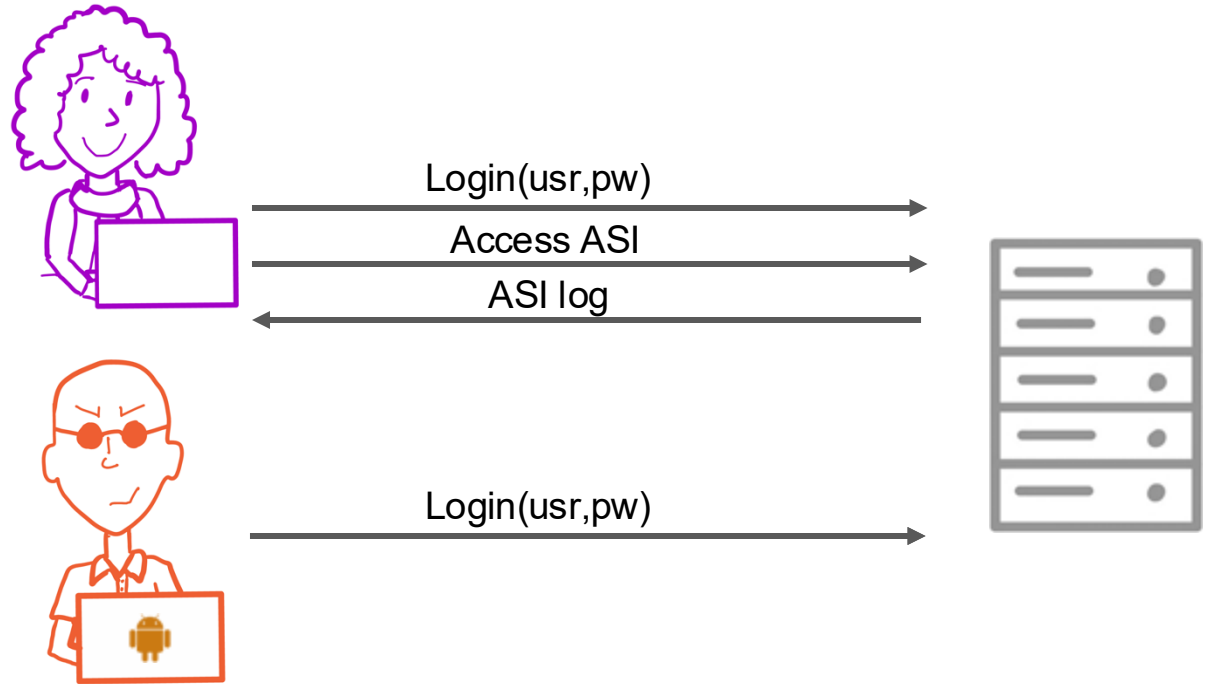
Account compromise is a frequent problem for survivors

- Abusers can often bypass authentication
- May not be safe to remove abuser
- Survivors often need to know whether access has occurred

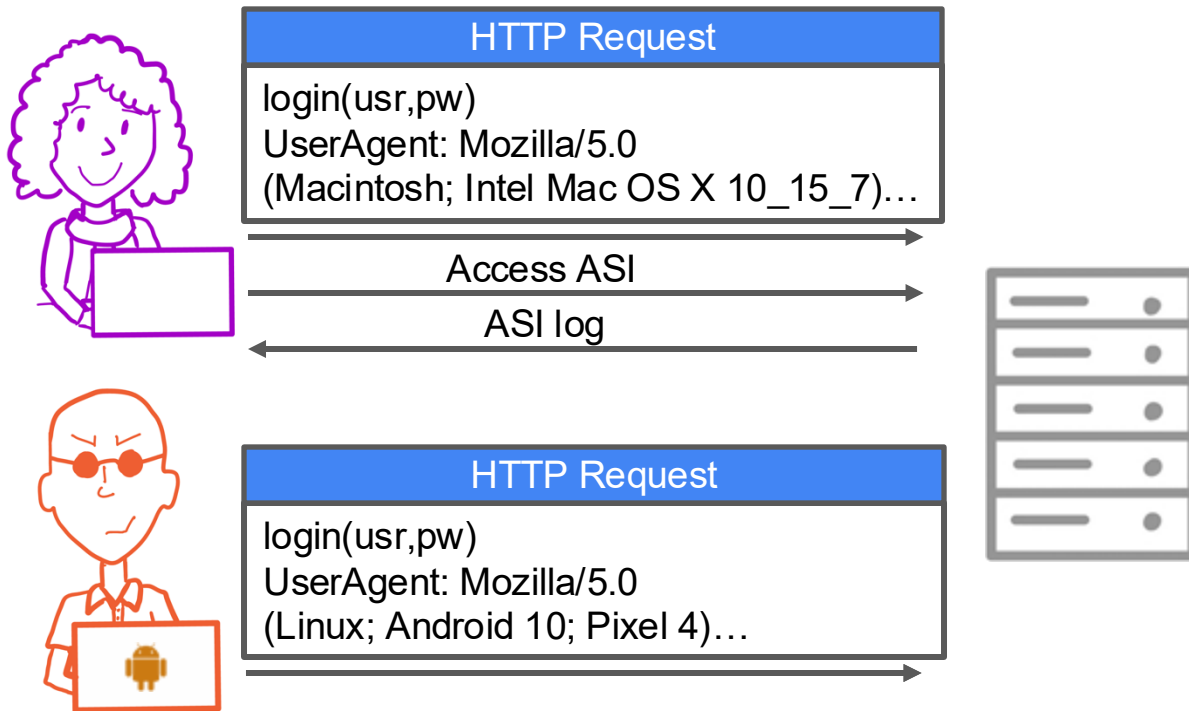
ASIs critically important for user safety

ASIs are easy to spoof

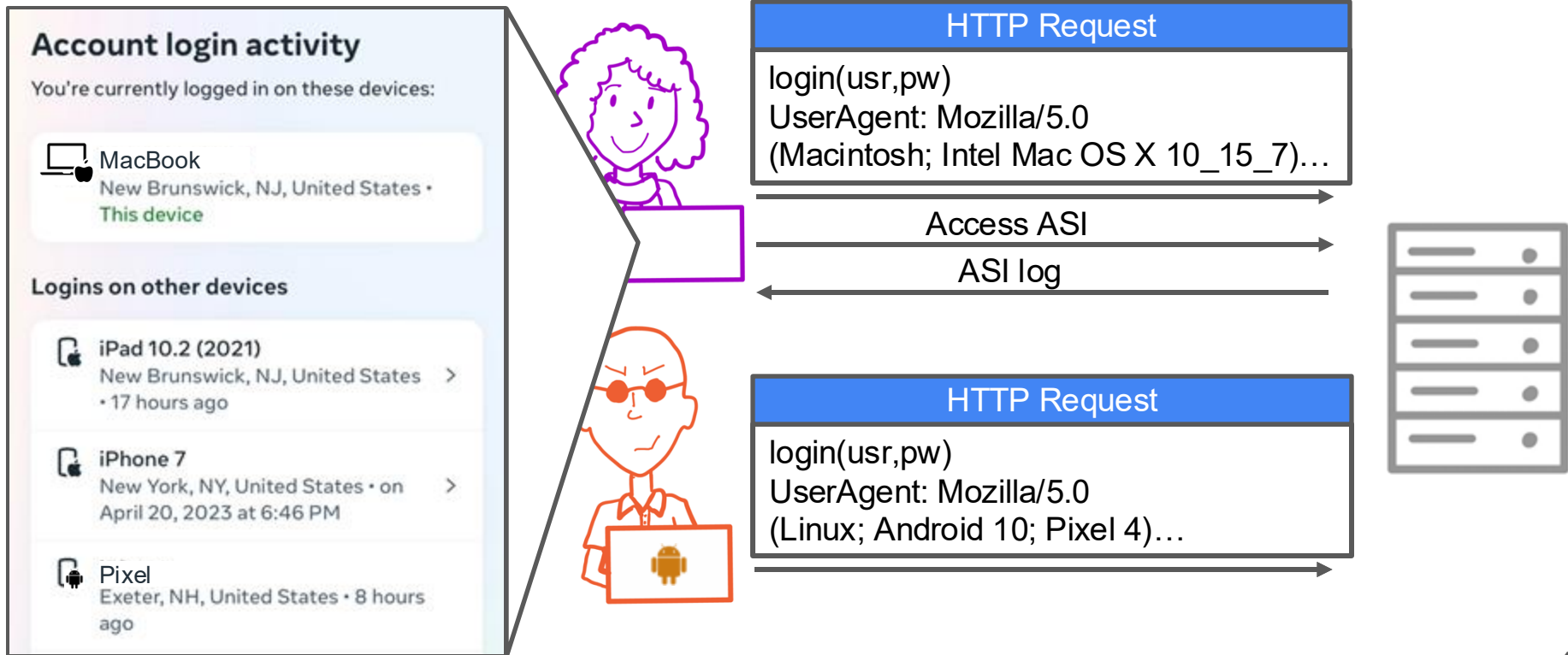
ASIs are easy to spoof



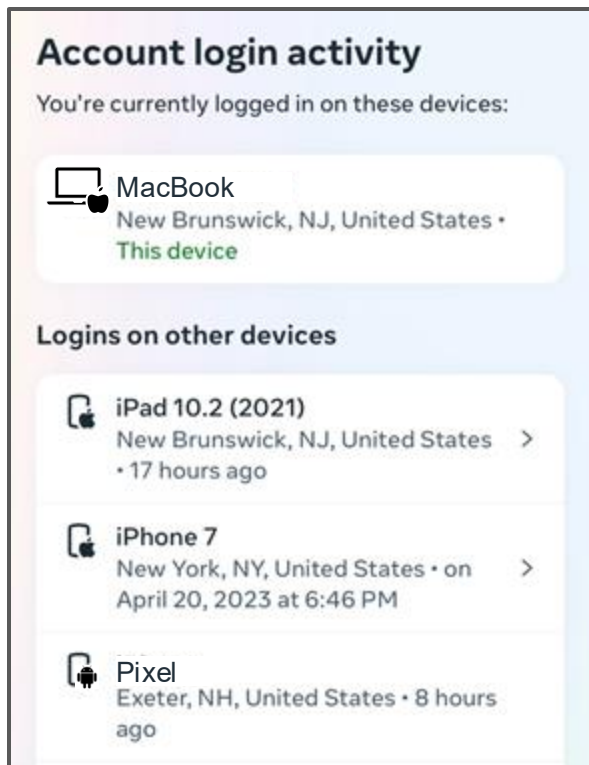
ASIs are easy to spoof



ASIs are easy to spoof

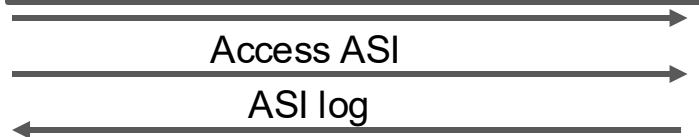


ASIs are easy to spoof



HTTP Request

```
login(usr,pw)
UserAgent: Mozilla/5.0
(Macintosh; Intel Mac OS X 10_15_7)...
```

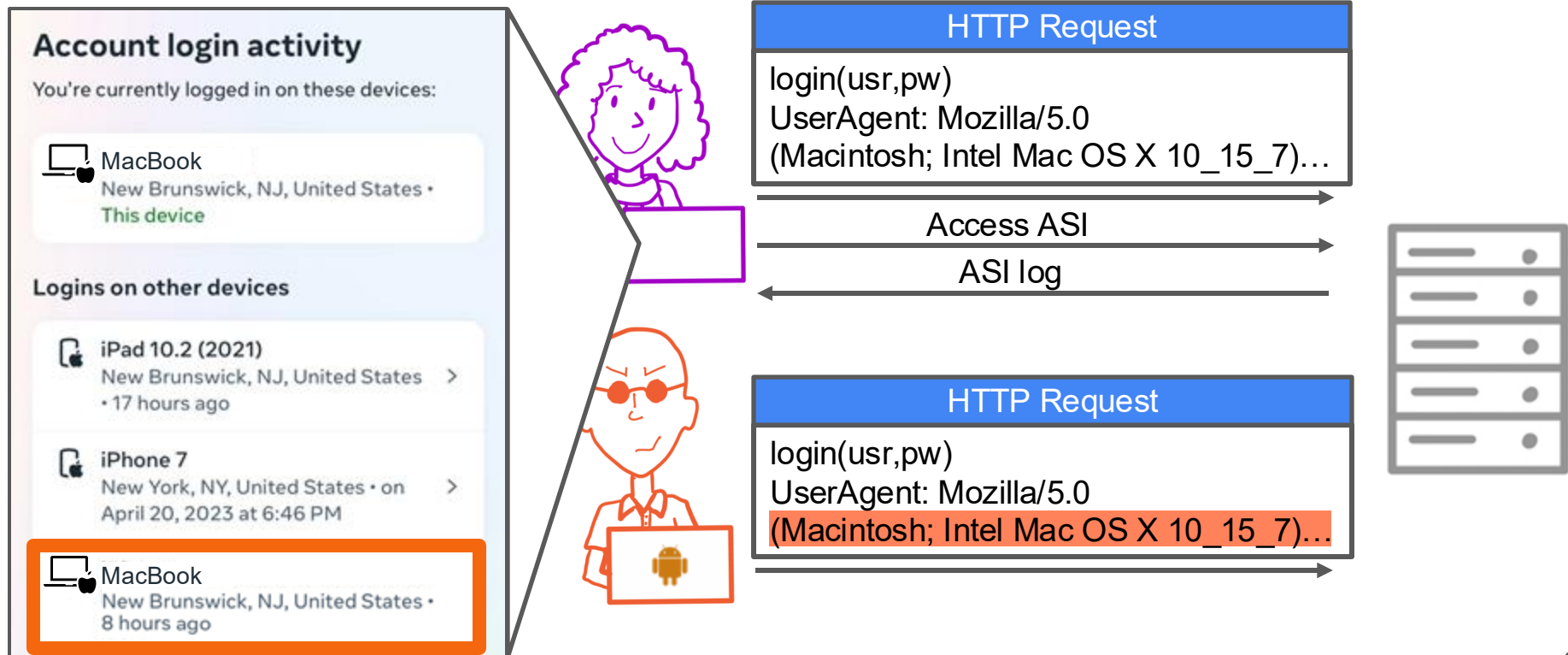


HTTP Request

```
login(usr,pw)
UserAgent: Mozilla/5.0
(Macintosh; Intel Mac OS X 10_15_7)...
```



ASIs are easy to spoof



ASIs integrity is a problem...

...what can we do about it?

Our work: Towards providing ASI integrity

We propose **client-side-encrypted access logging (CSAL)** protocols

- Agnostic to authentication mechanisms
- Do not rely on external services
- Require OS support (browsers are untrusted)

Our work: Towards providing ASI integrity

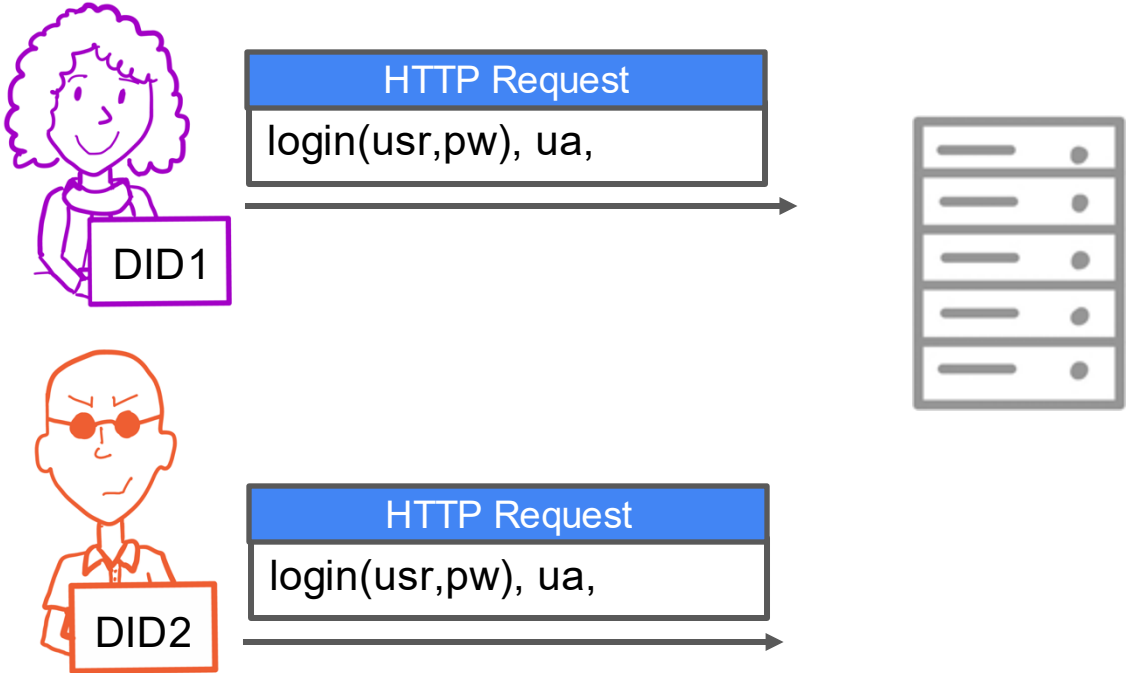
We propose **client-side-encrypted access logging (CSAL)** protocols

- Agnostic to authentication mechanisms
- Do not rely on external services
- Require OS support (browsers are untrusted)

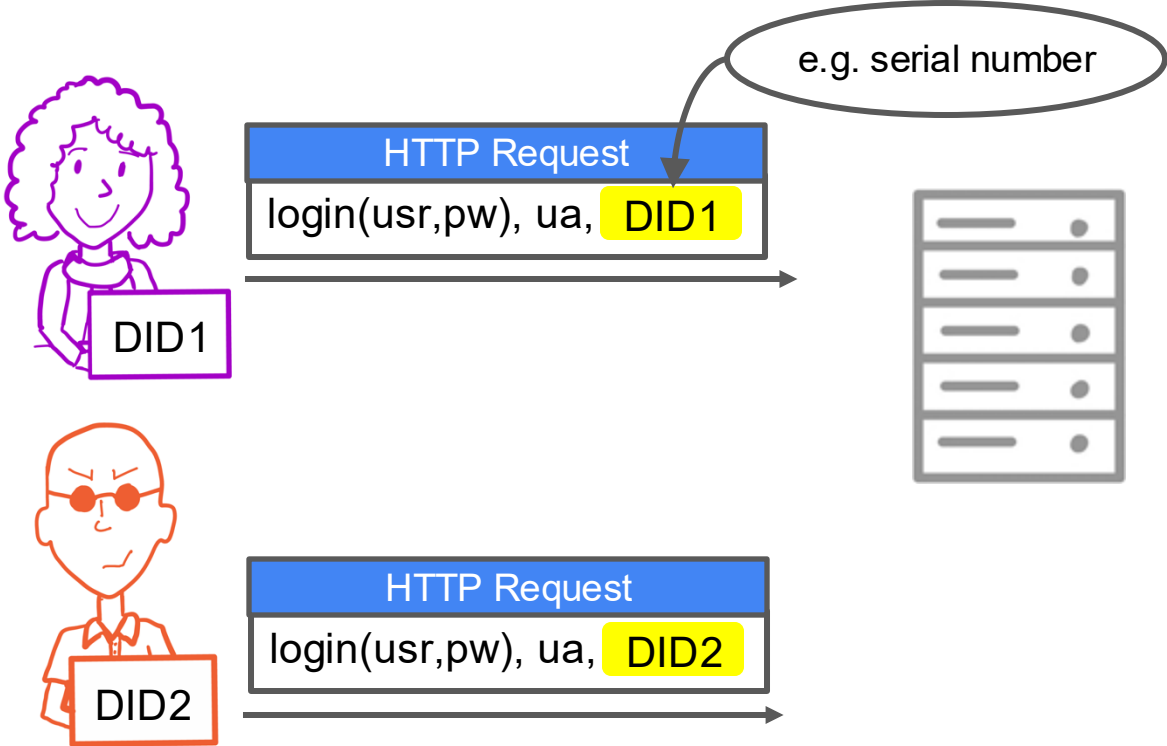
In the paper we:

- Formalize CSAL protocols
- Detail a full CSAL protocol and formally analyze it
- Proof-of-concept CSAL implementation and deployment considerations

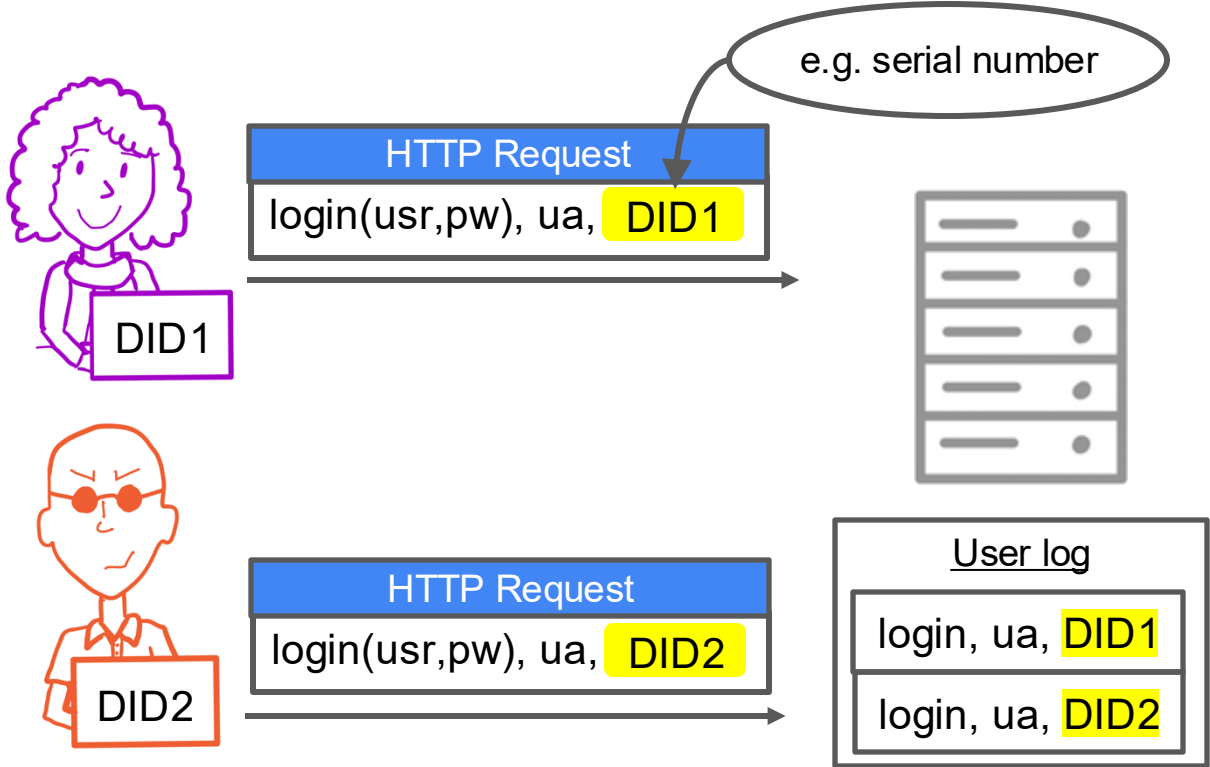
Straw approach: Adding reliable OS-provided information



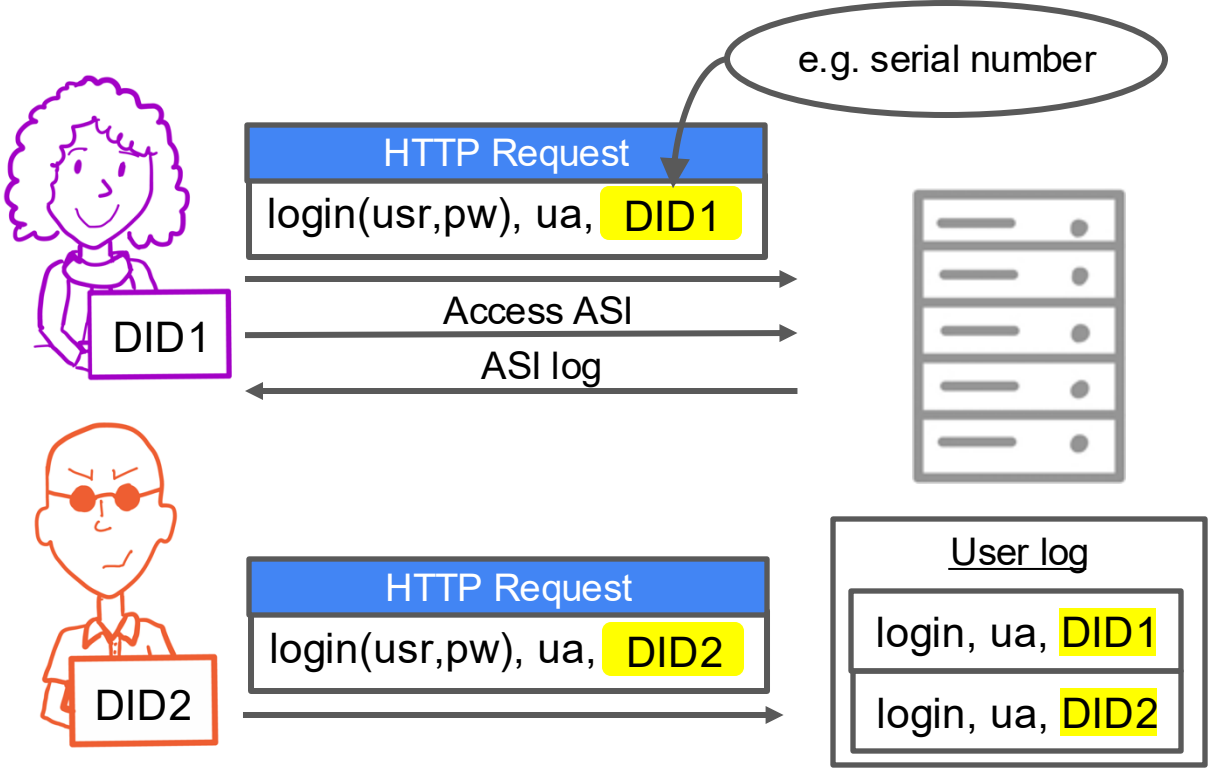
Straw approach: Adding reliable OS-provided information



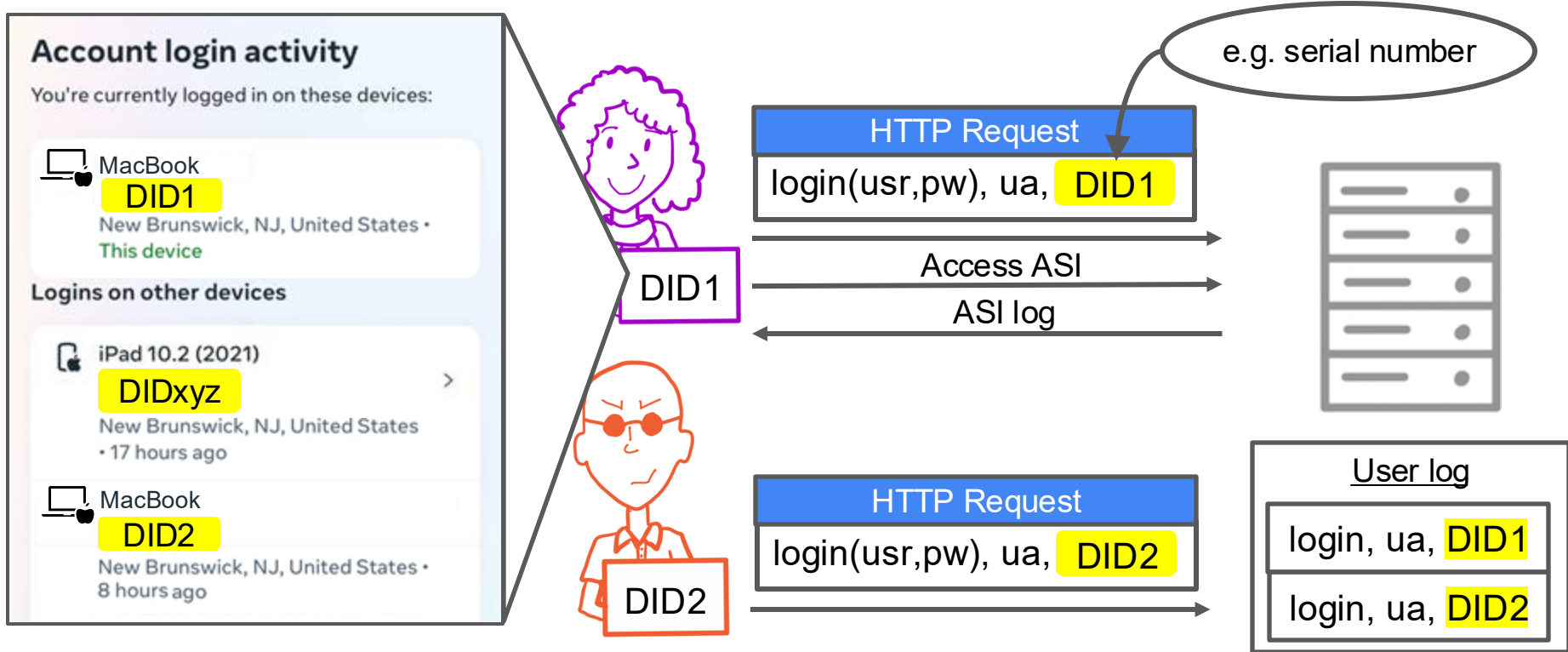
Straw approach: Adding reliable OS-provided information



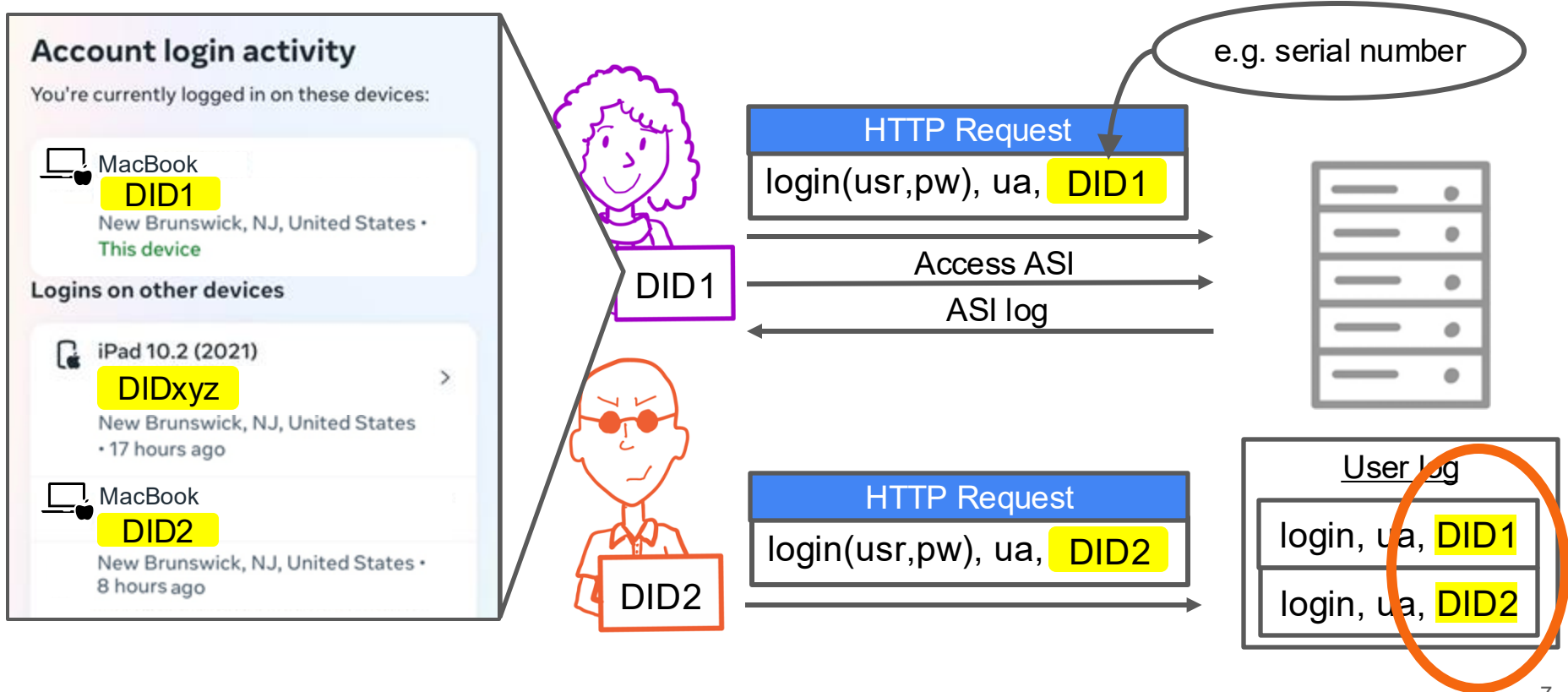
Straw approach: Adding reliable OS-provided information



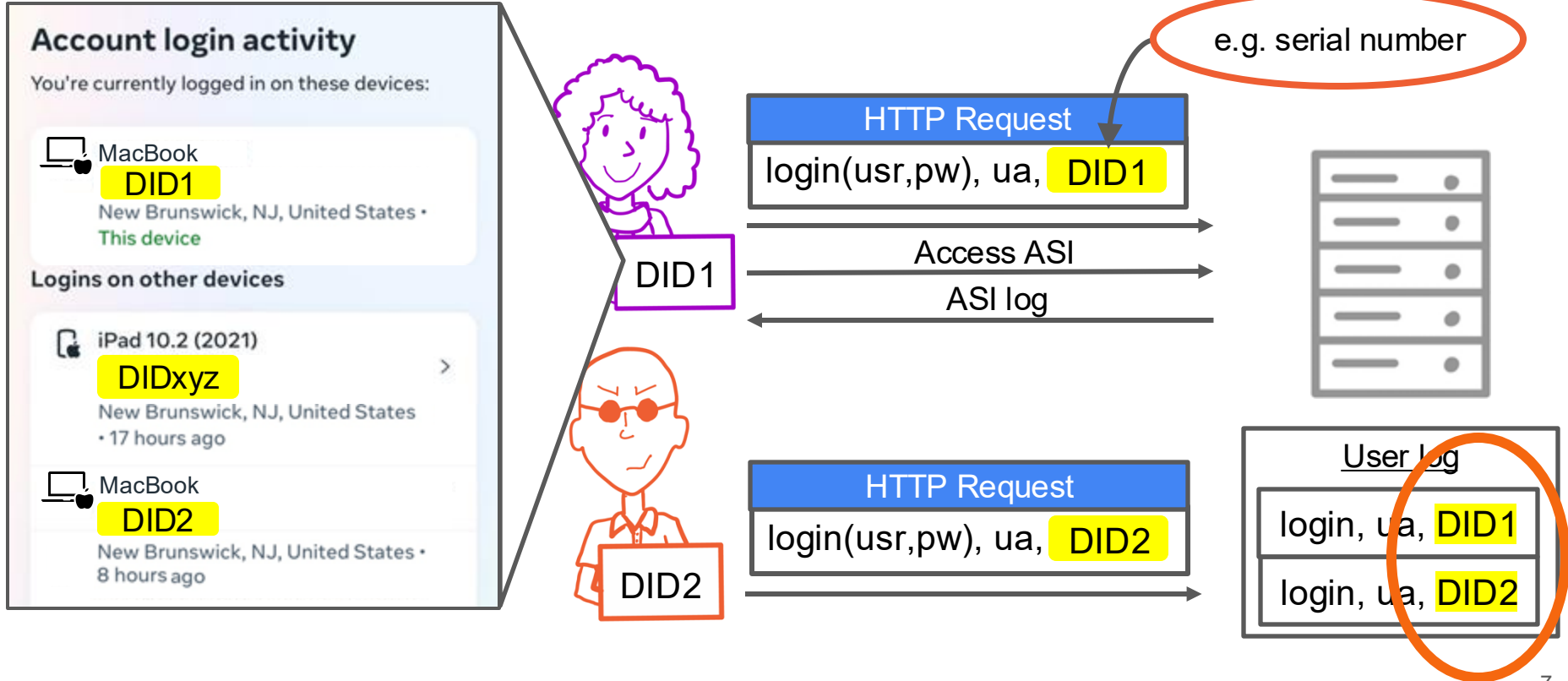
Straw approach: Adding reliable OS-provided information



Straw approach: Adding reliable OS-provided information



Straw approach: Adding reliable OS-provided information



Straw approach: Adding reliable OS-provided information

Decades of work highlighting the dangers of device fingerprinting

- [Eckersley 2010]
- [Egele et al. 2011]
- [Nikiforakis et al. 2013]
- [Acar et al. 2014]
- [Kurtz et al. 2016]
- [Yen et al. 2017]

...

MacBook

DID2

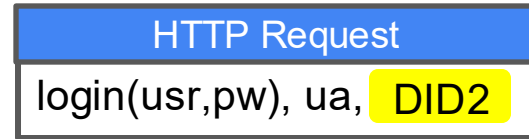
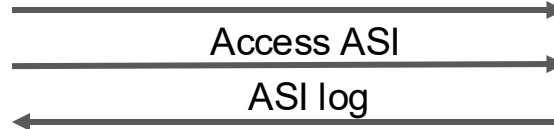
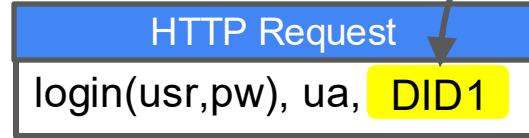
New Brunswick, NJ, United States •
8 hours ago



DID1



DID2



e.g. serial number



User log

login, ua, DID1

login, ua, DID2

Straw approach: Adding reliable OS-provided information

Decades of work highlighting the dangers of device fingerprinting

- [Eckersley 2010]
- [Egele et al. 2011]
- [Nikiforakis et al. 2013]
- [Acar et al. 2014]
- [Kurtz et al. 2015]
- [Yen et al. 2016]

DID1

HTTP Request
login(usr,pw), ua, DID1

e.g. serial number

Access ASI

Best practices for working with Android identifiers

To protect the privacy of your users, use the most restrictive identifier that satisfies your app's use case. In particular, follow these best practices:

1. **Choose user-resettable identifiers whenever possible.** Your app can achieve most of its use cases even when it uses identifiers other than non-resettable hardware IDs.

MacBook

DID2

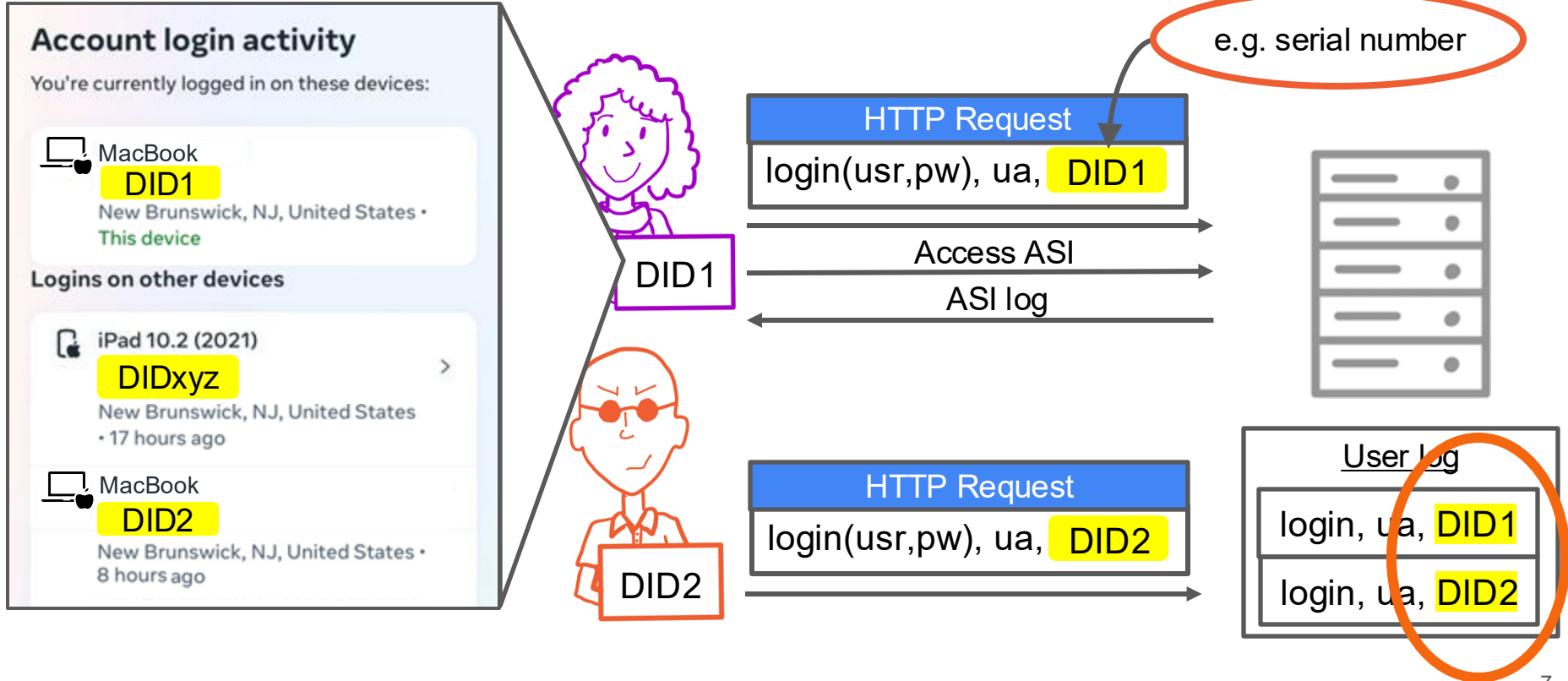
New Brunswick, NJ, United States
8 hours ago

Log

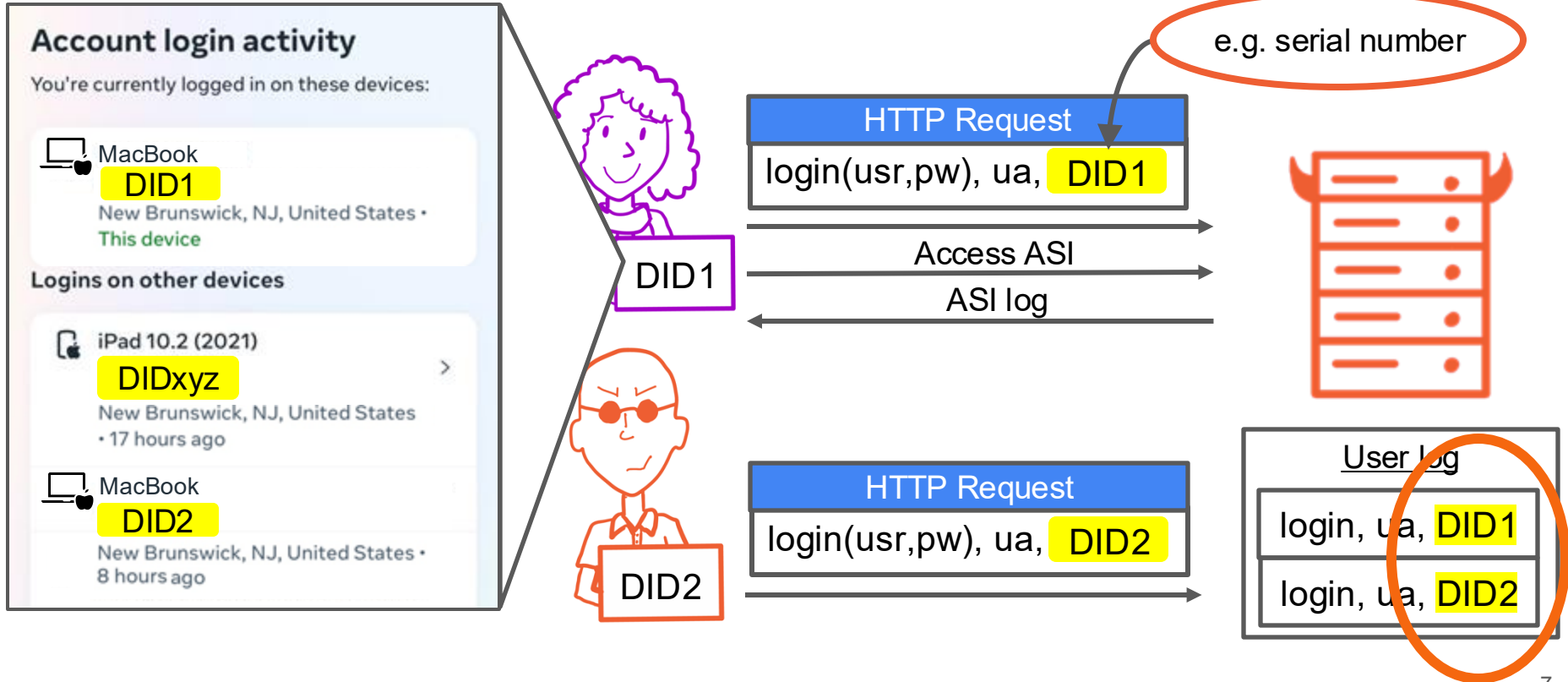
a, DID1

a, DID2

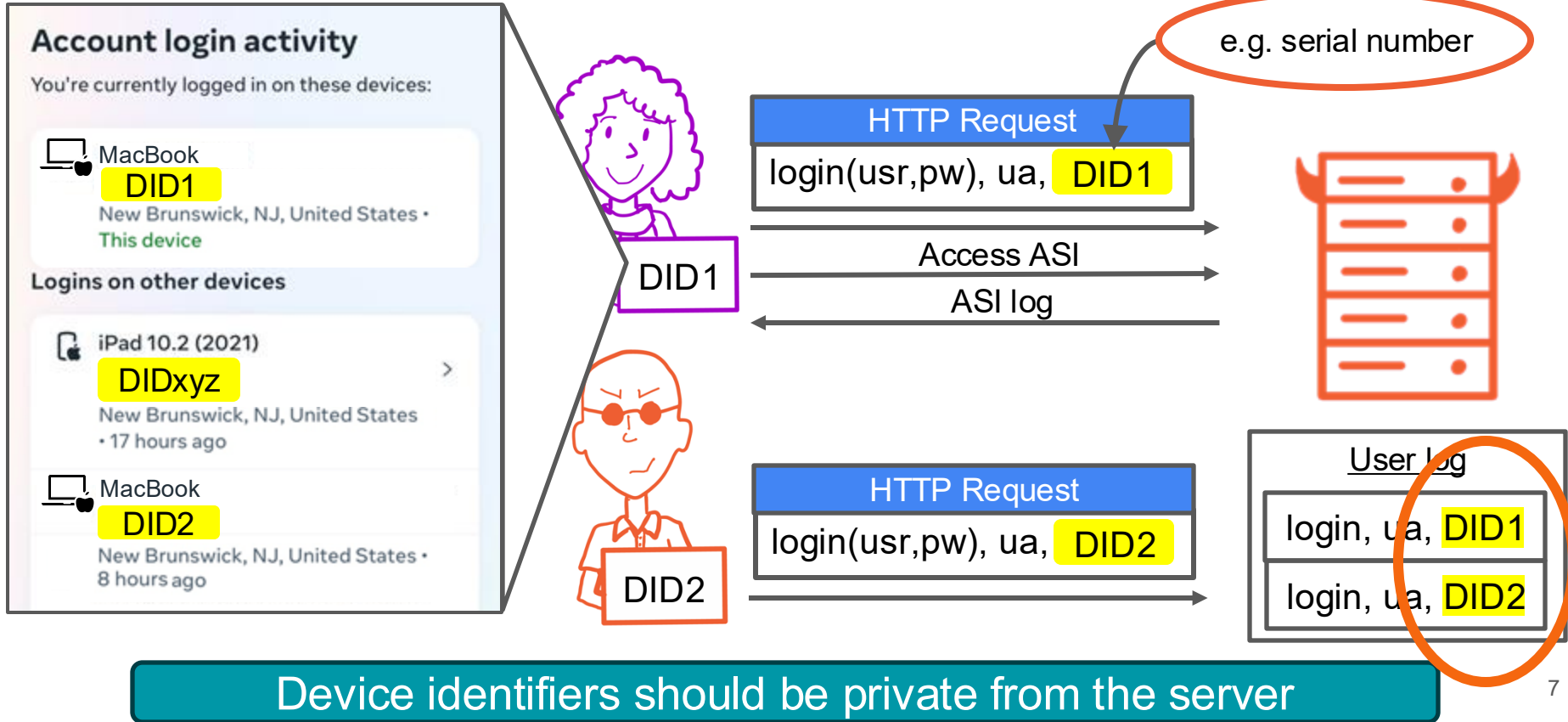
Straw approach: Adding reliable OS-provided information



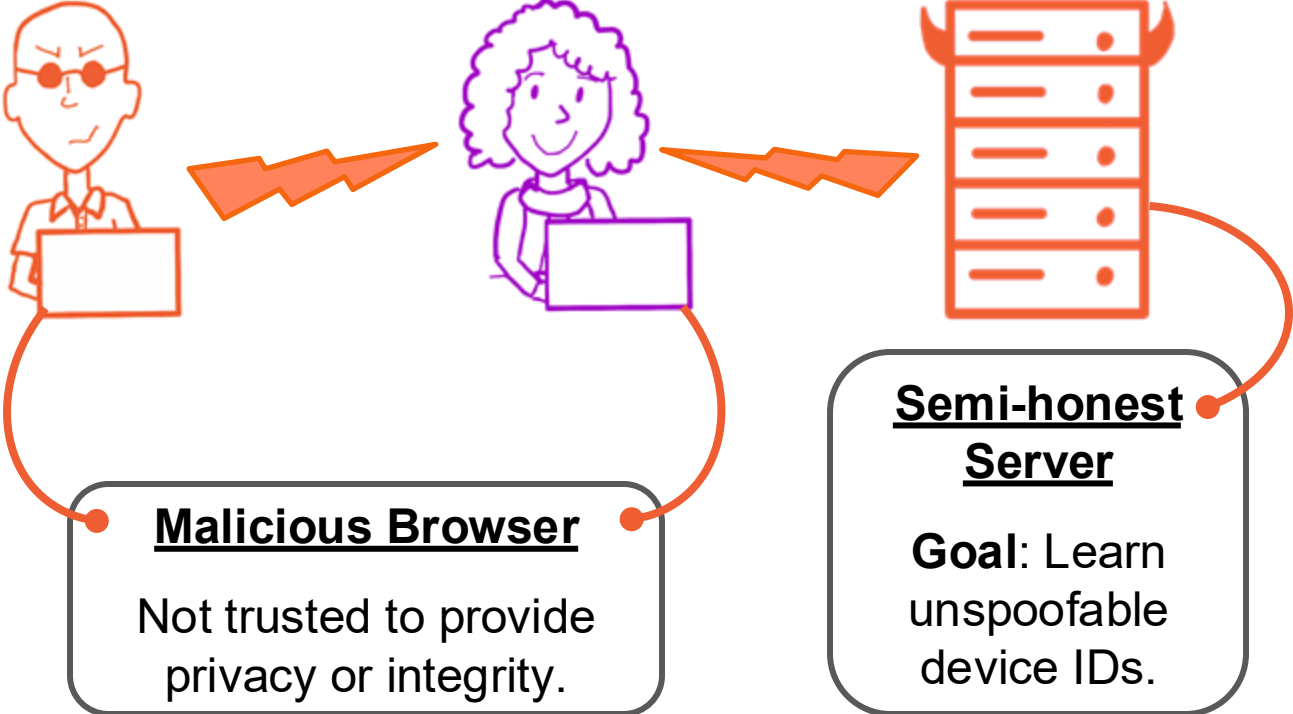
Straw approach: Adding reliable OS-provided information



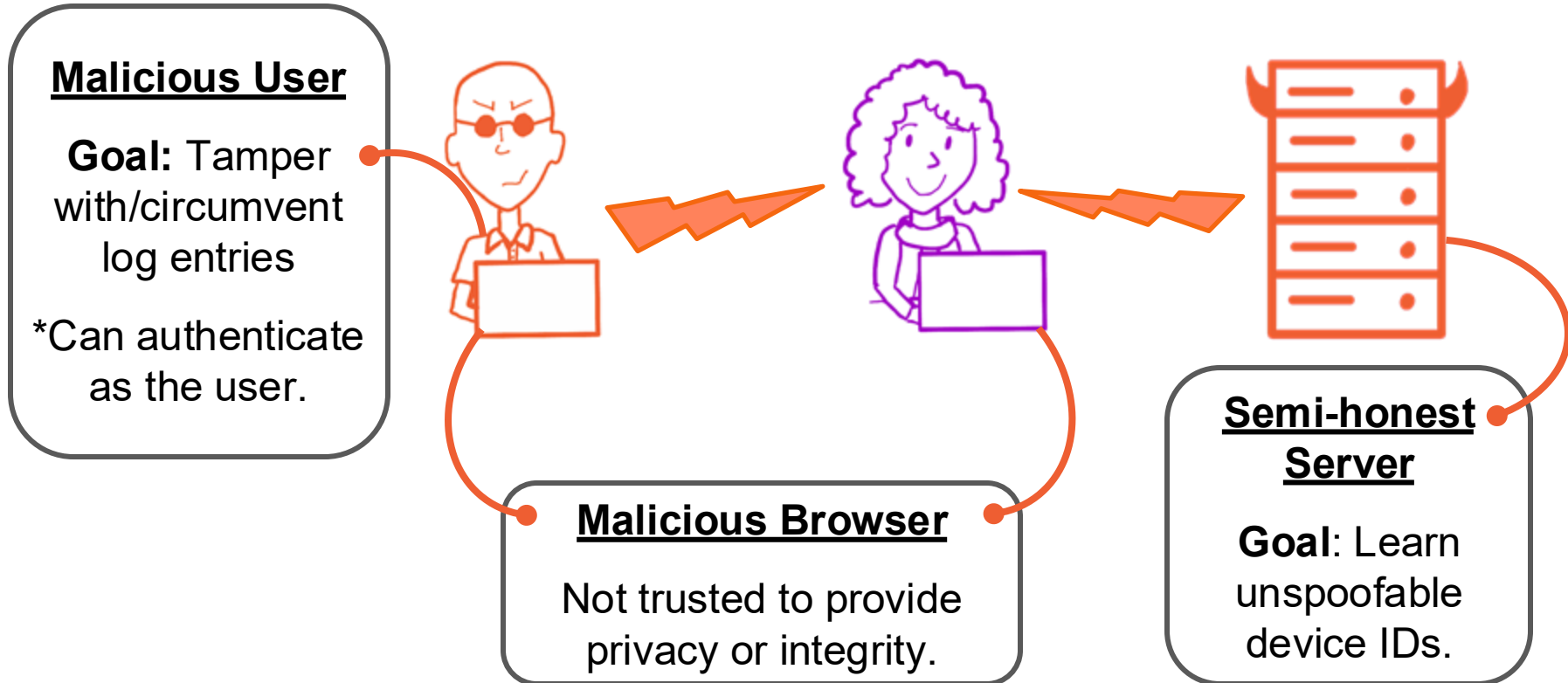
Straw approach: Adding reliable OS-provided information



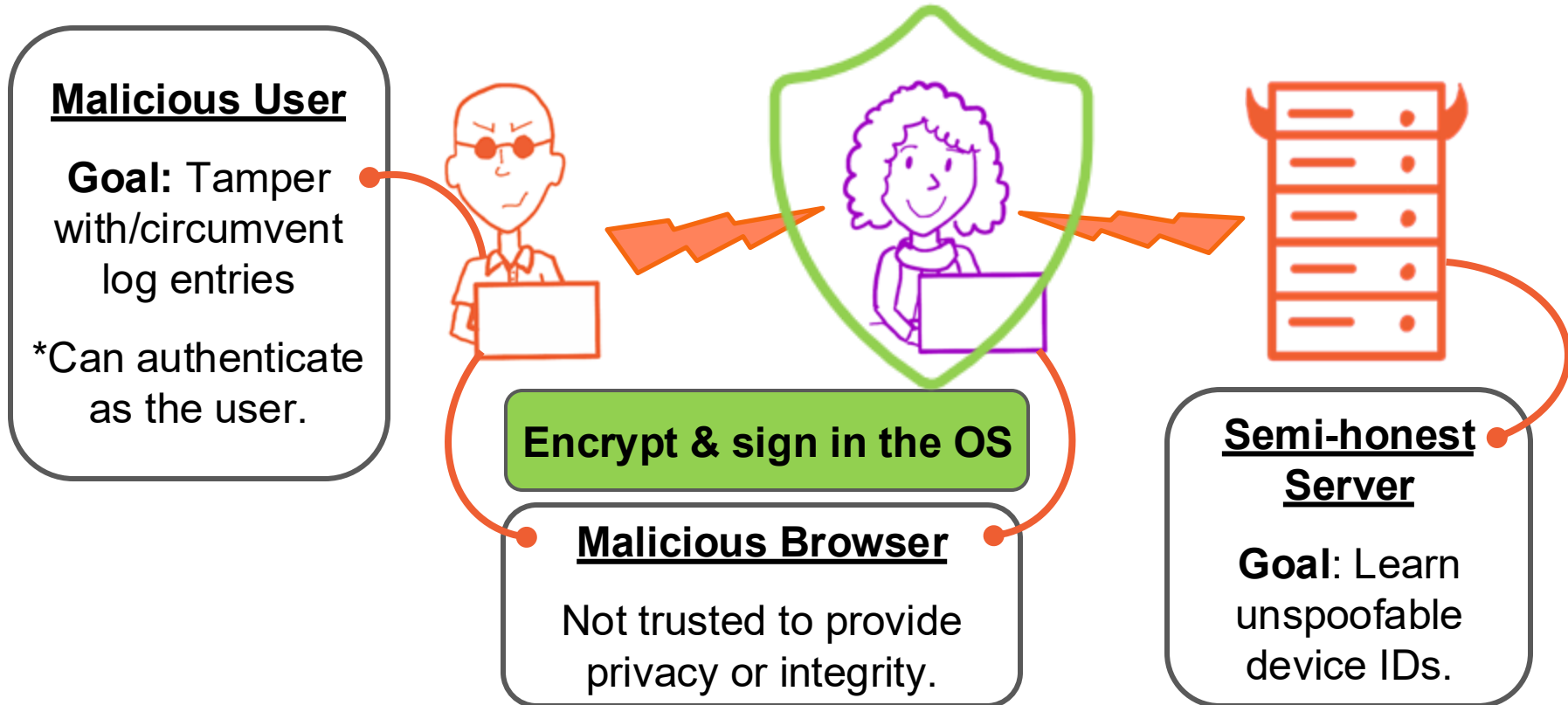
Providing attribution and privacy



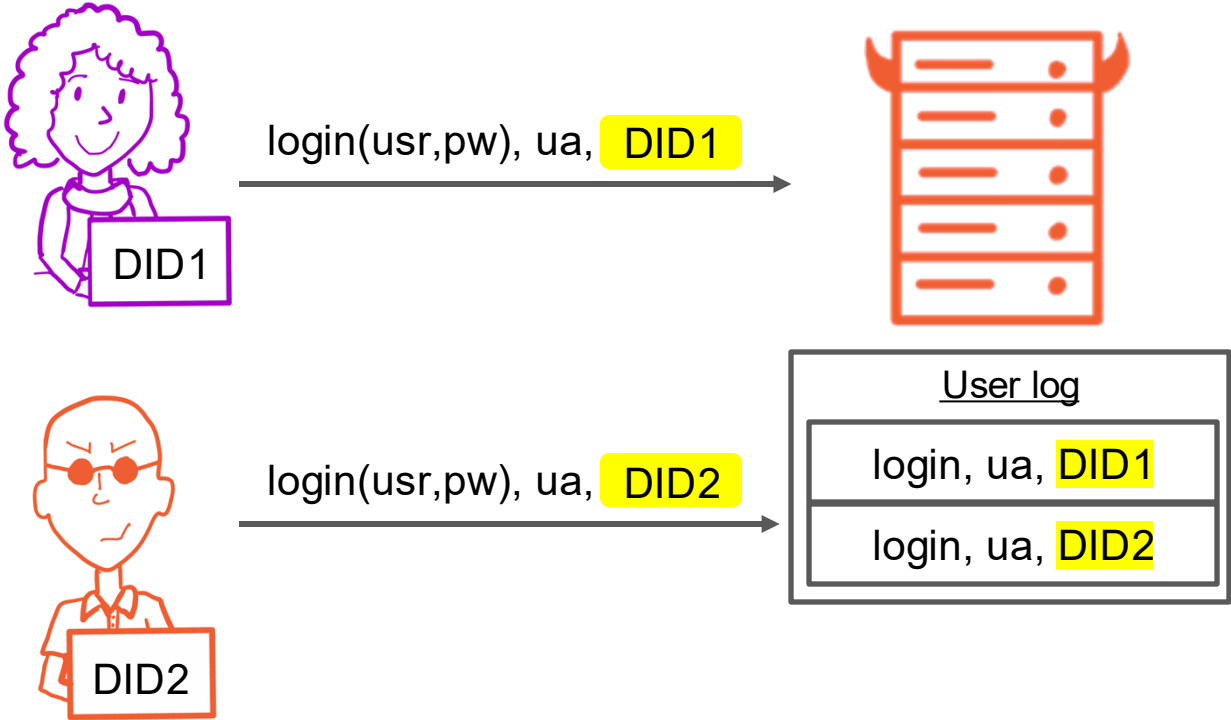
Providing attribution and privacy



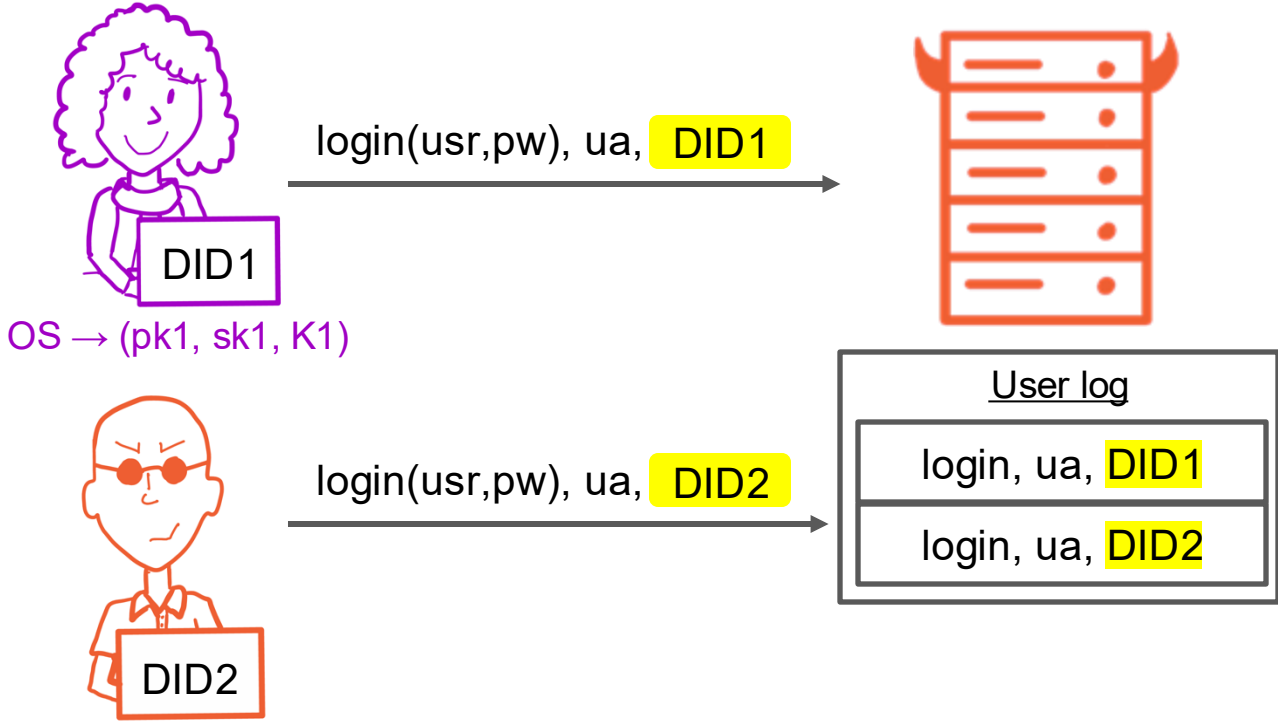
Providing attribution and privacy



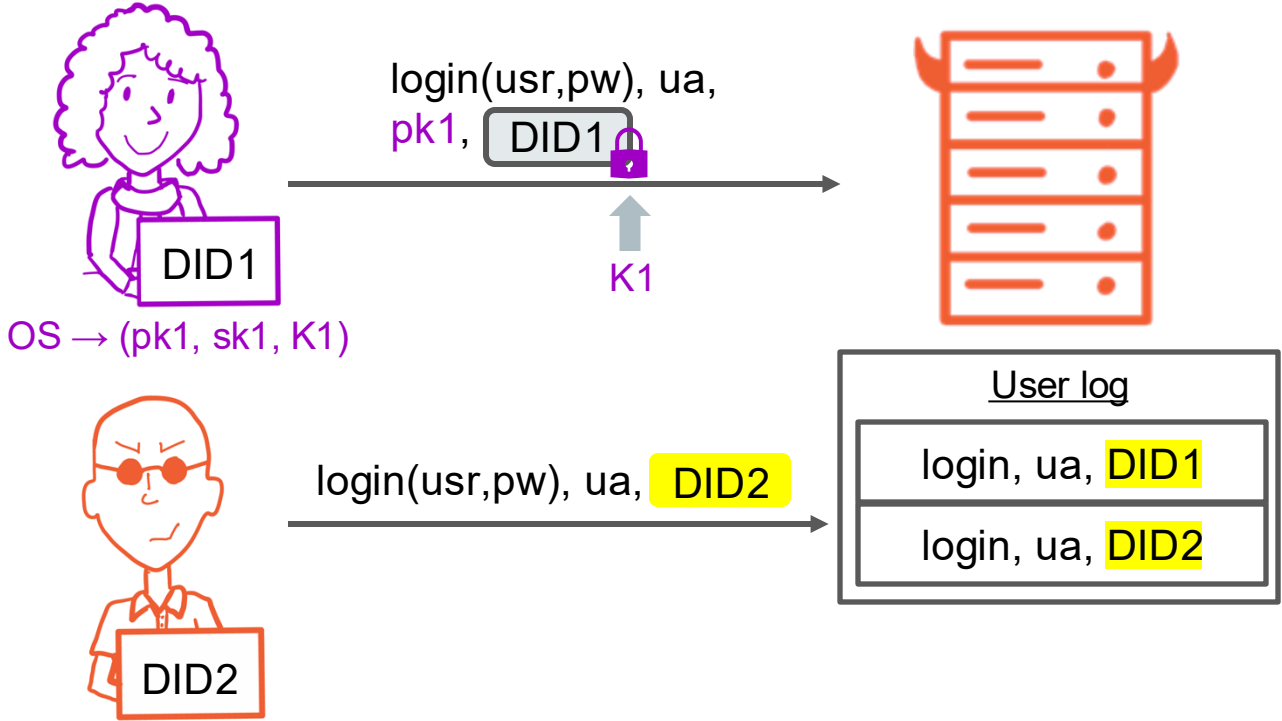
Client-side-encrypted access logging (CSAL)



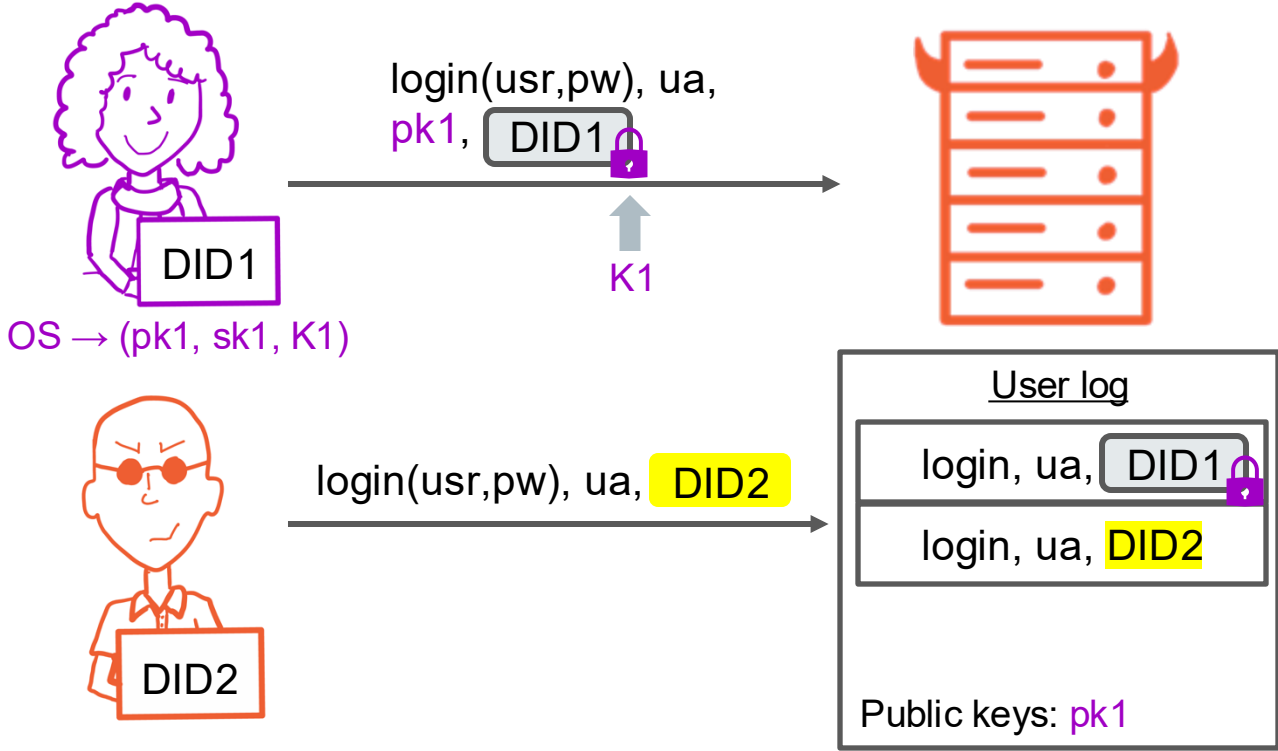
Client-side-encrypted access logging (CSAL)



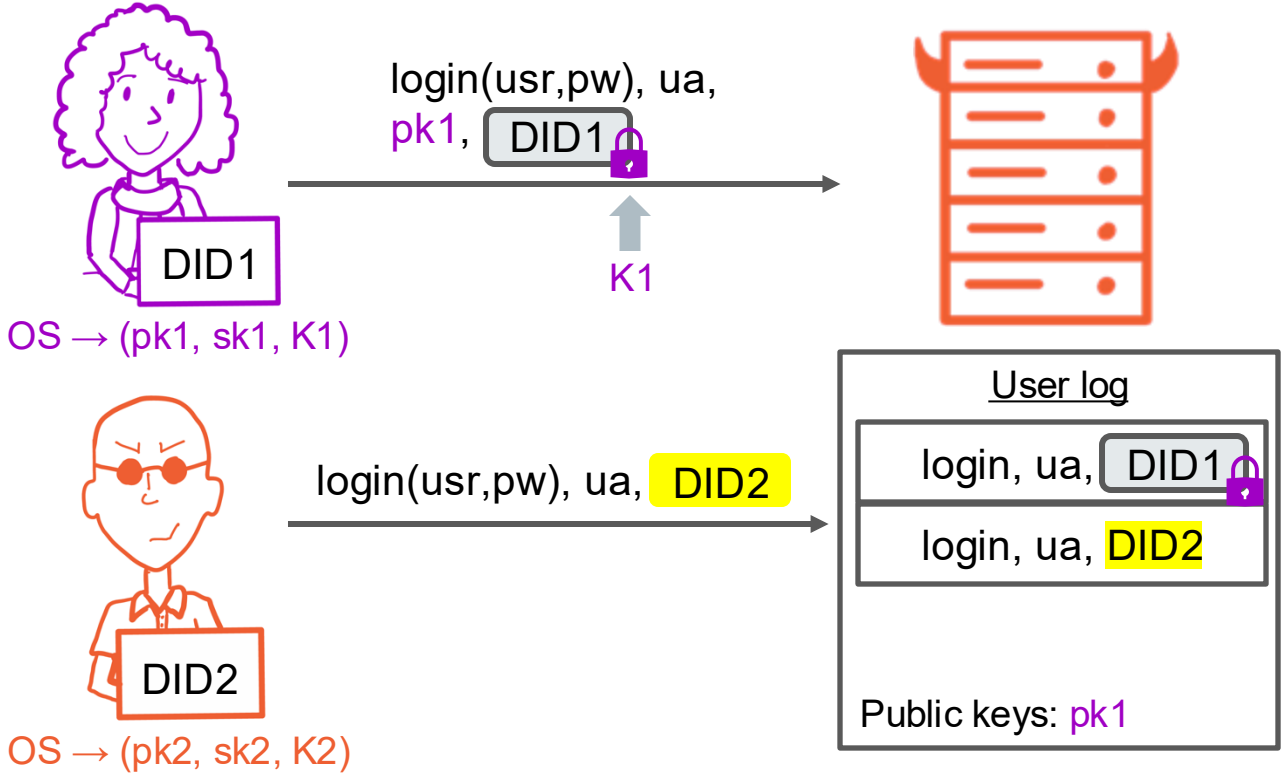
Client-side-encrypted access logging (CSAL)



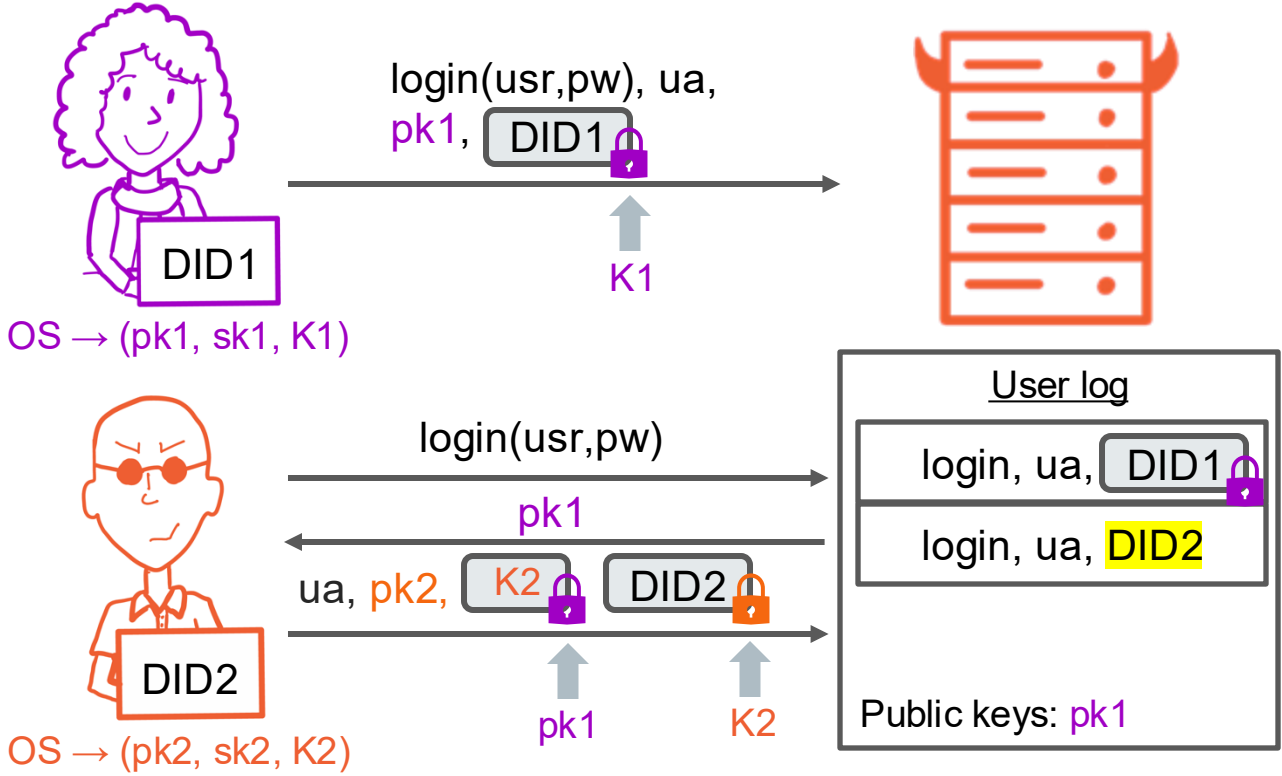
Client-side-encrypted access logging (CSAL)



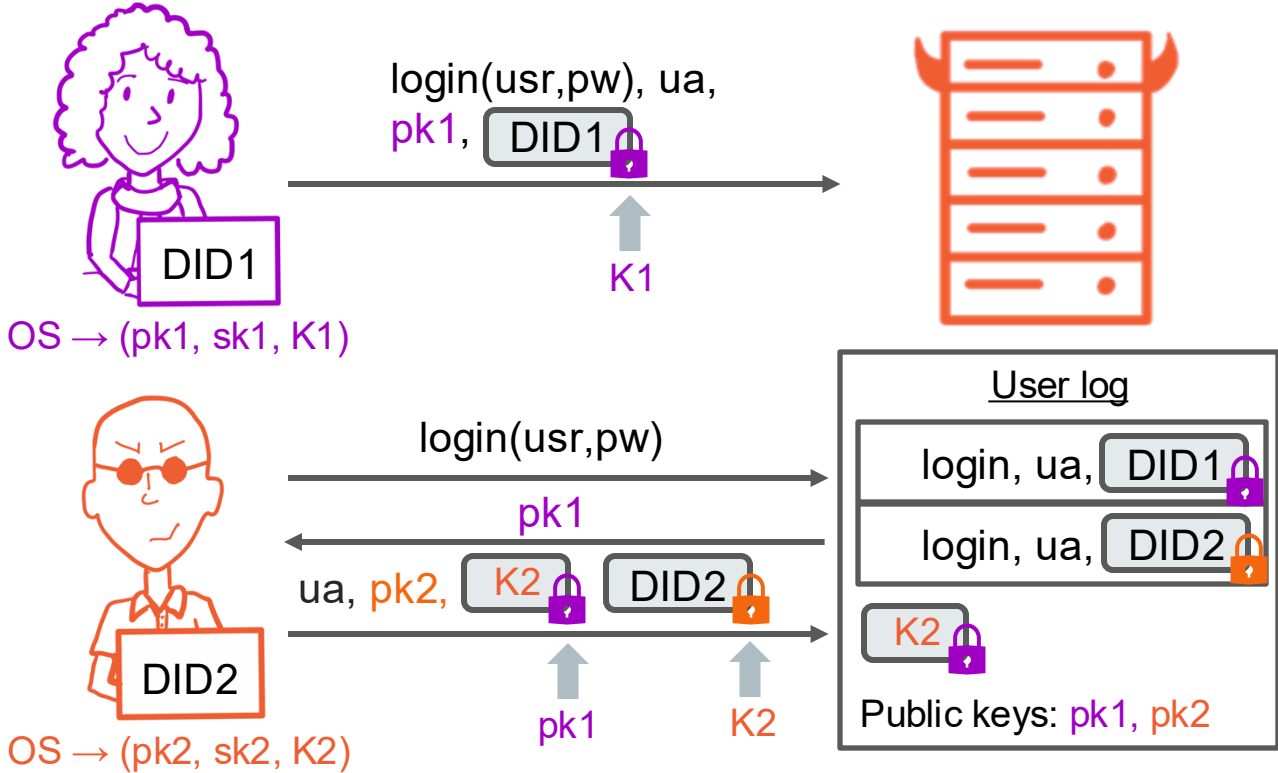
Client-side-encrypted access logging (CSAL)



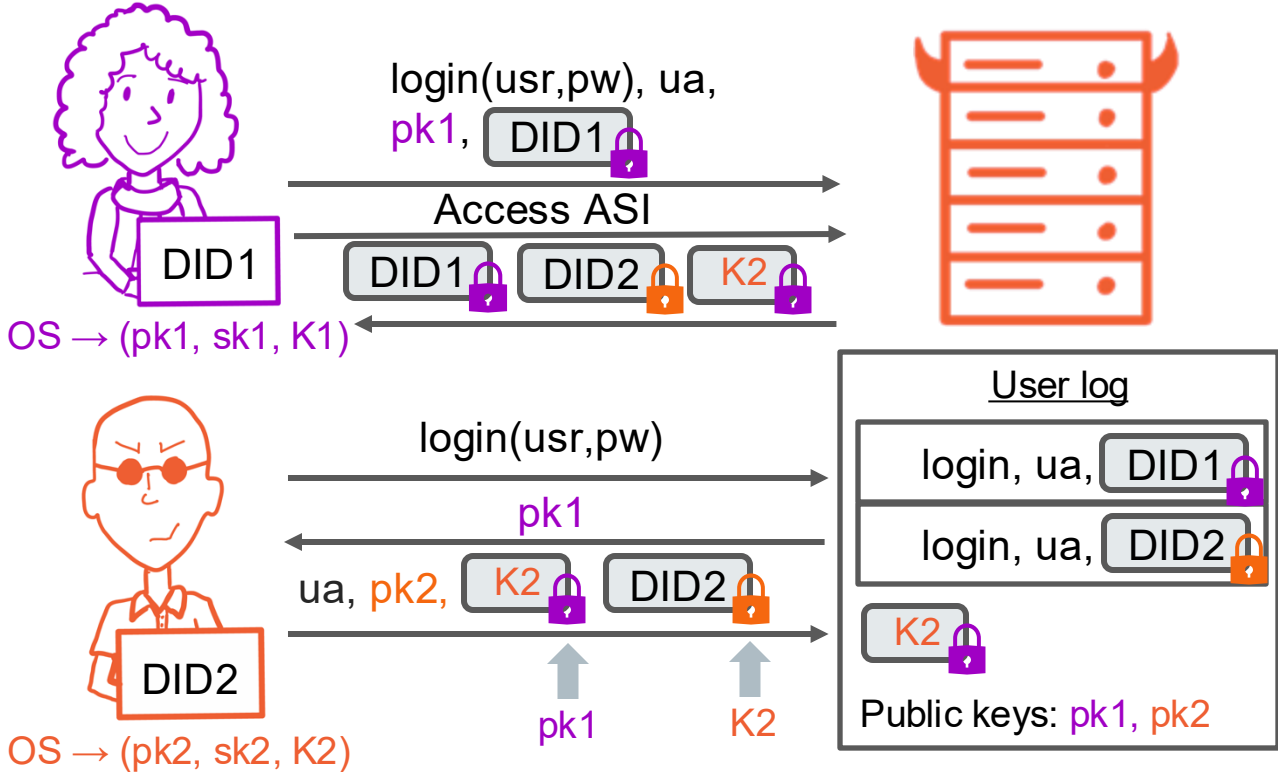
Client-side-encrypted access logging (CSAL)



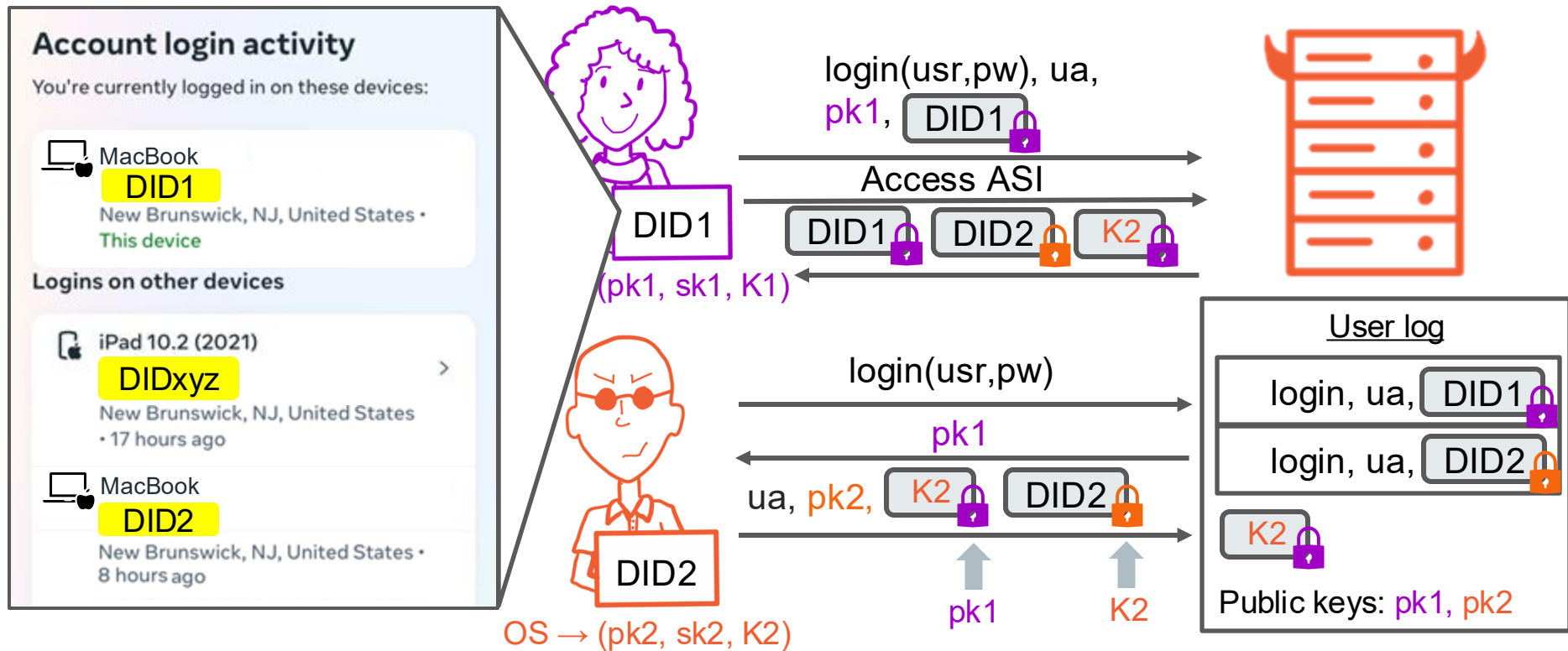
Client-side-encrypted access logging (CSAL)



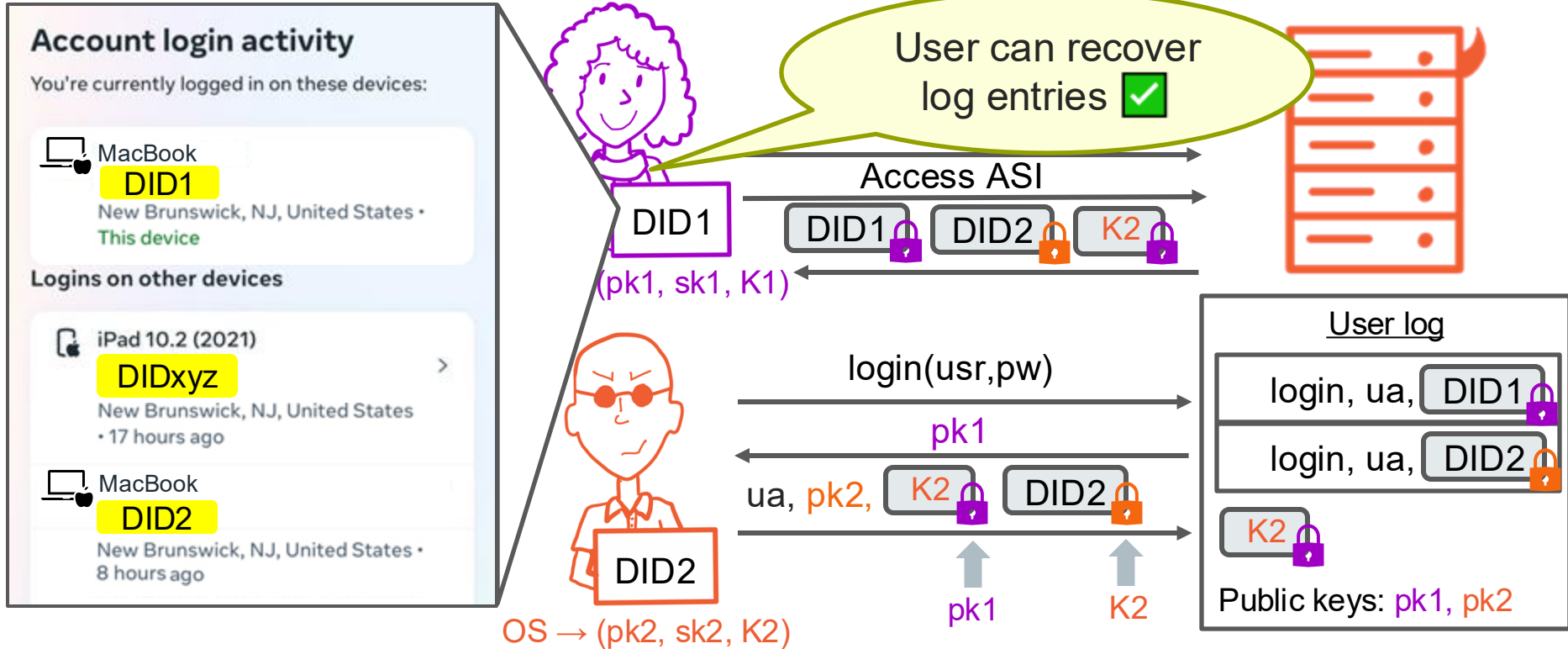
Client-side-encrypted access logging (CSAL)



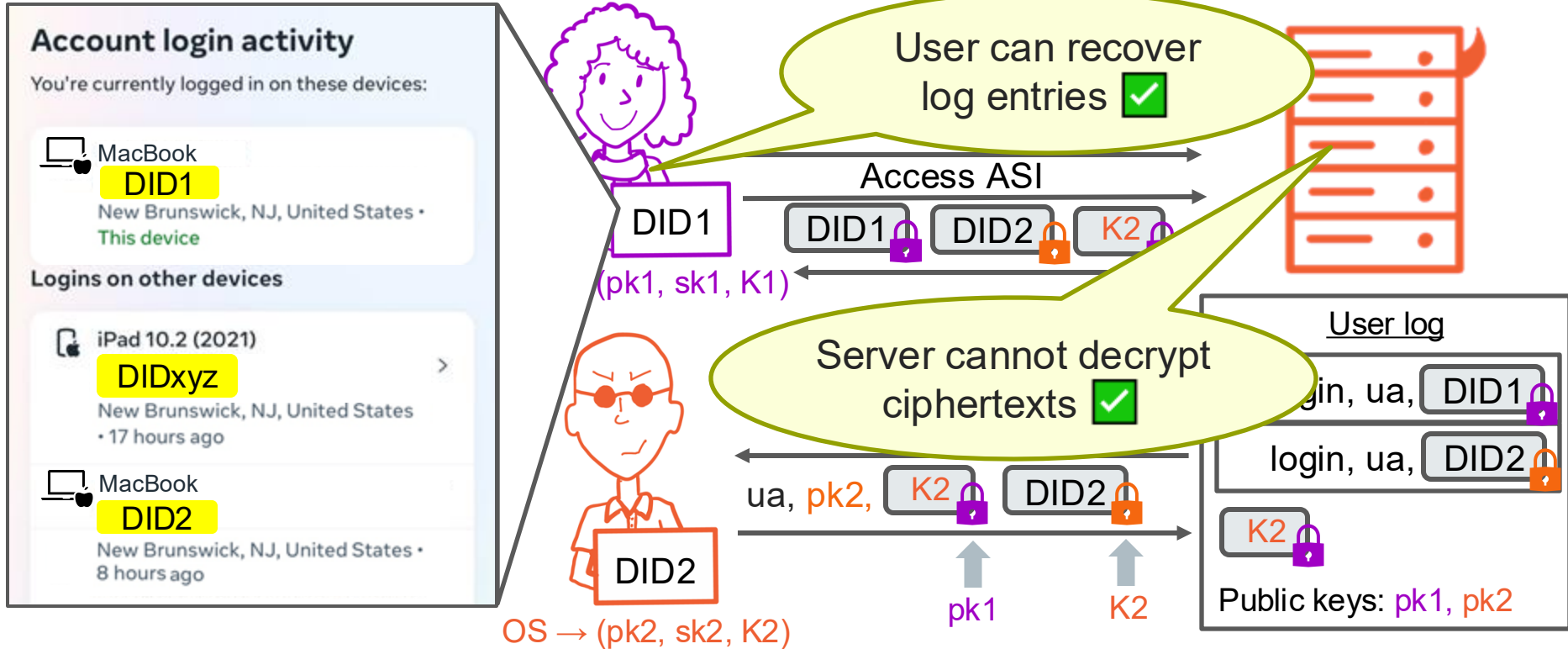
Client-side-encrypted access logging (CSAL)



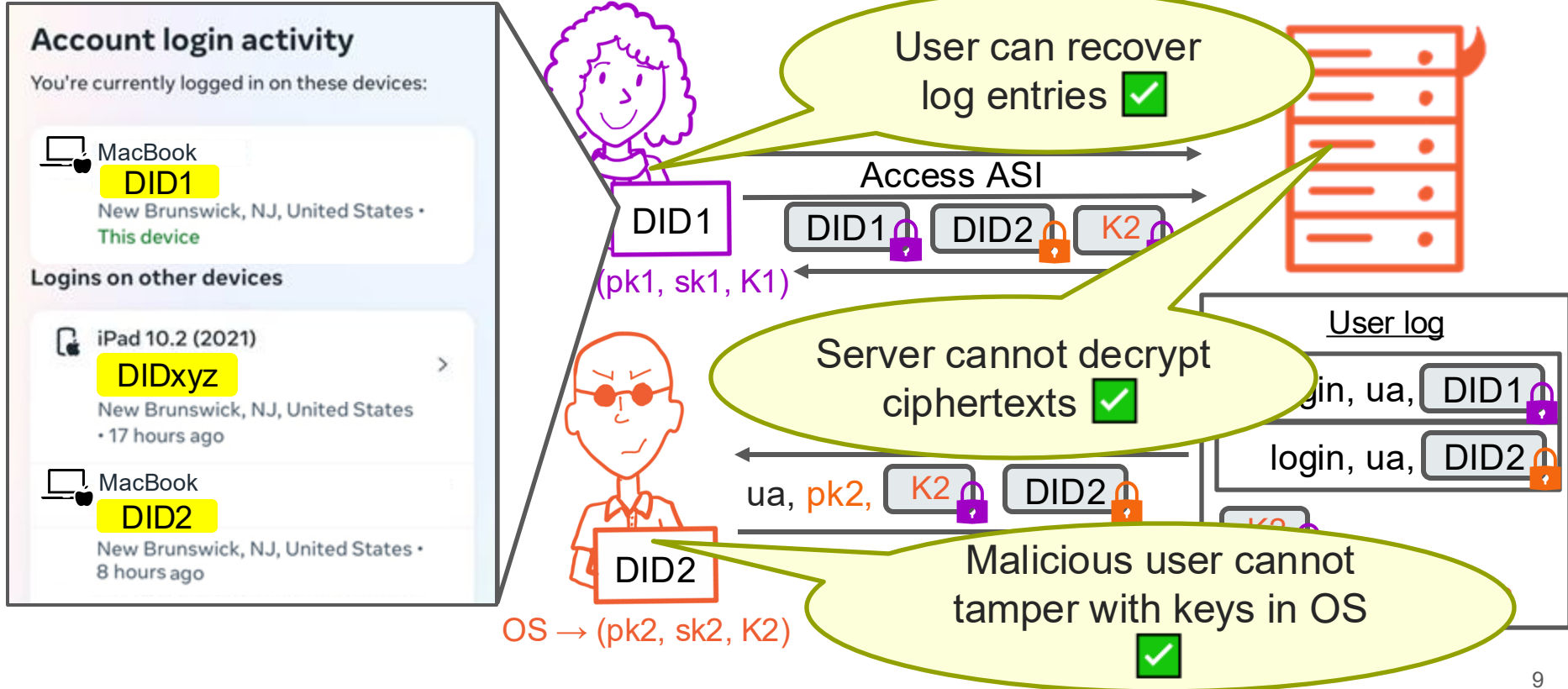
Client-side-encrypted access logging (CSAL)



Client-side-encrypted access logging (CSAL)



Client-side-encrypted access logging (CSAL)



Formal treatment of CSAL

- **Log privacy** and **session unlinkability** against server
- “**Ability to access**” log entries

<u>PRIV$_{\Pi}(\mathcal{D})$</u>	$st_{rp} \leftarrow \$ \mathcal{I}_s ; b \leftarrow \$ \{0, 1\}$ $b' \leftarrow \$ \mathcal{D}^{\mathcal{O}}(st_{rp})$ Return (st_{rp}, b, b')
<u>UNLINK$_{\Pi}(\mathcal{D})$</u>	$b \leftarrow \$ \{0, 1\}$ $\mu \leftarrow \mu$ $st_{rp} \leftarrow \$ \mathcal{I}_s$ $b' \leftarrow \$ \mathcal{D}^{\mathcal{O}}(st_{rp})$
<u>LoginL</u>	Return $\text{LIS}_{\Pi, \text{prune}}(\mathcal{A})$
If $c > \mu$	$st_{rp} \leftarrow \$ \mathcal{I}_s ; \text{win} \leftarrow 0$
(sid, st_c)	<u>InitClient</u> $\mathcal{A}^{\mathcal{O}}$
$\gamma_{c, sid}$	$\mu \leftarrow \mu$ Return win
Return	$st_{\mu} \leftarrow \$$
<u>ActionL</u>	<u>InitClient</u>
If $\gamma_{c, sid}$	$\mu \leftarrow \mu + 1 ; st_{\mu} \leftarrow \$ \mathcal{I}_c$
(st_c, st_{rp})	(sid, st_c) <u>Login</u> (c, OS, CL, RP)
Return	$\gamma[sid]$ If $c > \mu$ then Return \perp
Re-enc	Return $(sid, st_c, st_{rp}) \leftarrow \$ \mathcal{L}((st_c, OS, CL, RP))$
If $\gamma_{c, sid}$	$\gamma_{c, sid} \leftarrow \text{True}$
(st_c, st_{rp})	<u>Action</u> (c, sid, OS, CL, RP)
Return	$q \leftarrow q + 1$
Re-enc	If $\gamma[sid]$ $\mathcal{T}^*[q] \leftarrow (\text{INIT}, c, sid, OS, CL, RP)$
If $\gamma[sid]$	Return (sid, st_c)
Return	<u>Action</u> (c, sid, OS, CL, RP)
Re-enc	If $\gamma_{c, sid} = \perp$ then Return \perp
If $\gamma[sid]$	$(st_c, st_{rp}) \leftarrow \$ \mathcal{N}((st_c, sid, OS, CL, RP))$
	$q \leftarrow q + 1$

Formal treatment of CSAL

- Log privacy and session unlinkability against server
- “Ability to access” log entries

Theorem: Cannot have privacy and access all log entries.

```

PRIV $\Pi$ ( $\mathcal{D}$ )
 $st_{rp} \leftarrow \$ \mathcal{I}_s$  ;  $b \leftarrow \$ \{0, 1\}$ 
 $b' \leftarrow \$ \mathcal{D}^{\mathcal{O}}(st_{rp})$ 
Return  $(b, b')$ 

UNLINK $\Pi$ ( $\mathcal{D}$ )
InitClient
 $b \leftarrow \$ \{0, 1\}$ 
 $\mu \leftarrow \mu$ 
 $st_{rp} \leftarrow \$ \mathcal{I}_s$ 
 $b' \leftarrow \$ \mathcal{D}^{\mathcal{O}}(st_{rp})$ 
LoginL
Return  $(b, b')$ 
If  $c > \mu$ 
 $(sid, st_{rp}) \leftarrow \$ \mathcal{A}^{\mathcal{O}}$ 
 $\gamma_{c, sid} \leftarrow \mu$ 
Return  $st_{rp}$ 

LIS $\Pi, \text{prune}(\mathcal{A})$ 
InitClient
 $st_{rp} \leftarrow \$ \mathcal{I}_s$  ; win  $\leftarrow 0$ 
 $\mathcal{A}^{\mathcal{O}}$ 
Return win

Login(c)
InitClient
 $\mu \leftarrow \mu + 1$  ;  $st_{\mu} \leftarrow \$ \mathcal{I}_c$ 
If  $c > \mu$ 
Login(c, OS, CL, RP)
If  $c > \mu$  then Return  $\perp$ 
 $(sid, st_c, st_{rp}) \leftarrow \$ \mathcal{L}((st_c, OS, CL, RP))$ 
 $\gamma_{c, sid} \leftarrow \text{True}$ 
Return  $(sid, st_c)$ 

Action(c)
If  $\gamma_{c, sid} = \perp$ 
 $q \leftarrow q + 1$ 
If  $\gamma[sid]$ 
 $\mathcal{T}^*[q] \leftarrow (\text{INIT}, c, sid, OS, CL, RP)$ 
Return  $(sid, st_c)$ 

Re-encr
Action(c, sid, OS, CL, RP)
If  $\gamma_{c, sid} = \perp$  then Return  $\perp$ 
 $(st_c, st_{rp}) \leftarrow \$ \mathcal{N}((st_c, sid, OS, CL, RP))$ 
Return  $(st_c, st_{rp})$ 

```

Formal treatment of CSAL

- **Log privacy** and **session unlinkability** against server
- “**Ability to access**” log entries

Theorem: Cannot have privacy and access all log entries.

$\text{PRIV}_{\Pi}(\mathcal{D})$

$st_{rp} \leftarrow \$ \mathcal{I}_s ; b \leftarrow \$ \{0, 1\}$

$b' \leftarrow \$ \mathcal{D}^{\mathcal{O}}(st_{rp})$

Return

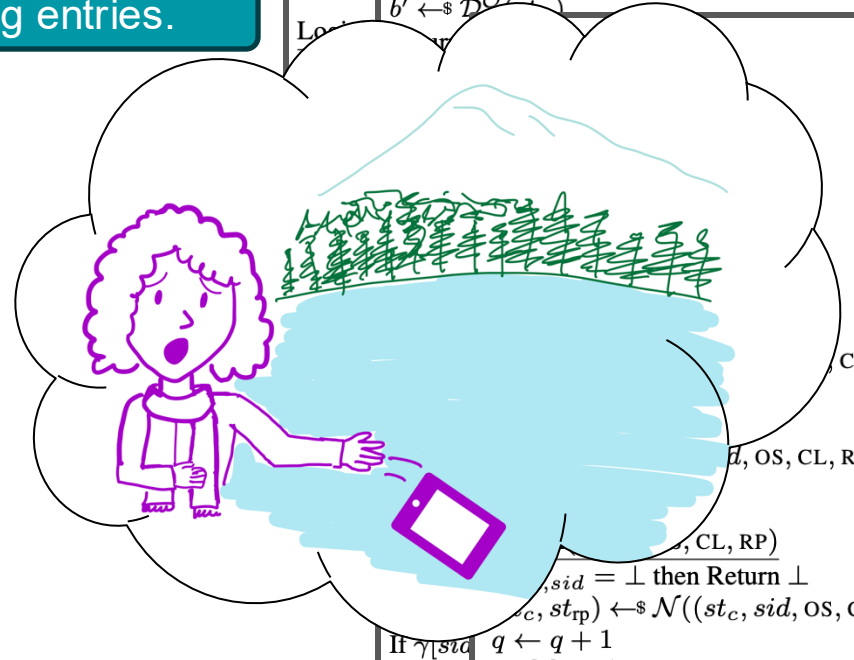
$\text{UNLINK}_{\Pi}(\mathcal{D})$

InitClic $b \leftarrow \$ \{0, 1\}$

$\mu \leftarrow \mu ; st_{rp} \leftarrow \$ \mathcal{I}_s$

$b' \leftarrow \$ \mathcal{D}^{\mathcal{O}}(st_{rp})$

Log



Formal treatment of CSAL

- Log privacy and session unlinkability against server
- “Ability to access” log entries

Theorem: Cannot have privacy and access all log entries.

```

PRIV $\Pi$ ( $\mathcal{D}$ )
 $st_{rp} \leftarrow \$ \mathcal{I}_s$  ;  $b \leftarrow \$ \{0, 1\}$ 
 $b' \leftarrow \$ \mathcal{D}^{\mathcal{O}}(st_{rp})$ 
Return  $(b, b')$ 

UNLINK $\Pi$ ( $\mathcal{D}$ )
InitClient
 $b \leftarrow \$ \{0, 1\}$ 
 $\mu \leftarrow \mu$ 
 $st_{rp} \leftarrow \$ \mathcal{I}_s$ 
 $b' \leftarrow \$ \mathcal{D}^{\mathcal{O}}(st_{rp})$ 
LoginL
Return  $(b, b')$ 
If  $c > \mu$ 
 $(sid, st_{rp}) \leftarrow \$ \mathcal{A}^{\mathcal{O}}$ 
 $\gamma_{c, sid} \leftarrow \mu$ 
Return  $st_{rp}$ 

LIS $\Pi, \text{prune}$ ( $\mathcal{A}$ )
InitClient
 $st_{rp} \leftarrow \$ \mathcal{I}_s$  ; win  $\leftarrow 0$ 
Return win

Login(c)
 $\mu \leftarrow \mu + 1$  ;  $st_{\mu} \leftarrow \$ \mathcal{I}_c$ 
If  $c > \mu$ 
 $(sid, st_{rp}) \leftarrow \$ \mathcal{L}((st_c, OS, CL, RP))$ 
Return  $\gamma[sid]$ 

Re-enc
 $\gamma_{c, sid} \leftarrow \text{True}$ 
Action(c)
 $q \leftarrow q + 1$ 
If  $\gamma[sid] = \perp$ 
 $\mathcal{T}^*[q] \leftarrow (\text{INIT}, c, sid, OS, CL, RP)$ 
Return  $(sid, st_c)$ 

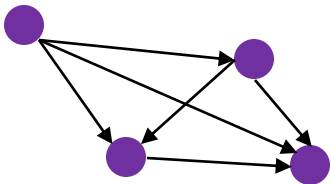
Action(c, sid, OS, CL, RP)
If  $\gamma_{c, sid} = \perp$  then Return  $\perp$ 
Return  $(st_c, st_{rp}) \leftarrow \$ \mathcal{N}((st_c, sid, OS, CL, RP))$ 
Re-enc
 $q \leftarrow q + 1$ 

```

Formal treatment of CSAL

- Log privacy and session unlinkability against server
- “Ability to access” log entries

Theorem: Cannot have privacy and access all log entries.



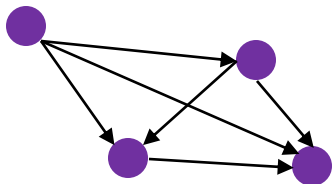
- Define reachability graph to characterize ciphertext access

$\text{PRIV}_{\Pi}(\mathcal{D})$	$st_{rp} \leftarrow \$ \mathcal{I}_s ; b \leftarrow \$ \{0, 1\}$ $b' \leftarrow \$ \mathcal{D}^{\mathcal{O}}(st_{rp})$ Return (b, b')
$\text{UNLINK}_{\Pi}(\mathcal{D})$	$b \leftarrow \$ \{0, 1\}$ $\mu \leftarrow \mu$ $st_{rp} \leftarrow \$ \mathcal{I}_s$ $b' \leftarrow \$ \mathcal{D}^{\mathcal{O}}(st_{rp})$
$\text{LoginLIS}_{\Pi, \text{prune}}(\mathcal{A})$	Return $\text{LIS}_{\Pi, \text{prune}}(\mathcal{A})$
InitClient	$st_{rp} \leftarrow \$ \mathcal{I}_s ; \text{win} \leftarrow 0$ $\mathcal{A}^{\mathcal{O}}$ Return win
Login	$\mu \leftarrow \mu + 1 ; st_{\mu} \leftarrow \$ \mathcal{I}_c$
Action	$\text{Login}(c, \text{OS}, \text{CL}, \text{RP})$ If $c > \mu$ then Return \perp Return $(sid, st_c, st_{rp}) \leftarrow \$ \mathcal{L}((st_c, \text{OS}, \text{CL}, \text{RP}))$
Re-enc	$\gamma_{c, sid} \leftarrow \text{True}$
Action	$q \leftarrow q + 1$ If $\gamma[sid]$ then $\mathcal{T}^*[q] \leftarrow (\text{INIT}, c, sid, \text{OS}, \text{CL}, \text{RP})$ Return (sid, st_c)
Action	$\text{Action}(c, sid, \text{OS}, \text{CL}, \text{RP})$ If $\gamma_{c, sid} = \perp$ then Return \perp
Re-enc	$(st_c, st_{rp}) \leftarrow \$ \mathcal{N}((st_c, sid, \text{OS}, \text{CL}, \text{RP}))$
Action	$q \leftarrow q + 1$

Formal treatment of CSAL

- **Log privacy** and **session unlinkability** against server
- “**Ability to access**” log entries

Theorem: Cannot have privacy and access all log entries.



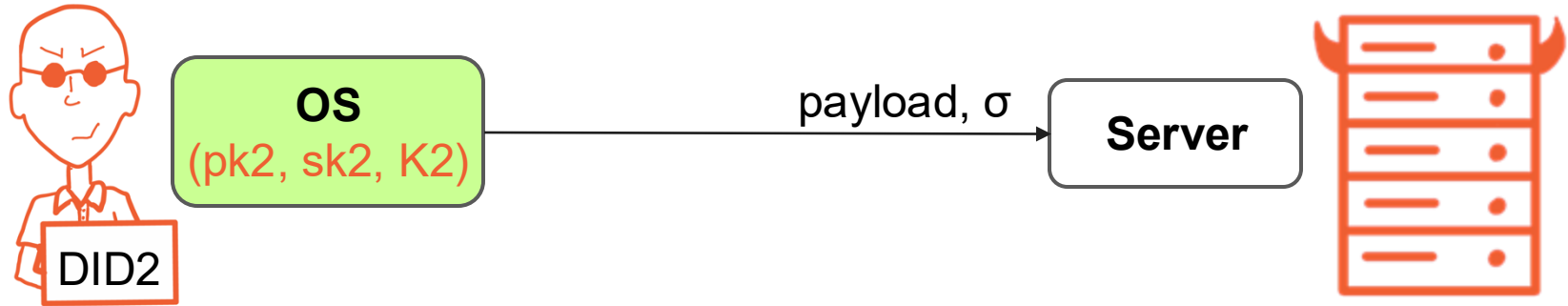
- Define reachability graph to characterize ciphertext access

Theorem: Assuming secure encryption, our scheme achieves privacy, unlinkability, and log access determined by the reachability graph

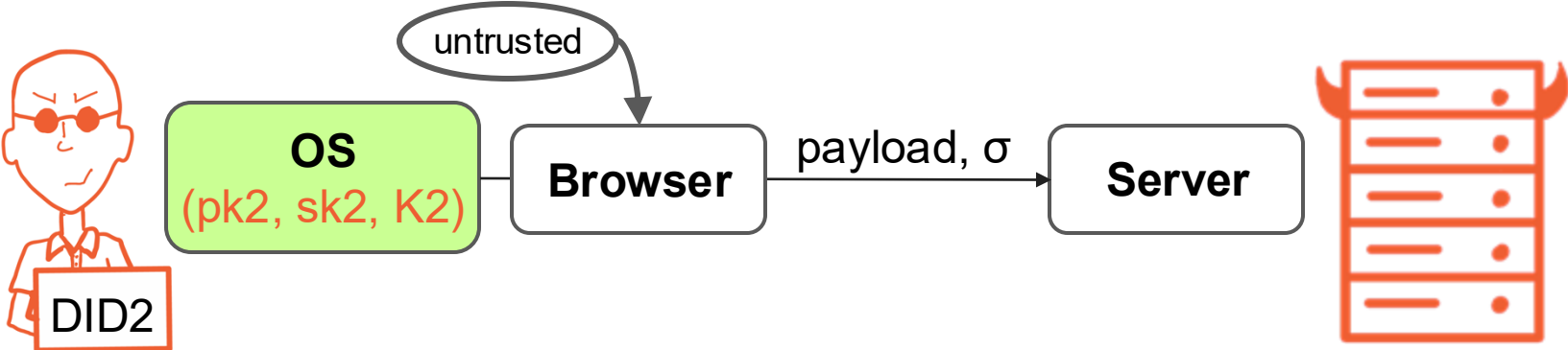
$\text{PRIV}_{\Pi}(\mathcal{D})$ $st_{rp} \leftarrow \mathcal{I}_s ; b \leftarrow \{0, 1\}$ $b' \leftarrow \mathcal{D}^{\mathcal{O}}(st_{rp})$ Return (b, b')	$\text{UNLINK}_{\Pi}(\mathcal{D})$ $b \leftarrow \{0, 1\}$ $\mu \leftarrow \mu$ $st_{rp} \leftarrow \mathcal{I}_s$ $b' \leftarrow \mathcal{D}^{\mathcal{O}}(st_{rp})$
LoginL If $c > \mu$ $(sid, st_c) \leftarrow \mathcal{A}^{\mathcal{O}}$ $\gamma_{c, sid} \leftarrow \mu$ Return $st_{\mu} \leftarrow st_c$	$\text{LIS}_{\Pi, \text{prune}}(\mathcal{A})$ $st_{rp} \leftarrow \mathcal{I}_s ; \text{win} \leftarrow 0$ $\mathcal{A}^{\mathcal{O}}$ Return win
ActionL If $\gamma_{c, sid} = \perp$ $(st_c, st_{rp}) \leftarrow \mathcal{L}(st_c, OS, CL, RP)$ Return $\gamma[sid]$	InitClient $\mu \leftarrow \mu + 1 ; st_{\mu} \leftarrow \mathcal{I}_c$
Re-enc If $\gamma_{c, sid} = \perp$ $(st_c, st_{rp}) \leftarrow \mathcal{N}(st_c, sid, OS, CL, RP)$ Return $q \leftarrow q + 1$	$\text{Login}(c, OS, CL, RP)$ If $c > \mu$ then Return \perp $(sid, st_c, st_{rp}) \leftarrow \mathcal{L}(st_c, OS, CL, RP)$ $\gamma_{c, sid} \leftarrow \text{True}$
$\text{Action}(c, sid, OS, CL, RP)$ If $\gamma_{c, sid} = \perp$ then Return \perp $(st_c, st_{rp}) \leftarrow \mathcal{N}(st_c, sid, OS, CL, RP)$ Return $q \leftarrow q + 1$	$\text{Return } (sid, st_c)$

CSAL deployment architecture challenges

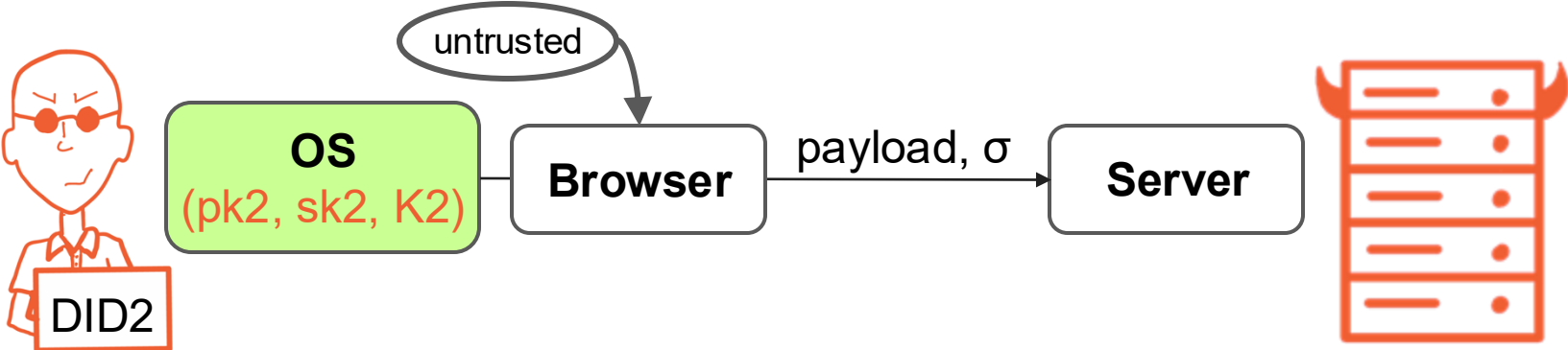
CSAL deployment architecture challenges



CSAL deployment architecture challenges

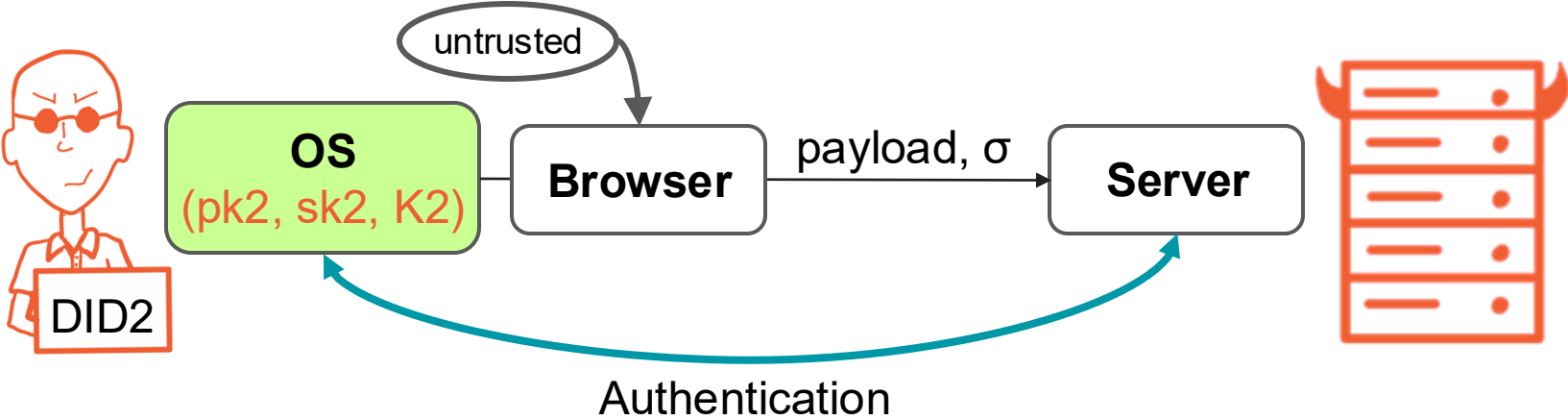


CSAL deployment architecture challenges



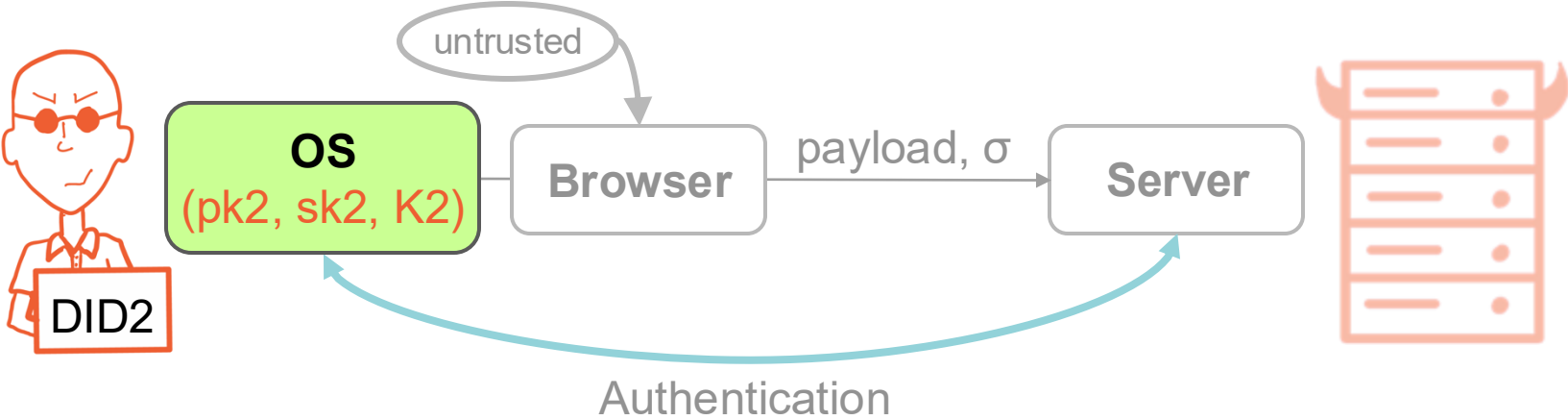
What about active attacks?

CSAL deployment architecture challenges



What about active attacks?

CSAL deployment architecture challenges



What about active attacks?

CSAL deployment architecture: OS authentication

- Based on the **FIDO2 framework**
 - Specifications for device authentication
 - WebAuthn → Passkeys
 - API to register and authenticate users using an authenticator

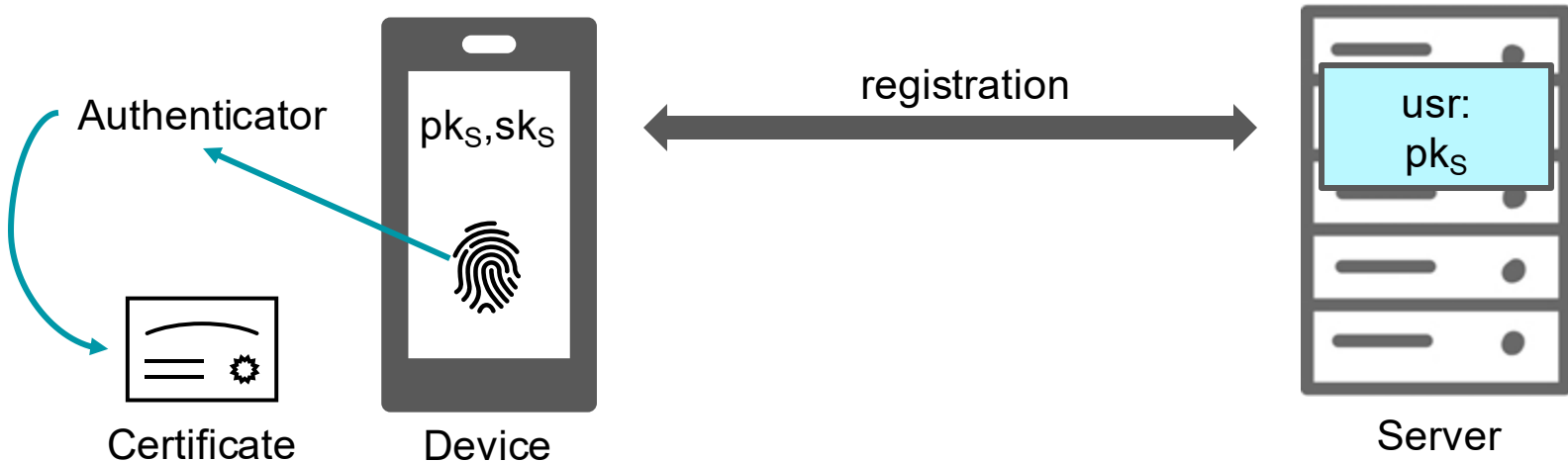
CSAL deployment architecture: OS authentication

- Based on the **FIDO2** framework
 - Specifications for device authentication
 - WebAuthn → Passkeys
 - API to register and authenticate users using an authenticator



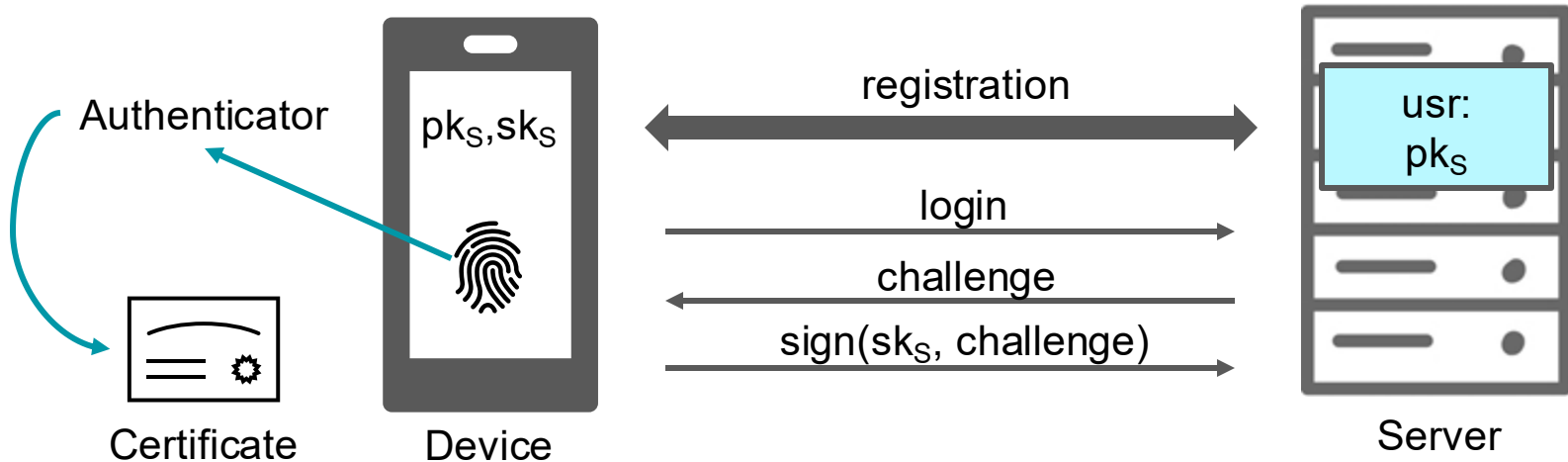
CSAL deployment architecture: OS authentication

- Based on the **FIDO2** framework
 - Specifications for device authentication
 - WebAuthn → Passkeys
 - API to register and authenticate users using an authenticator



CSAL deployment architecture: OS authentication

- Based on the **FIDO2** framework
 - Specifications for device authentication
 - WebAuthn → Passkeys
 - API to register and authenticate users using an authenticator

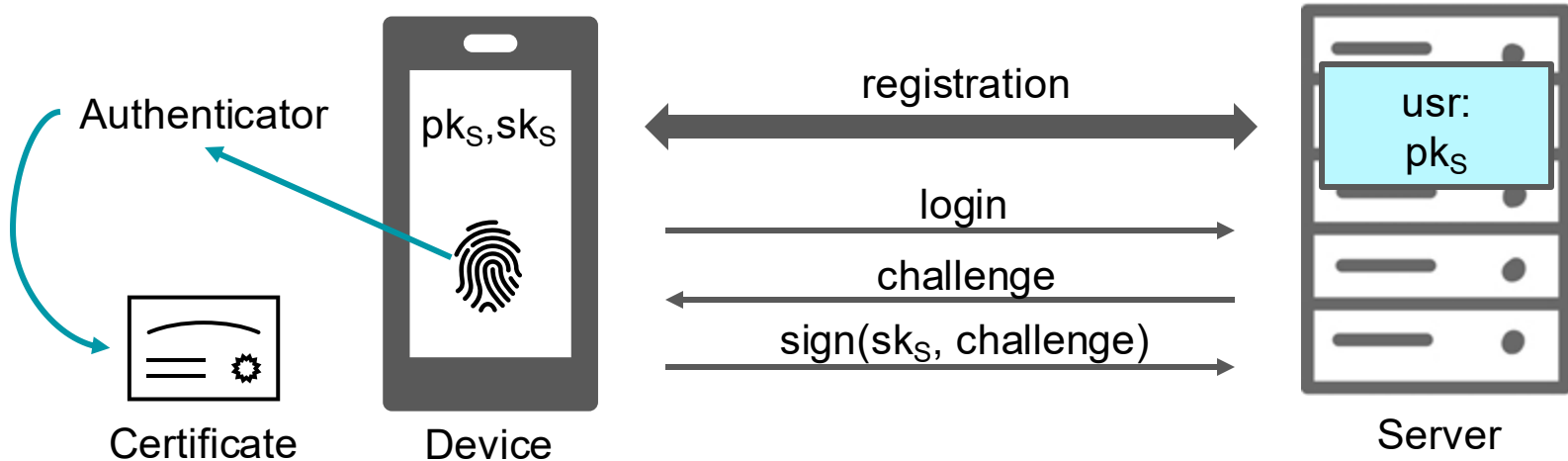


CSAL deployment architecture: OS authentication

- Based on the **FIDO2** framework
 - Specifications for device authentication
 - WebAuthn → Passkeys
 - API to register and authenticate users using an authenticator

Why FIDO2?

- Collaboration with OS vendors
- Handles cryptographic keys
- Widely deployed

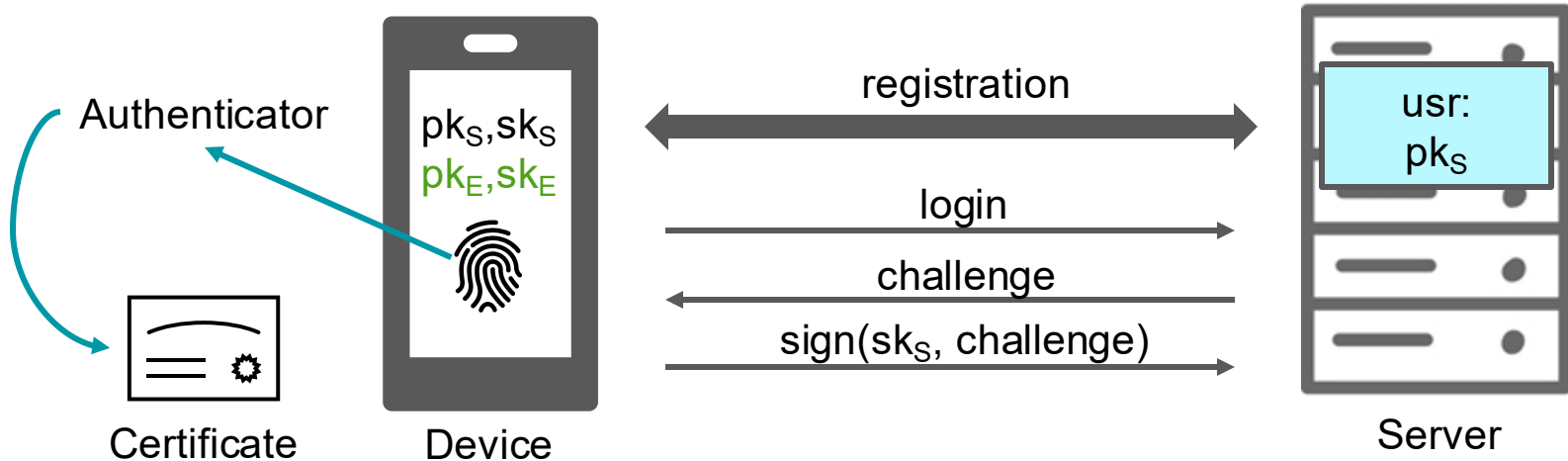


CSAL deployment architecture: OS authentication

- Based on the **FIDO2** framework
 - Specifications for device authentication
 - WebAuthn → Passkeys
 - API to register and authenticate users using an authenticator

Why FIDO2?

- Collaboration with OS vendors
- Handles cryptographic keys
- Widely deployed

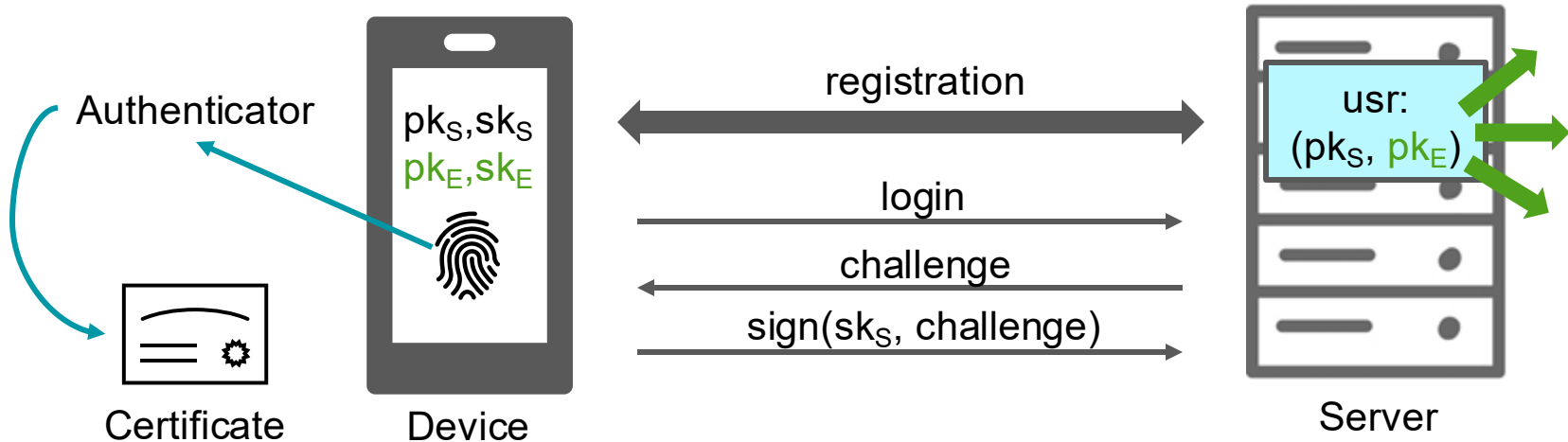


CSAL deployment architecture: OS authentication

- Based on the **FIDO2** framework
 - Specifications for device authentication
 - WebAuthn → Passkeys
 - API to register and authenticate users using an authenticator

Why FIDO2?

- Collaboration with OS vendors
- Handles cryptographic keys
- Widely deployed

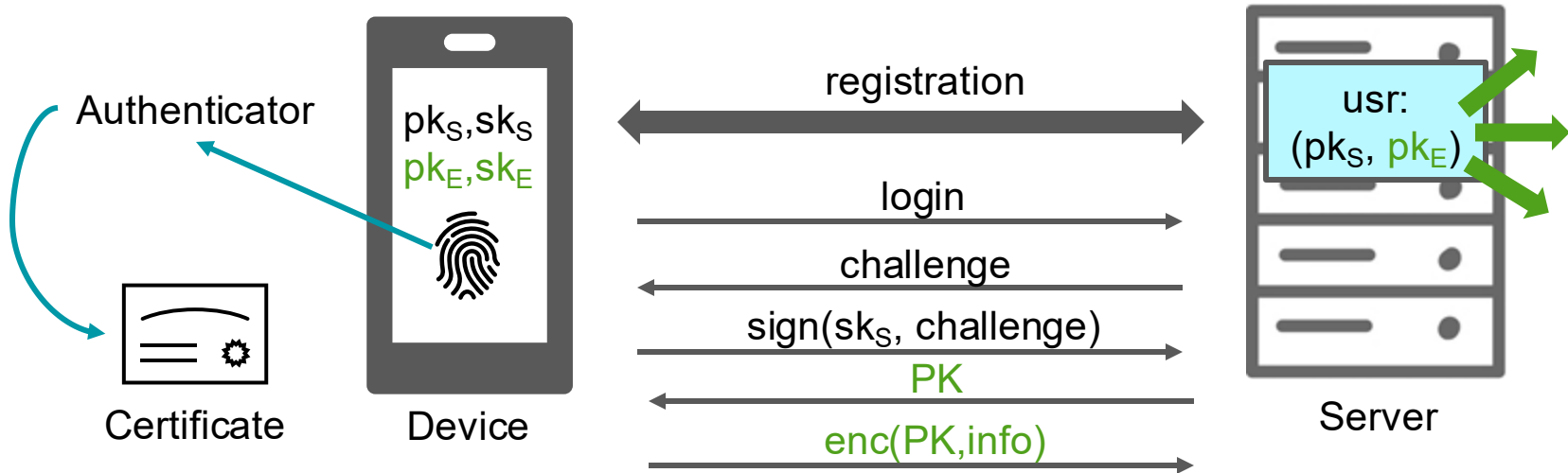


CSAL deployment architecture: OS authentication

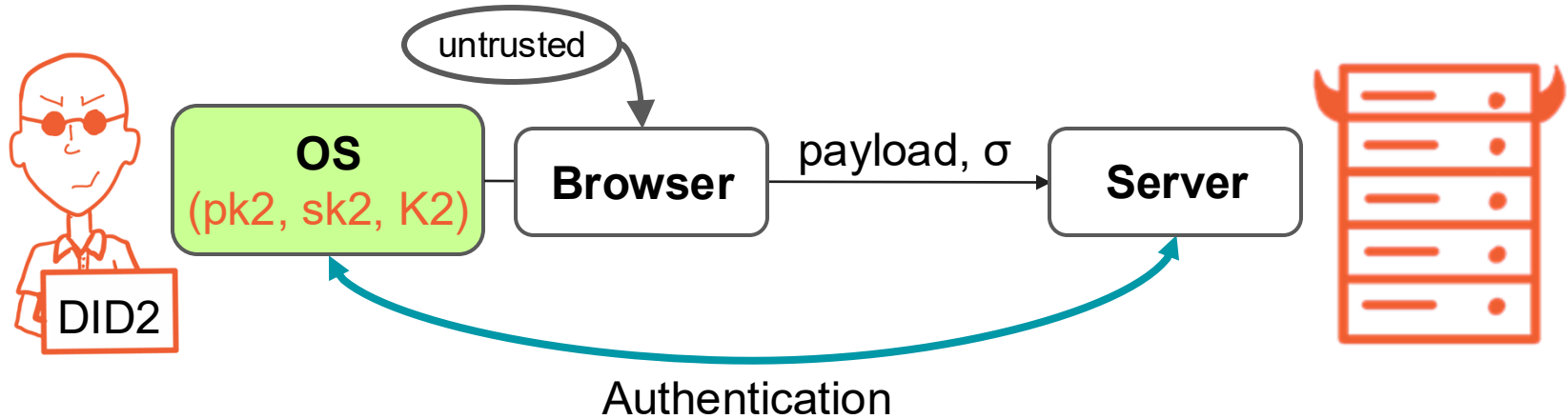
- Based on the **FIDO2** framework
 - Specifications for device authentication
 - WebAuthn → Passkeys
 - API to register and authenticate users using an authenticator

Why FIDO2?

- Collaboration with OS vendors
- Handles cryptographic keys
- Widely deployed



CSAL deployment architecture challenges

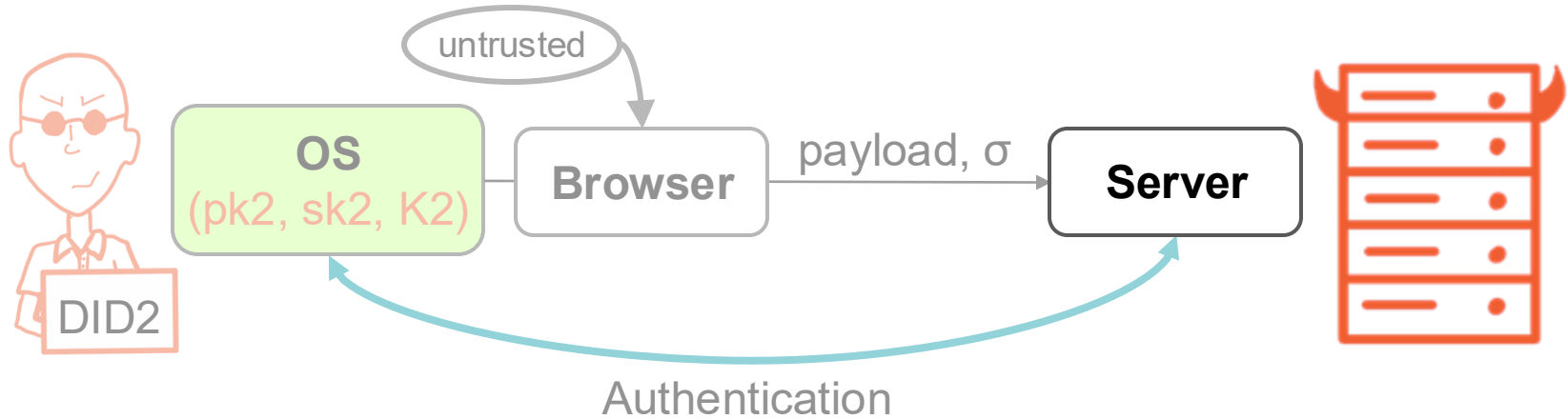


What about active attacks?

OS Authentication

FIDO2-style
certificates

CSAL deployment architecture challenges

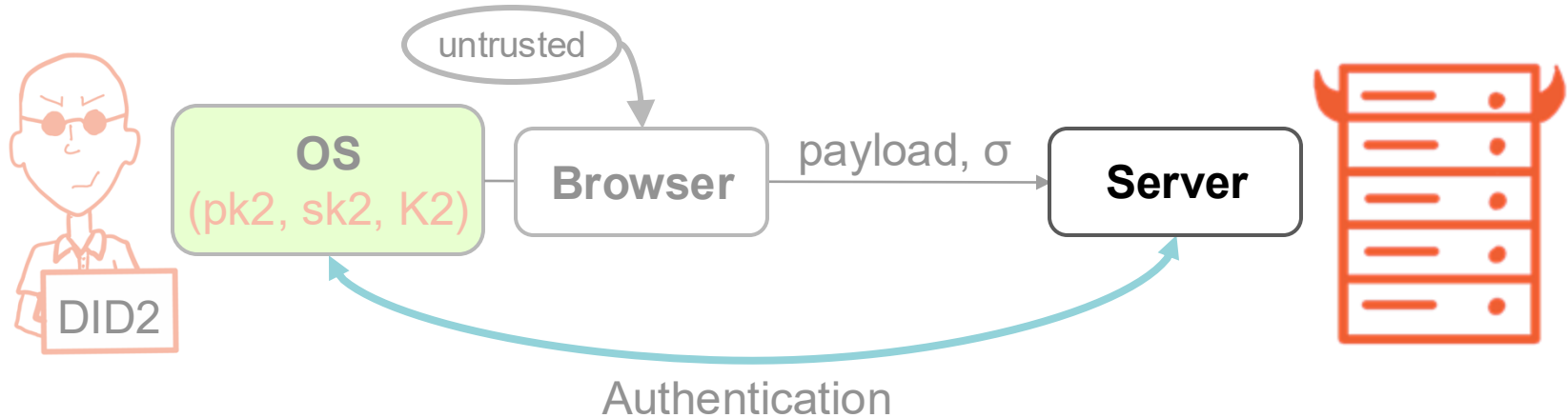


What about active attacks?

OS Authentication

FIDO2-style
certificates

CSAL deployment architecture challenges



What about active attacks?

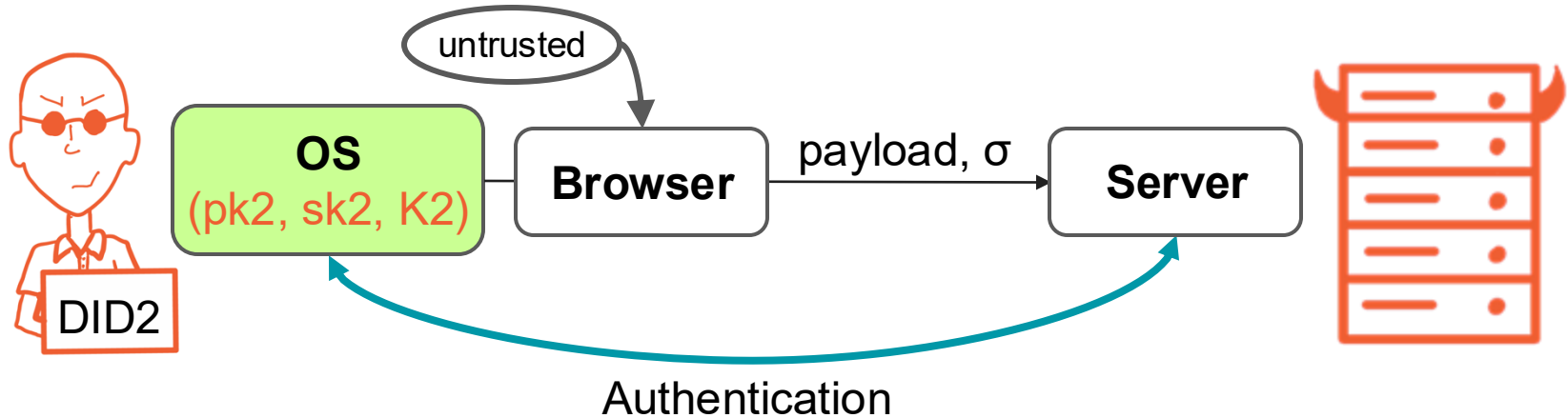
OS Authentication

FIDO2-style
certificates

Server PKI

Infrastructure
similar to TLS

CSAL deployment architecture challenges



What about active attacks?

OS Authentication

FIDO2-style
certificates

Server PKI

Infrastructure
similar to TLS

- ✓ Browser MiTM
- ✗ Server MiTM

Proof of concept

- Prototype Python implementation of a server, client, and encryptor
 - Login:
 - Bandwidth: ~5KB per single session login
 - Latency: 146ms for single session login
 - ASI log retrieval:
 - Bandwidth: ~2.6KB for one session
 - Latency: 0.63ms for single entry

Proof of concept

- Prototype Python implementation of a server, client, and encryptor
 - Login:
 - Bandwidth: ~5KB per single session login
 - Latency: 146ms for single session login
 - ASI log retrieval:
 - Bandwidth: ~2.6KB for one session
 - Latency: 0.63ms for single entry

Performance-wise, the system is practical

Future work

- Deployment
 - Collaboration between OS vendors and browsers and other clients
 - Similar to FIDO2
- Formalization against malicious server
- ASIs potential risks
 - Risks of user monitoring by abuser
- ASIs UX
 - What type of information should we include in ASIs?

Encrypted Access Logging for Online Accounts: Device Attributions without Device Tracking

Takeaways:

- ASIs are important
- Trade-offs between integrity, privacy, and full access to logs
- OS signed identifiers prevent other users from tampering with logs
- Encryption ensures privacy from server
- Open challenges surrounding architecture that requires collaboration between OS vendors and platforms



Carolina Ortega Pérez
carolina@cs.cornell.edu



Alaa Daffalla
alaadaffalla@cs.cornell.edu



Thomas Ristenpart
ristenpart@cornell.edu



Paper:
<https://bit.ly/452AiTa>