NDSS SYMPOSIUM

Anchors of Trust: A Usability Study on User Awareness, Consent, and Control in Cross-Device Authentication

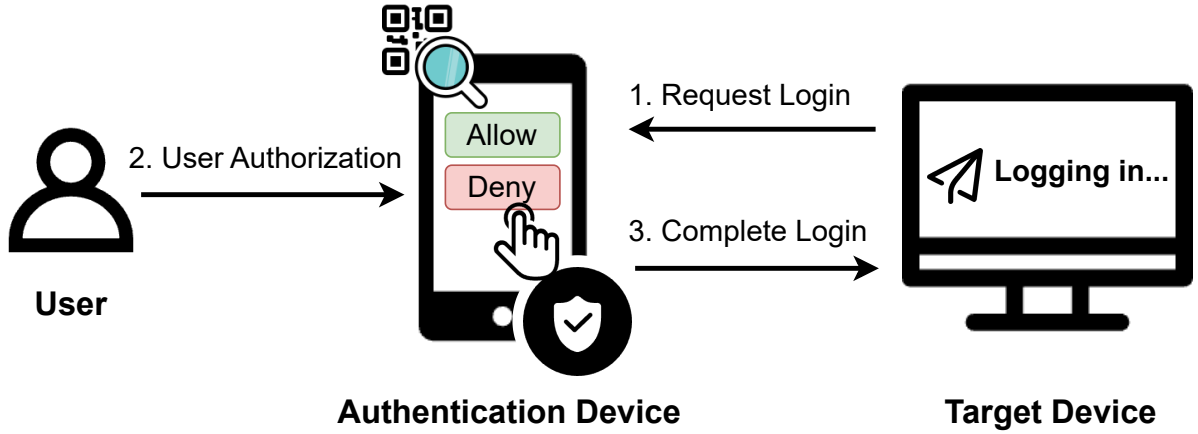
Xin Zhang, Xiaohan Zhang, Huijun Zhou, Bo Zhao

Fudan University

The Rise of Cross-Device Authentication (*XDAuth*)

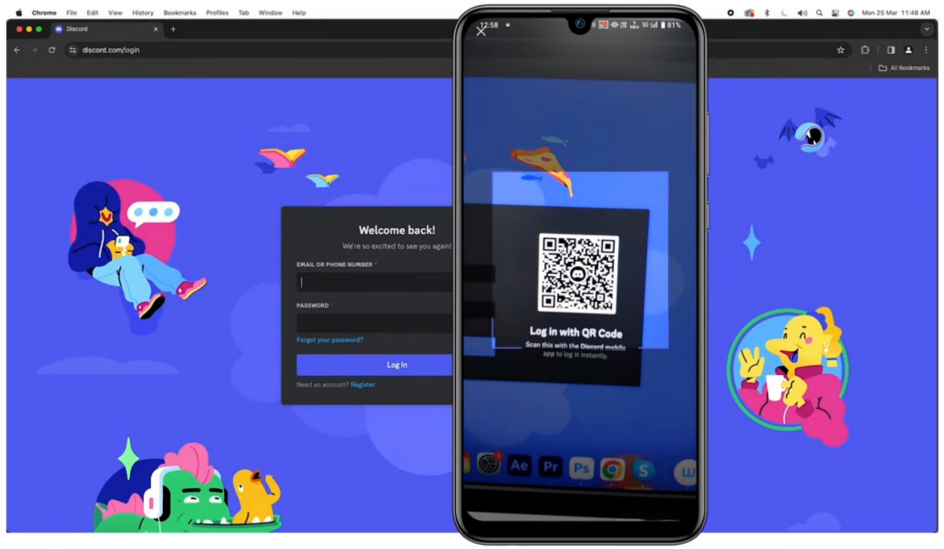
- **The Paradigm Shift**
  - Users now interact with services across **multiple devices**
  - ***XDAuth*** has become an essential mechanism for seamless, cross-platform account access

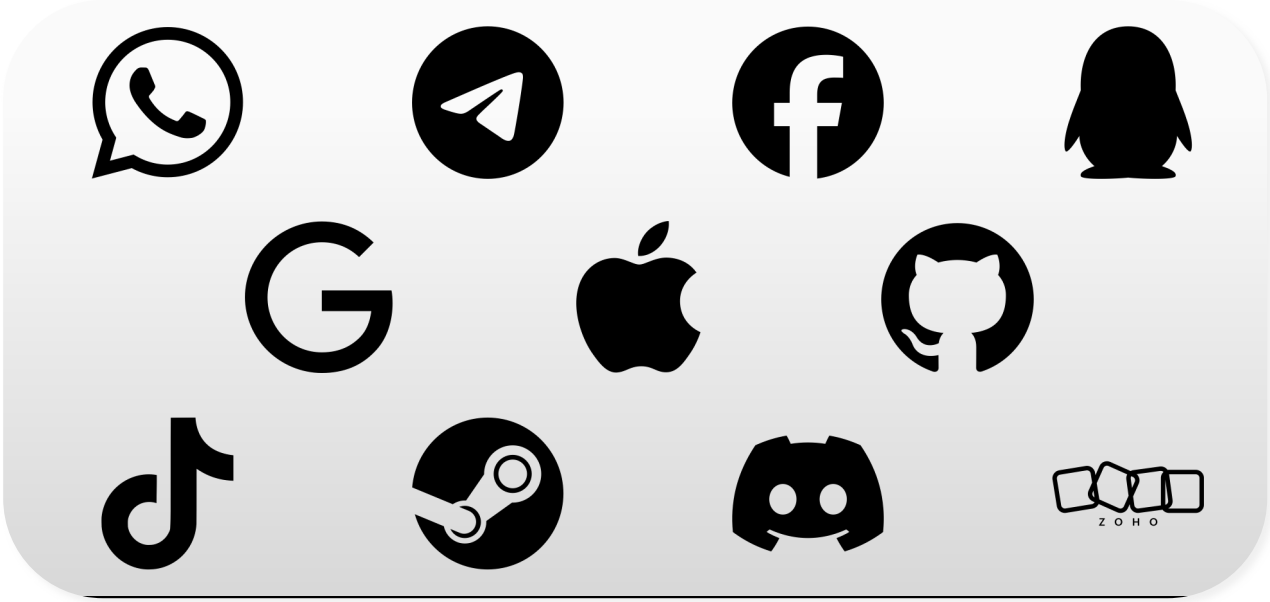
- **What is *XDAuth***
  - Initiate login on a **Target Device** and authorize it on a trusted **Authentication Device**



XDAuth in the Wild

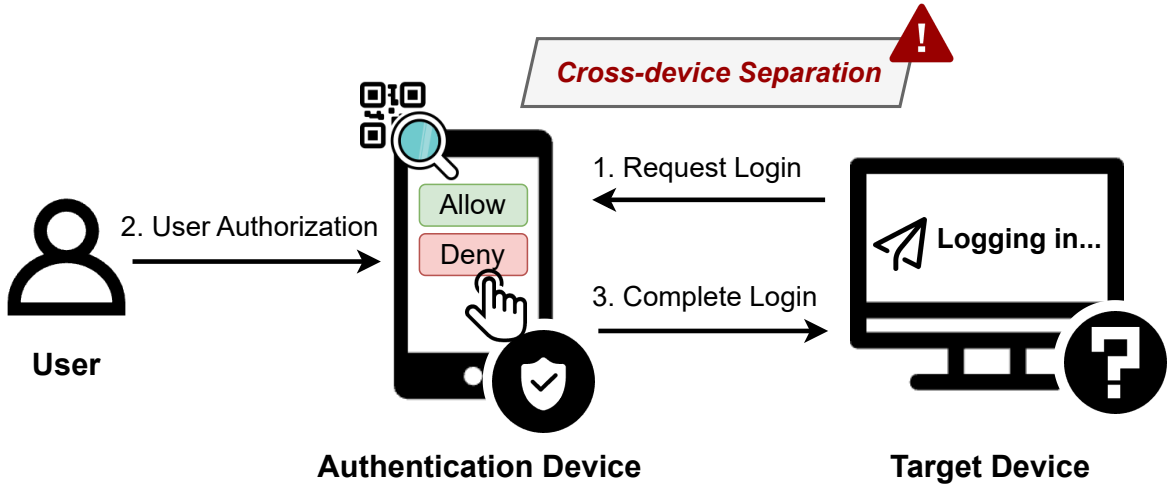
- **Popular Schemes**
  - QR Code-based, Push-based, WebAuthn
- **Key Advantages**
  - Frictionless UX, Passwordless …





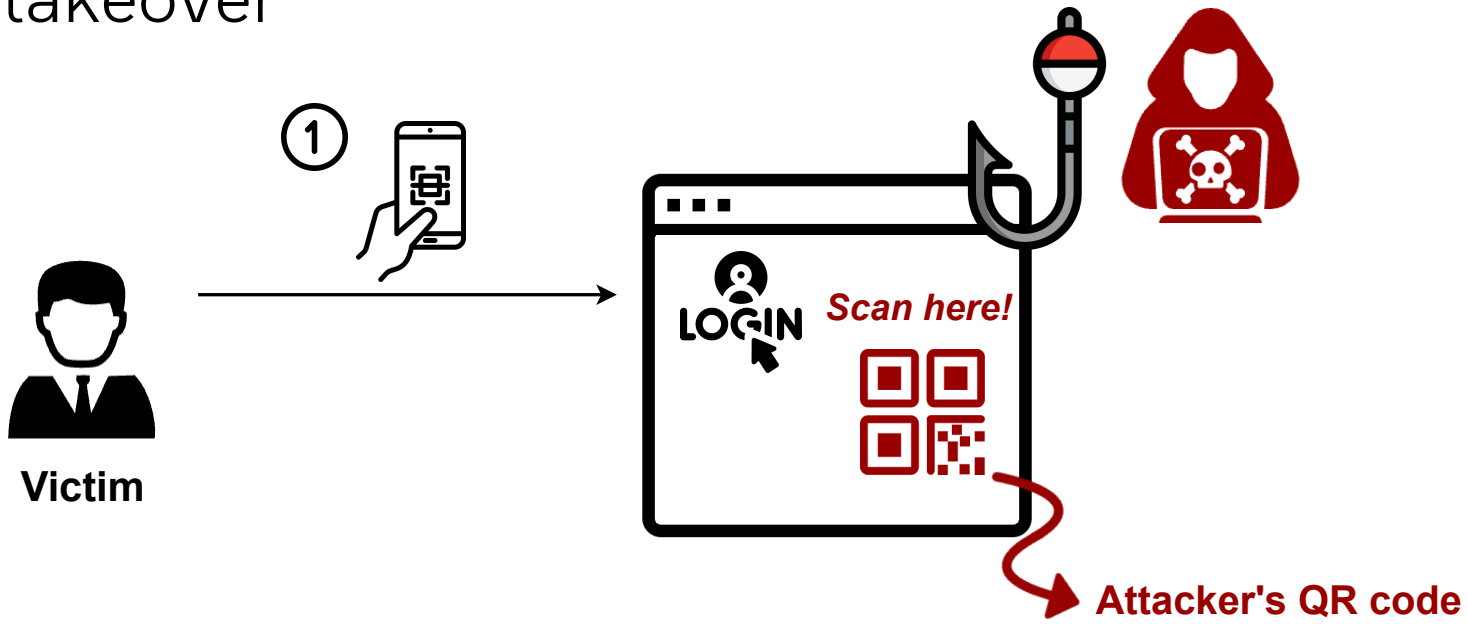
The Security-Usability Gap

- **Contextual Separation**
  - Devices no longer share situational cues
- **Information Asymmetry**
  - Users approve requests without seeing the target device's environment
- **Potential Risks**
  - Inadvertent approvals of malicious logins



Exploiting the Gap: QRLJacking[1]

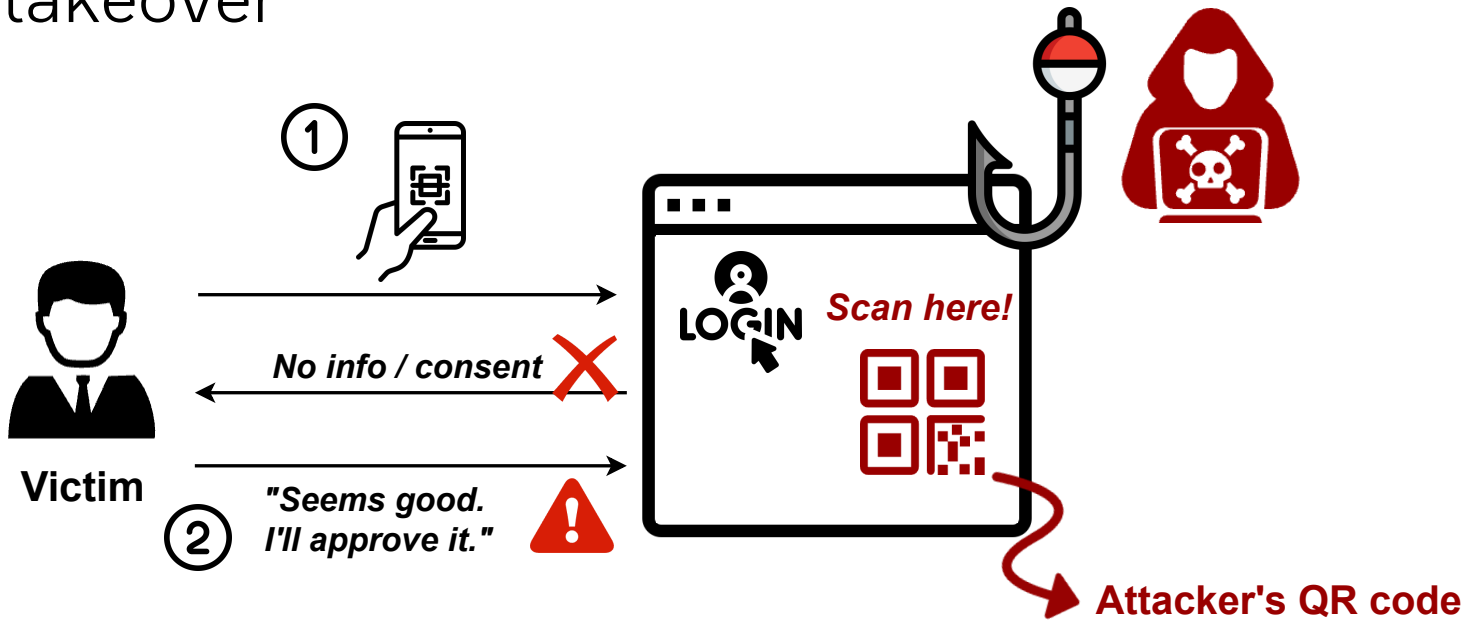
- **Attack Process**
  - Attackers trick users into scanning malicious QR codes
- **Problem**
  - Lack of target device details leads to blind approval, resulting in account takeover



[1] “Qrljacking, an attack introduced on owasp.” https://owasp.org/ www-community/attacks/Qrljacking, 2024.

Exploiting the Gap: QRLJacking[1]

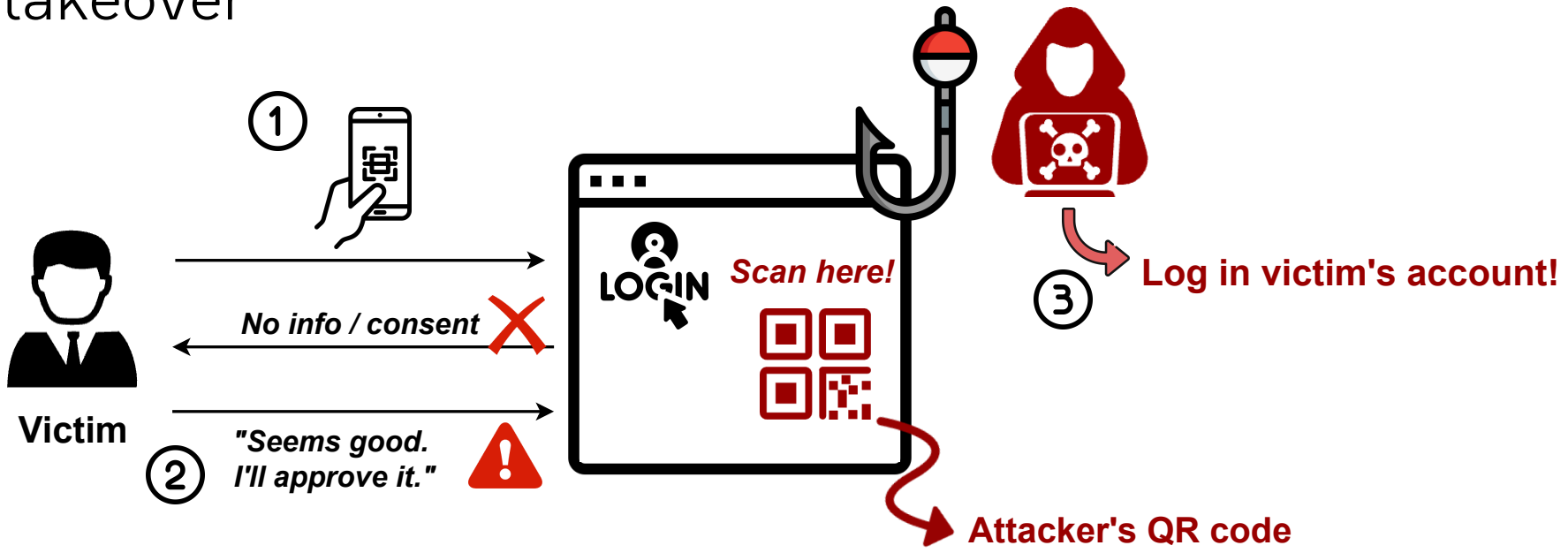
- **Attack Process**
  - Attackers trick users into scanning malicious QR codes
- **Problem**
  - Lack of target device details leads to blind approval, resulting in account takeover



[1] "Qrljacking, an attack introduced on owasp." https://owasp.org/ www-community/attacks/Qrljacking, 2024.

Exploiting the Gap: QRLJacking[1]

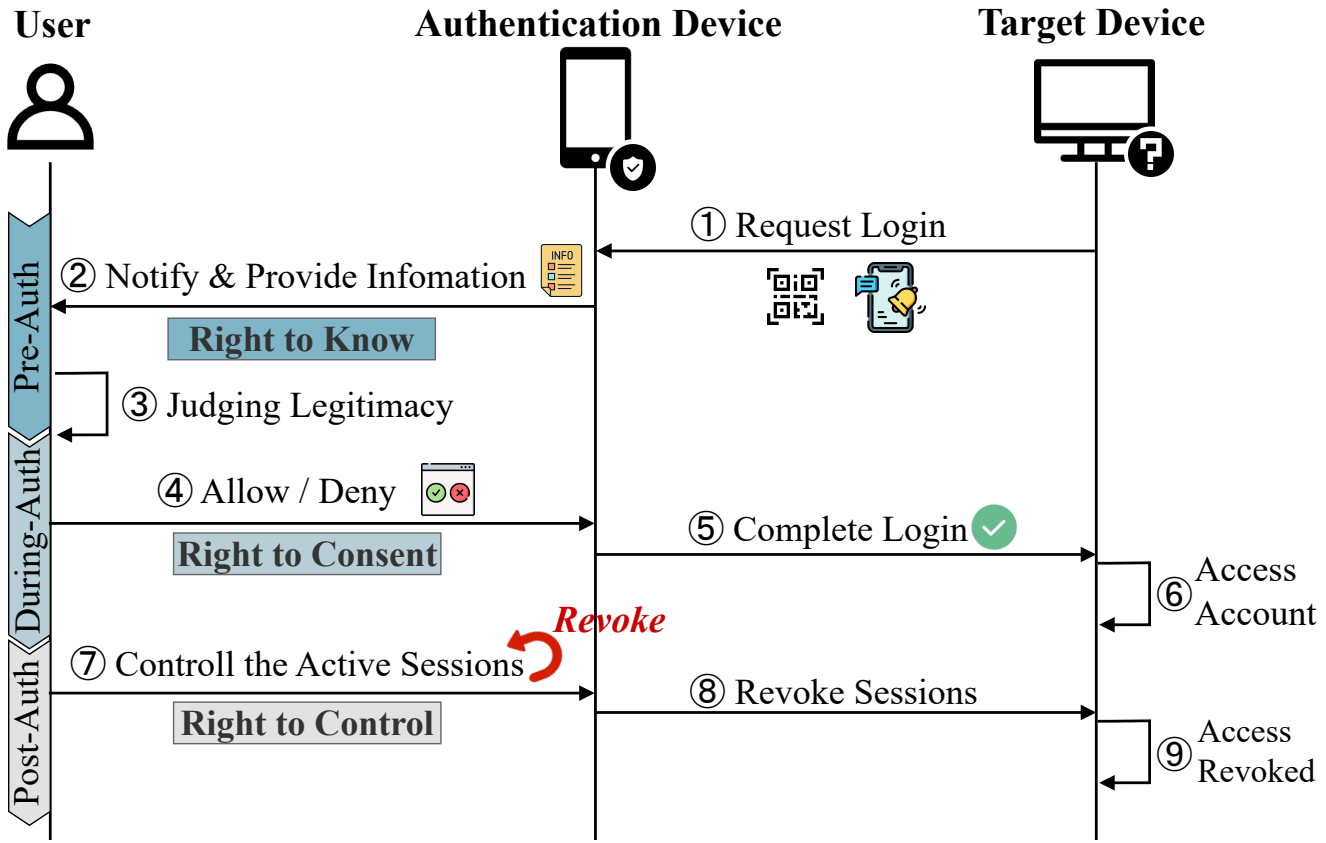
- **Attack Process**
  - Attackers trick users into scanning malicious QR codes
- **Problem**
  - Lack of target device details leads to blind approval, resulting in account takeover



[1] "Qrljacking, an attack introduced on owasp." https://owasp.org/ www-community/attacks/Qrljacking, 2024.

Restoring Contextual Integrity

- **Propose "Three User Rights" across the Workflow**
  - Adapting privacy principles to *XDAuth* security



A User-Centric Framework: Three Rights

- **Methodology of Deriving the Framework**
  - **Dataset**: 27 major services across 10 diverse categories
  - **Workflow Documentation**: Systematic recording of *XDAuth* workflow, including screenshots and detailed field notes
  - **Metric Identification**: Grounded Theory
    - **Open Coding**: Extracting conceptual labels from workflows
    - **Axial Coding**: Grouping concepts into generalizable categories

The *XDAuth* Evaluation Framework

Stage	Right	Category	Metrics
Pre-Auth	**Know**	Authorization activity	Purpose
			Time
			Capabilities & data
		Target device environment	Device info
			Location & network
			Device risks
During-Auth	**Consent**	Explicit authorization	Explicit consent & rejection
		Duration	Agreement on duration
Post-Auth	**Control**	Notification	Login notification
		Authorization review	Ease of finding
			Session details
		Authorization revocation	Revocable session

Evaluating Real-World Services

- **Overall Results**
  - **None** of the 27 evaluated services fully safeguard all three rights

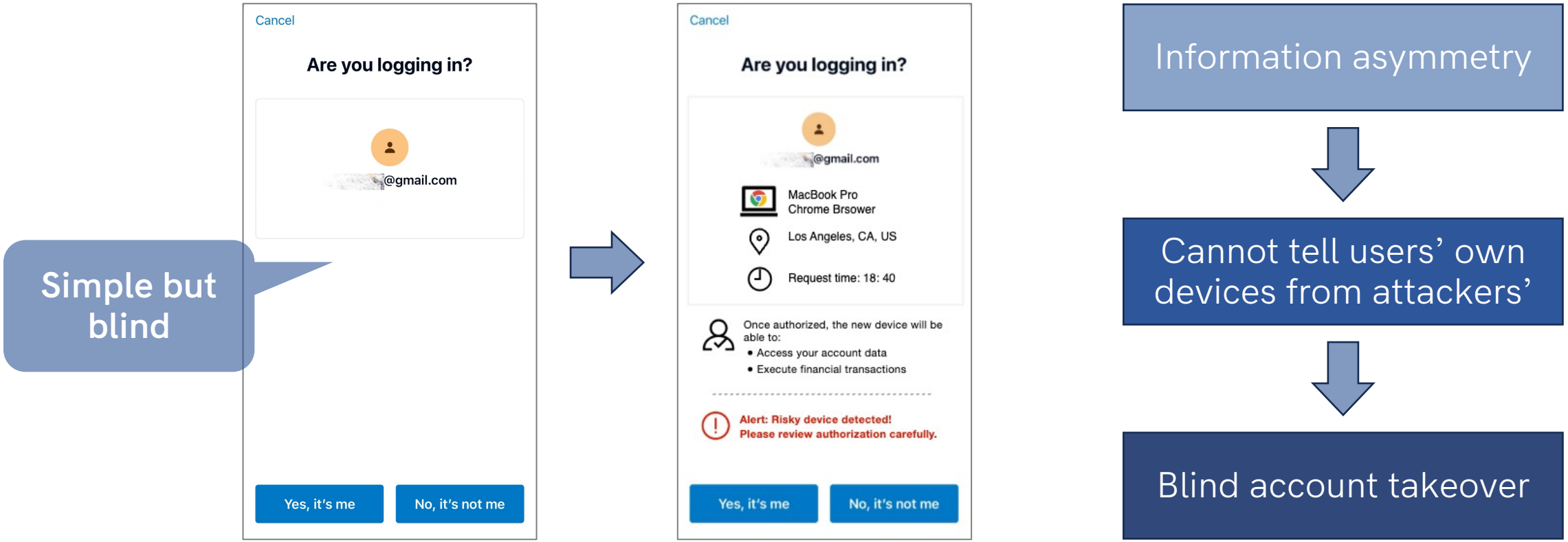
Mechanisms	Service	Category	Right to Know: Authorization Activity Info[1] (*Pur,Tm,Capability*)	Right to Know: Device and Environment Info[2] (*Dev,Loc,Risk*)	Right to Consent: Explicit Authorization	Right to Consent: Agreement on Durations	Right to Consent: Notification	Right to Control: Authorization Review[3] (*Pth/Tm,Mtd,Dev,Loc*)	Right to Control: Authorization Revocation
QR Code-based Authentication	WhatsApp	Chat (IM)/SMS	● ⊠[‡] ●	○ ○ ○	⊠	○	○	2 / ● ○ ◐ ○	●
	Telegram	Chat (IM)/SMS	○ ⊠ ○	○ ○ ○	⊠	◐	◐	3 / ● ○ ● ●	●
	TikTok	Audio/Video Clips	● ⊠ ●	○ ○ ○	◐	◐	○	5 / ● ● ● ○	●
	Steam	Games	● ⊠ ○	○ ● ○	●	●	◐	3 / ● ● ◐ ●	●
	Yandex	Search Engines/Portals	● ⊠ ○	◐ ● ○	◐	◐	○	x[‡] / ○ ○ ○ ○	○
	Uber	Travel	● ⊠ ○	◐ ● ○	●	◐	◐	x / ○ ○ ○ ○	○
	QQ	Chat (IM)/SMS	● ⊠ ○	○ ● ●	●	◐	◐	4 / ● ○ ● ●	●
	Mail App	Search Engines/Portals	● ⊠ ○	○ ○ ○	●	◐	◐	3 / ● ○ ◐ ●	●
	Roblox	Games	● ⊠ ●	○ ● ○	●	◐	◐	3 / ● ○ ◐ ●	●
	Discord	Chat (IM)/SMS	● ⊠ ○	○ ○ ○	●	◐	◐	3 / ● ○ ◐ ●	●
	Taobao	Shopping	● ⊠ ○	○ ○ ○	●	○	○	4 / ● ● ● ●	●
	Baidu	Search Engines/Portals	● ⊠ ○	○ ○ ○	●	◐	○	5 / ● ● ◐ ●	●
	VK	Social Networking	● ⊠ ○	◐ ● ○	●	◐	●	4 / ● ○ ● ●	●
	Ivi	Entertainment	○ ⊠ ○	○ ○ ○	○	◐	◐	2 / ○ ○ ● ○	●
	Weibo	Social Networking	● ⊠ ○	○ ○ ○	●	◐	○	4 / ● ○ ● ●	●
Push-based Authentication	Facebook	Social Networking	● ● ○	◐ ● ○	●	◐	●	6 / ● ○ ● ●	●
	Microsoft	Technology/Internet	● ○ ○	◐ ● ○	●	○	◐	2 / ● ○ ◐ ●	◐
	Steam	Games	● ○ ○	○ ● ○	●	●	◐	3 / ● ● ◐ ●	●
	GitHub	Technology/Internet	● ○ ○	○ ○ ○	●	◐	◐	x / ○ ○ ○ ○	○
	Keeper	Technology/Internet	● ● ○	○ ◐ ○	●	◐	◐	3 / ● ○ ○ ●	○
	Google Prompt	Search Engines/Portals	● ● ○	◐ ● ○	●	○	●	4 / ● ○ ● ●	●
	Zoho OneAuth	Business/Economy	● ○ ○	○ ○ ○	●	◐	●	1 / ● ○ ● ●	●
	Xero Verify	Business/Economy	● ○ ○	○ ○ ○	●	○	○	x / ○ ○ ○ ○	○
	Wise	Business/Economy	● ○ ○	◐ ● ○	●	◐	○	x / ○ ○ ○ ○	●
	Snapchat	Chat (IM)/SMS	● ● ○	◐ ● ○	●	◐	◐	3 / ● ○ ◐ ●	●
WebAuthn	Apple	Technology/Internet	● ⊠ ○	○ ○ ○	◐	◐	○	2 / ○ ○ ○ ○	○
	Google	Search Engines/Portals	● ⊠ ○	○ ○ ○	●	●	○	4 / ● ○ ● ●	●

- **Rights Performance**
  - Consent is most widely supported
  - Know and Control are often missing

- Significant **inconsistency** across industry leaders

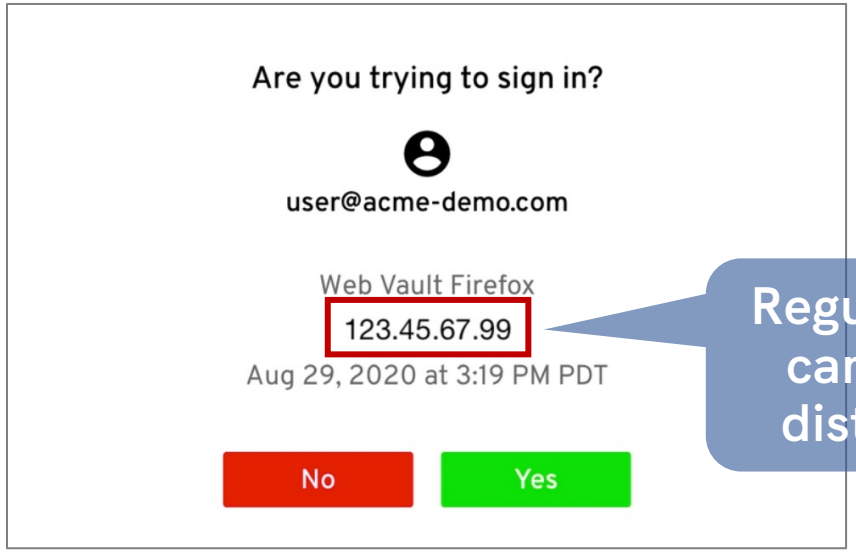
Findings – The Right to Know

- **Blind Approvals**
  - **52% (14/27)** of services provide **zero** target device/environment info

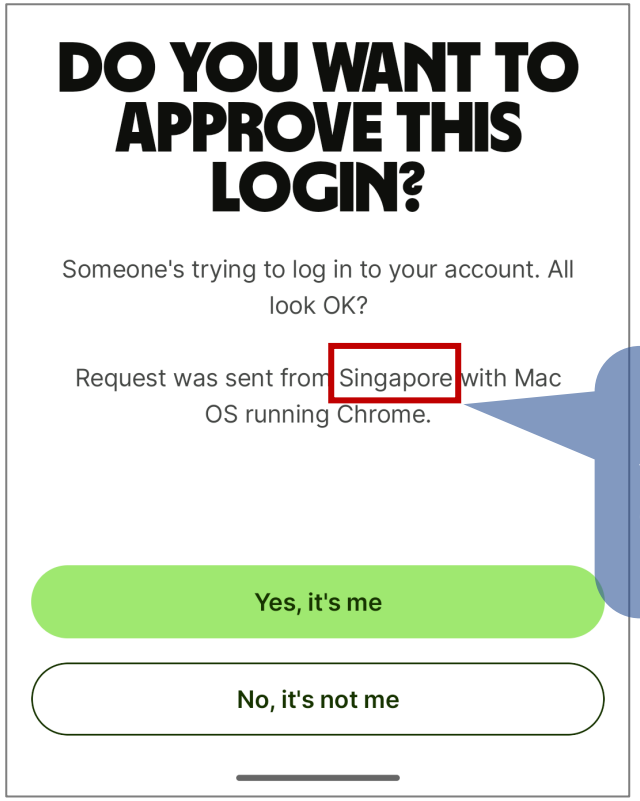


Findings – The Right to Know

- **Poor Info Quality**
  - **Unintuitive Formats**: Displaying raw IP addresses (e.g., Keeper)
  - **Coarse Grain**: Only providing country-level geolocations (e.g., Wise)



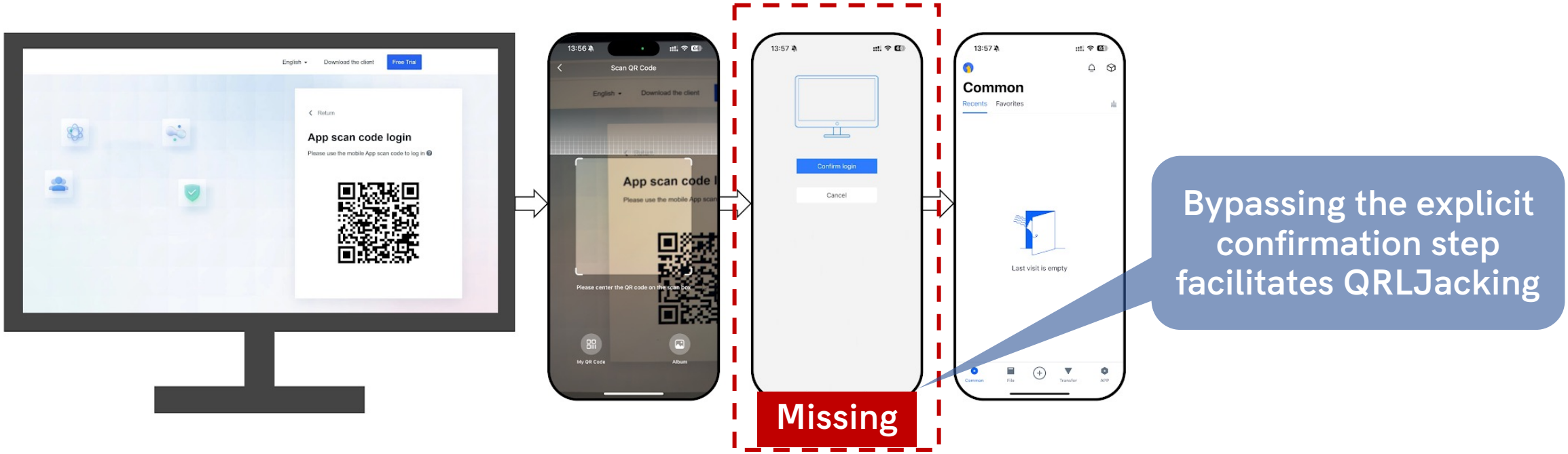
Regular users can hardly distinguish



Fails to flag suspicious local or intra-country logins

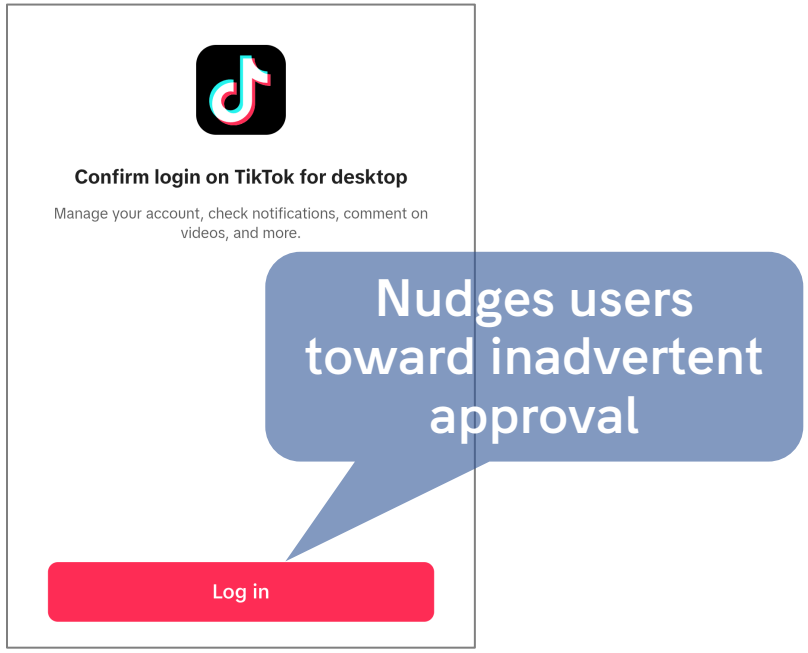
Findings – The Right to Consent

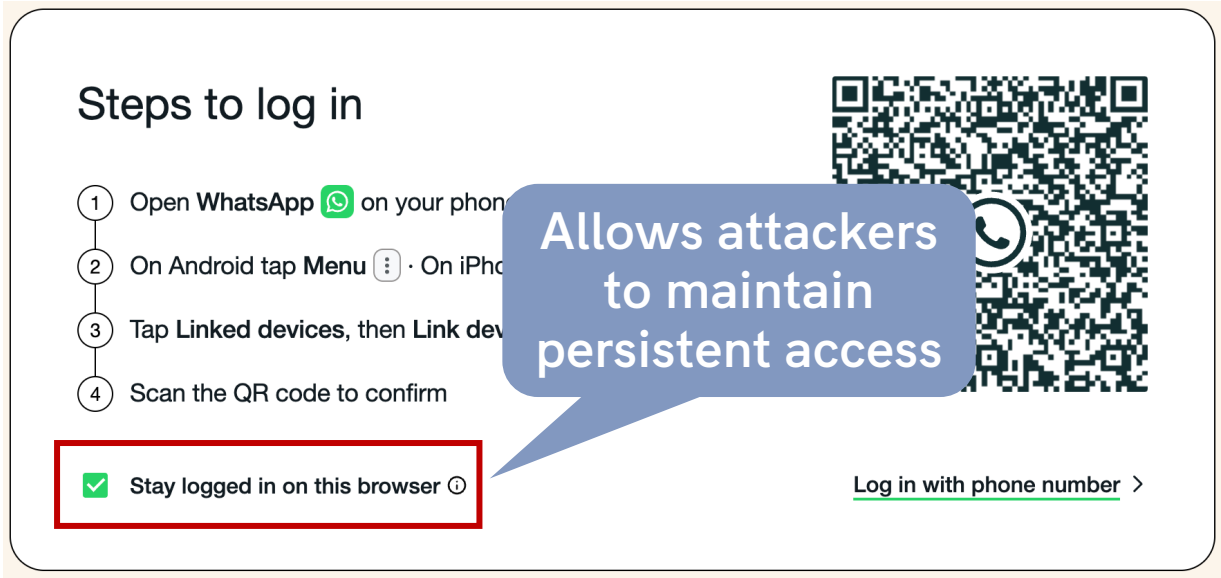
- **Implicit Consent**
  - Access granted immediately after scanning code (e.g., Ivi)



Findings – The Right to Consent

- **Missing Rejection**
  - 4 services lack a "Deny" button; others hide it with low-contrast colors
- **Delegated Control**
  - Session duration is decided by Target Device (potentially attacker-controlled)





Findings – The Right to Control

- **Post-Auth Control Gap**

Failed Awareness

Silent Logins: 10/27 services send No notification
Ephemeral Alerts: 13/17 rely on temporary alerts like Toast, easily missed

Hidden Management

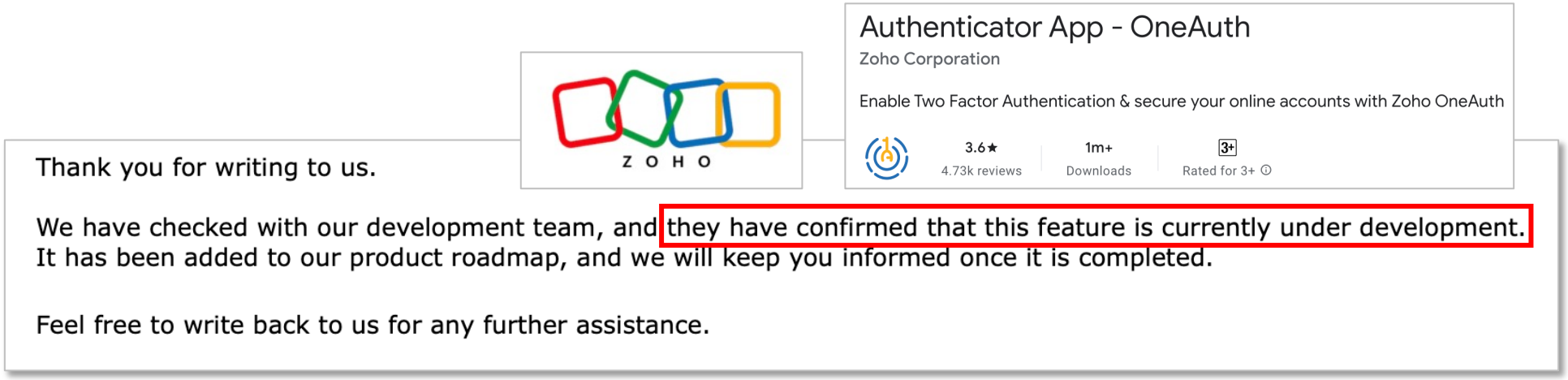
No Review: 5 services **lack** any Session Review function
Hard to Find: Functions buried deep in settings (e.g., 6 layers deep in Facebook)

Broken Revocation

No Revocation: 6 services provide **No** way to terminate sessions
Flawed Revocation: Real-time chat access persists after revocation in a top video app

Vendor Feedback

- **Reporting**
  - All findings were disclosed to affected service providers
- **Positive Feedback**
  - Zoho OneAuth: Formally acknowledged our findings
  - Confirmed the suggested features are added to their product roadmap and under development



User Perceptions

- **Study Design**
  - **Main Survey** (*N* = 100): Online questionnaire via Prolific (U.S.)
  - **Interactive Validation** (*N* = 10): A functional *XDAuth* prototype

Right to Know
Design with device/activity info
Risk Difference: +82% [83.8%, 95.2%]
91%

Right to Know
Design with explicit approval
Risk Difference: +46% [63.6%, 80.7%]
73%

Right to Know
Design with session management
Risk Difference: +70% [76.7%, 90.7%]
85%

✓ **Security & Usability Impact**

98%
believe these rights enhance XDAuth **security**

95%
find **usability** acceptable or better

Design Recommendations

- **Suggestions for Developers** 

For Awareness: Clarity without Overload

- **Progressive Disclosure:** Surface key cues (e.g., device, location) first
- **Adaptive Highlighting:** Flag anomalous attributes (e.g., unfamiliar city)

For Consent: Intentionality with Minimal Friction

- **Active Auth:** Avoid implicit "Scan-to-Login"; enforce explicit "Approve/Deny"
- **Scoped Duration:** Choose session length on the **Auth** device

For Control: Revocation with Easy Access

- **Actionable Alerts:** Notifications could link directly to controls
- **Instant Revocation:** Centralized, real-time termination of "Zombie Sessions"

Thanks!

Xin Zhang

Fudan University

zhangx22@m.fudan.edu.cn