Understanding Users' Perceptions of Client-Side Modifications and Anti-Cheat Engines in Social XR

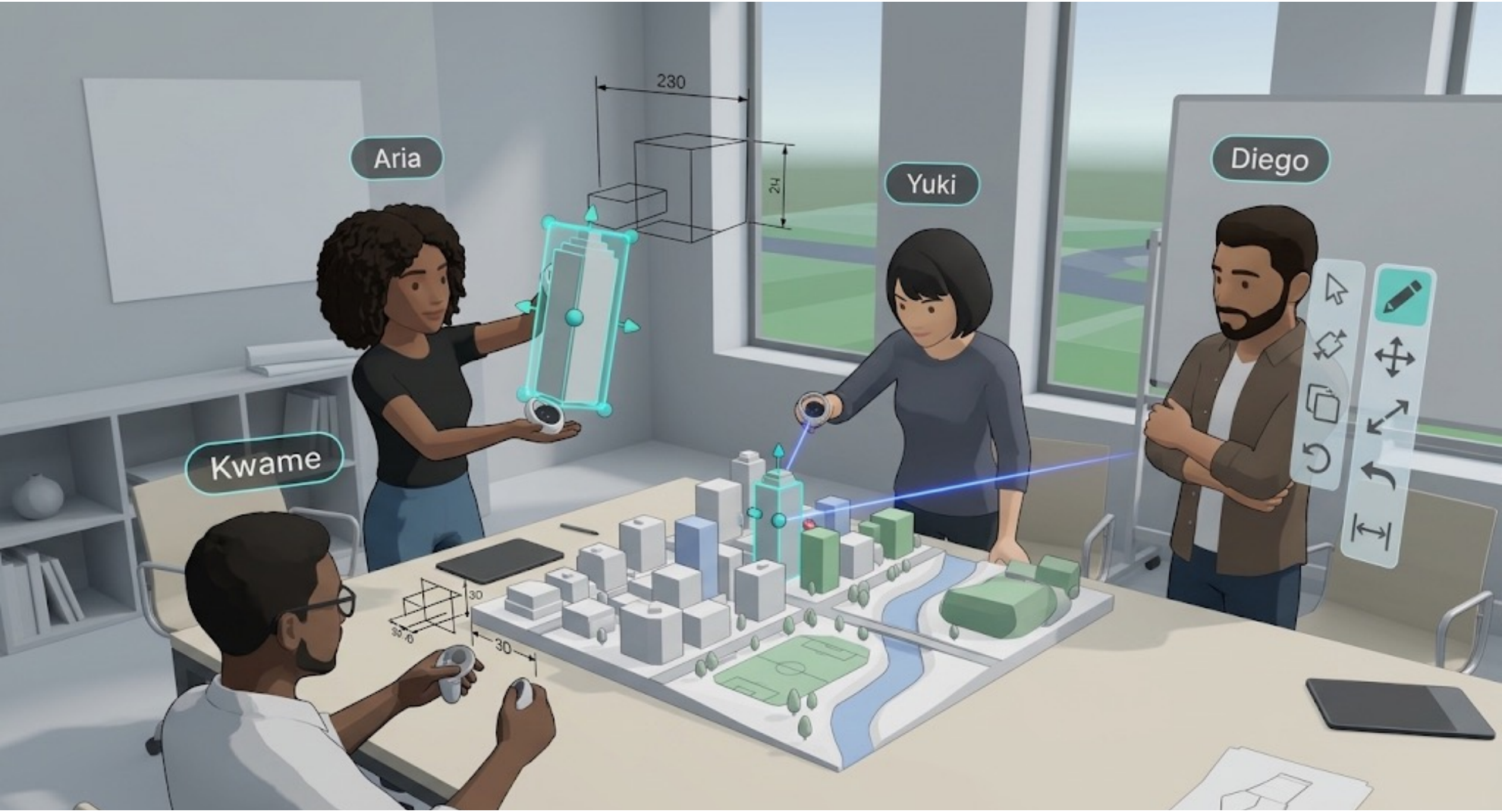
Iman Mohammadi*, **Mutahar Ali***, Habiba Farrukh

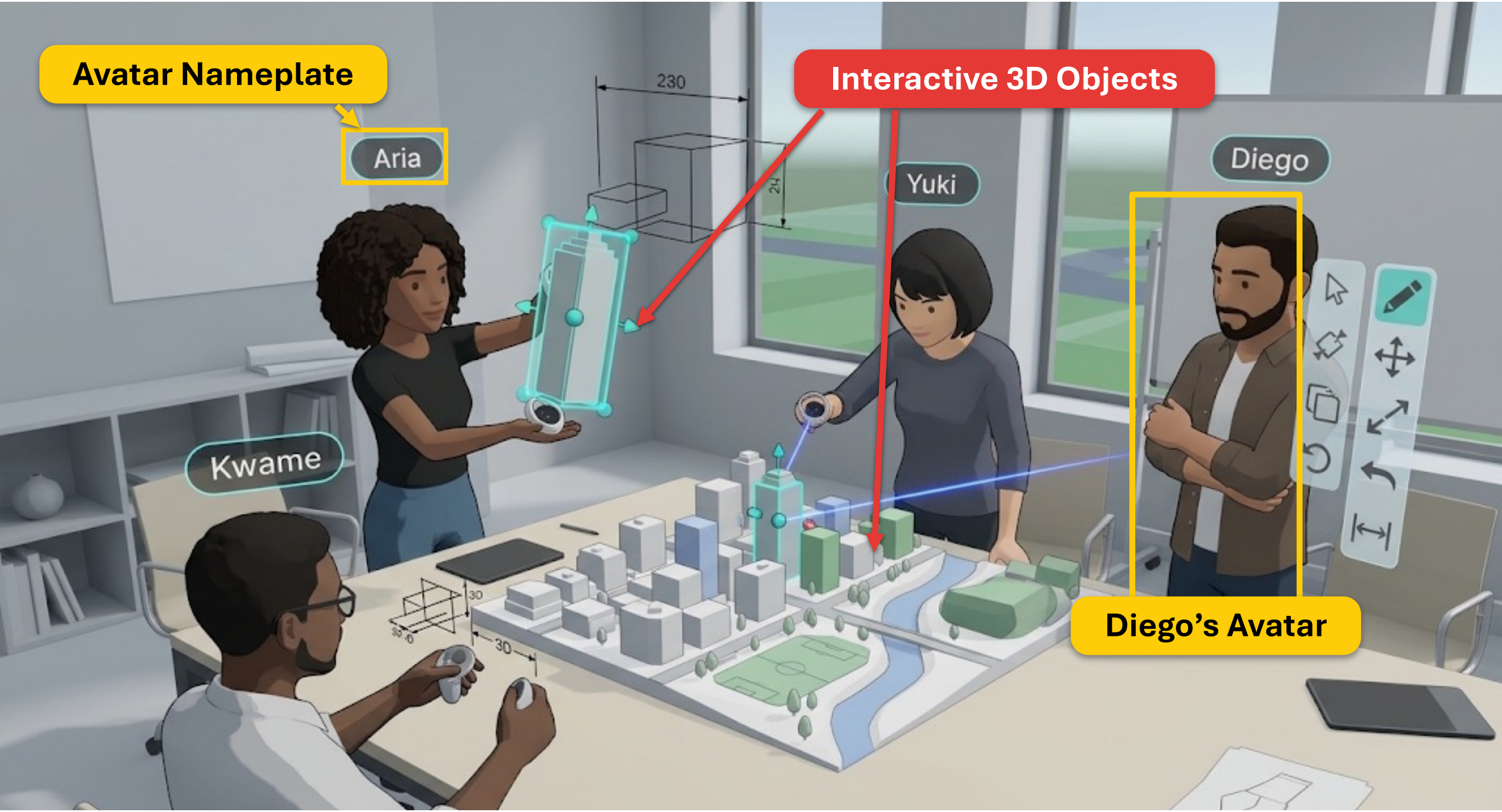
{imohamm1, mutahara, habibaf}@uci.edu

ACM Conference on Computer and Communications Security (CCS) 2026






Aria
Yuki
Diego
Kwame
230
24
30
30


Avatar Nameplate
Aria
Interactive 3D Objects
Yuki
Diego
Kwame
Diego's Avatar
230
24
30
30

Social XR Ecosystem



VR CHAT

REC ROOM

ENGAGE

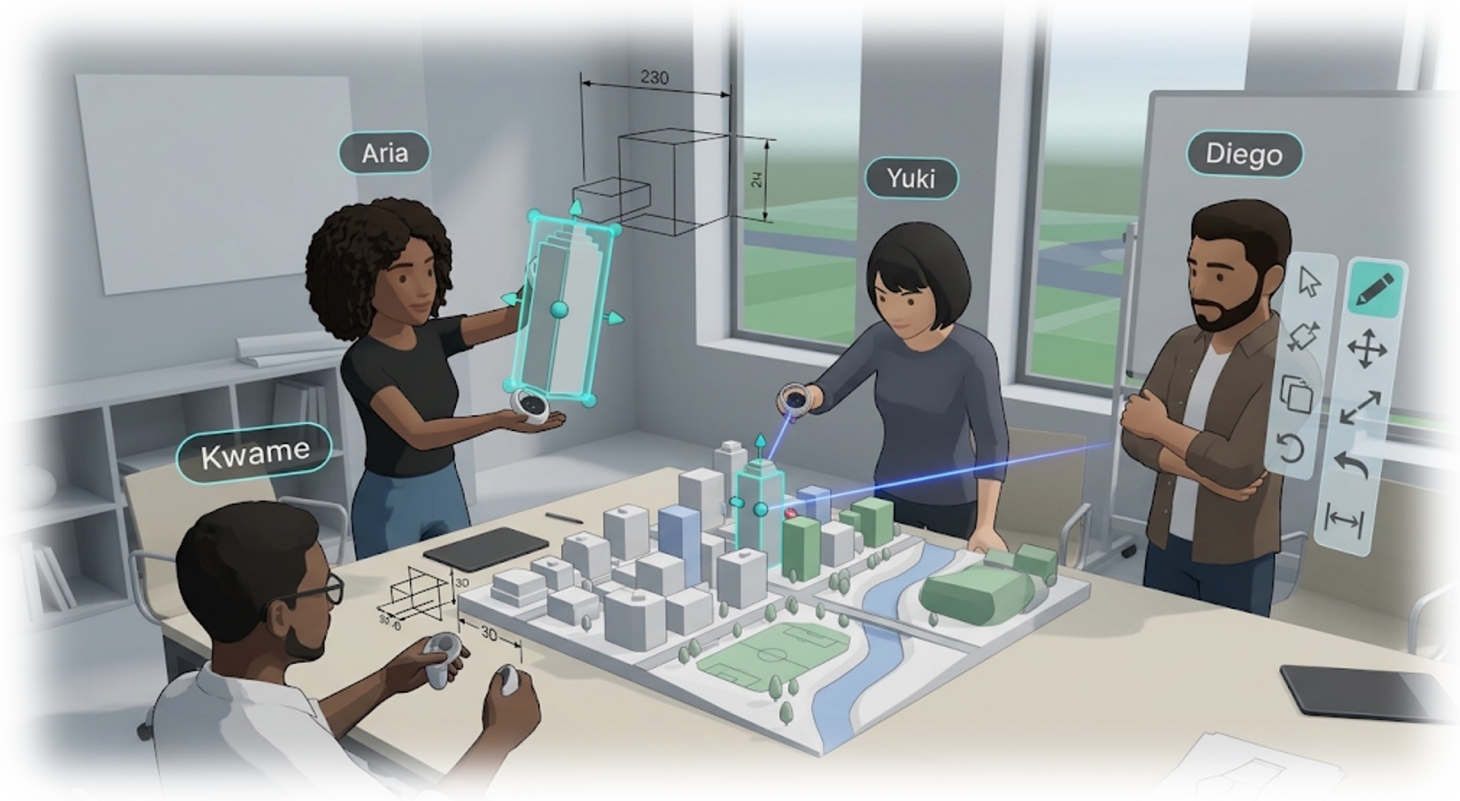
Arkio

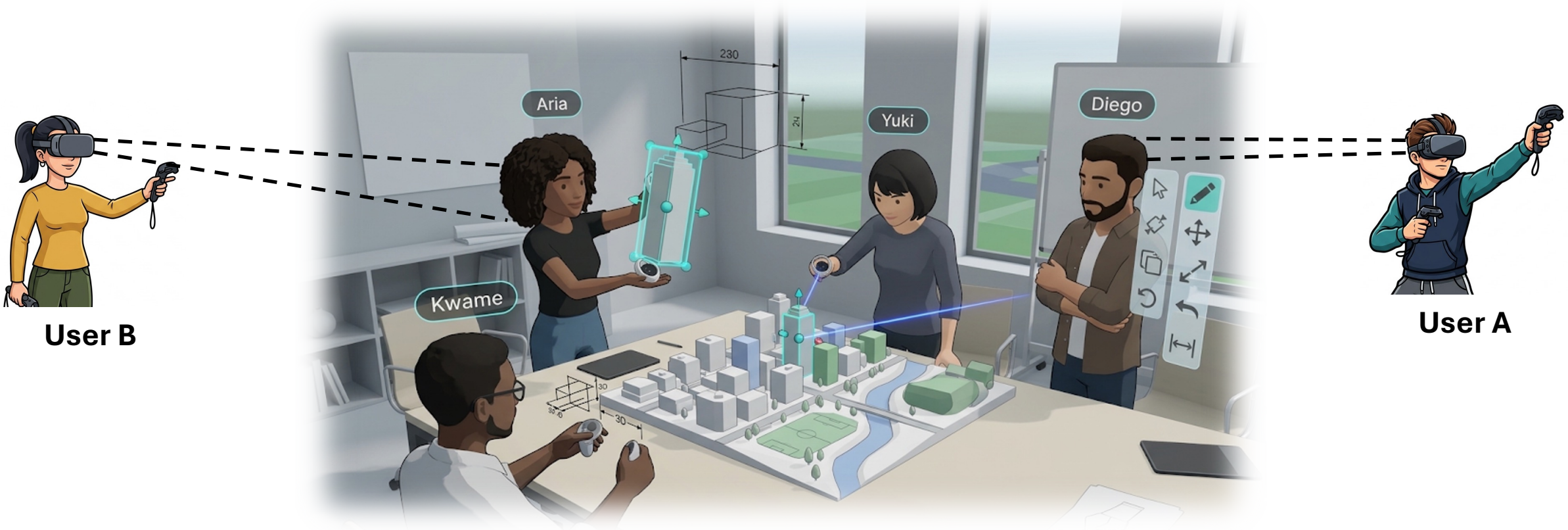
GORILLA TAG

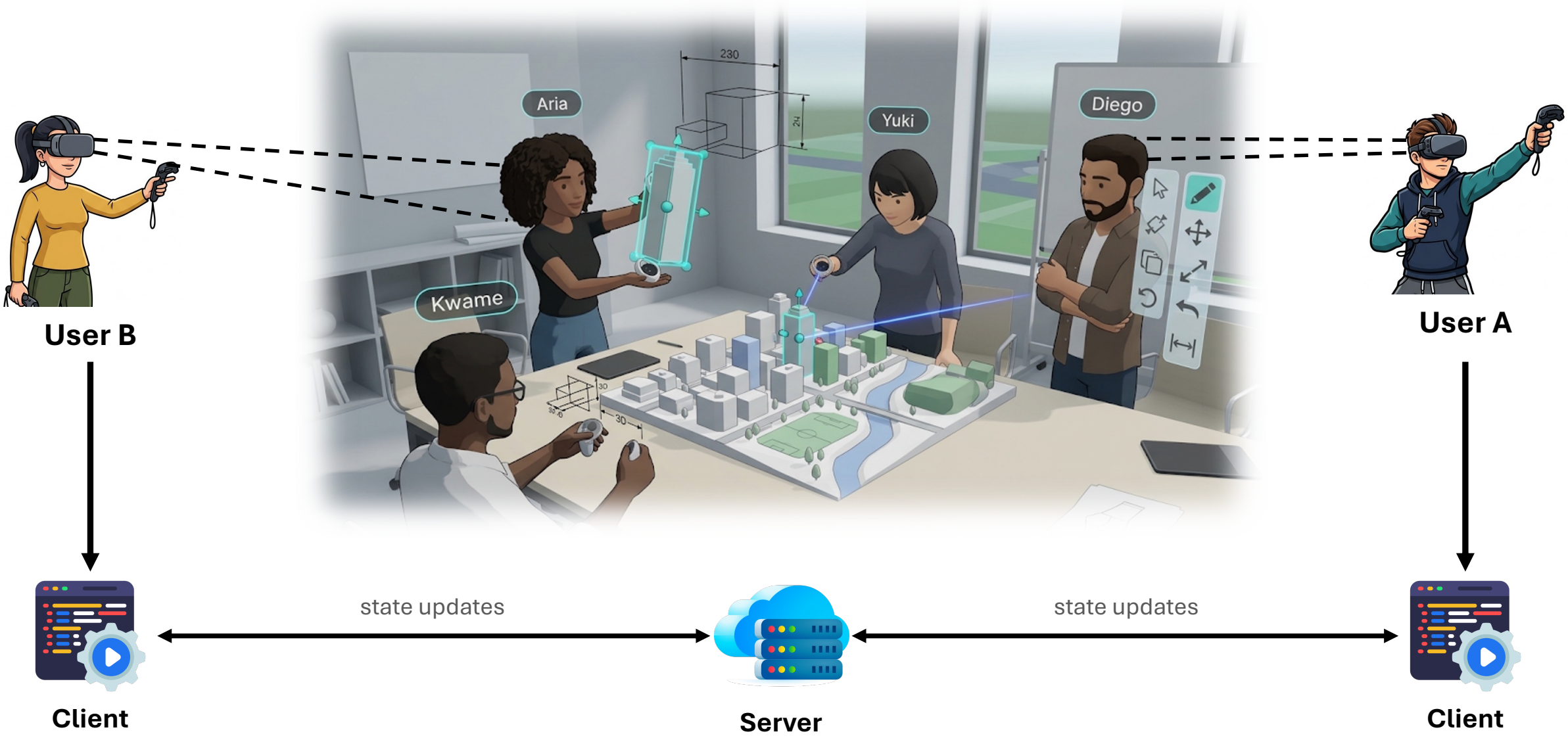
VICTORYXR™

STEAMVR™

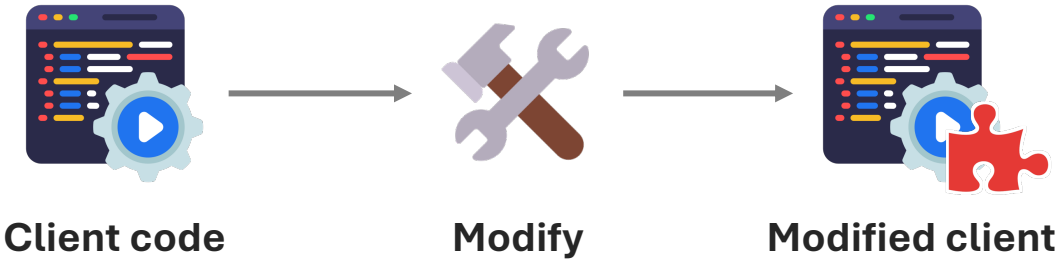
VIVE


Aria
Yuki
Diego
Kwame
230
24
30
30


Aria
Yuki
Diego
Kwame
230
24
30
30
User B
User A

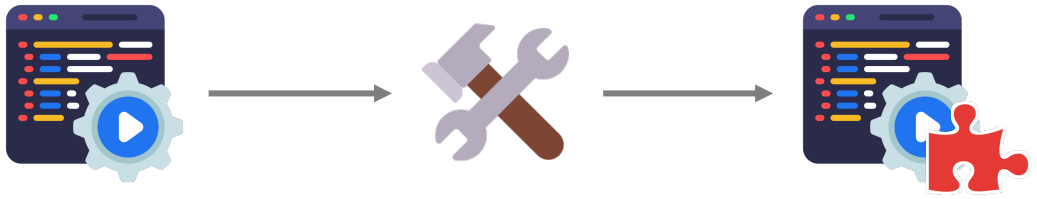

Aria
Yuki
Diego
Kwame
User B
User A
state updates
state updates
Client
Server
Client

Client Modifications



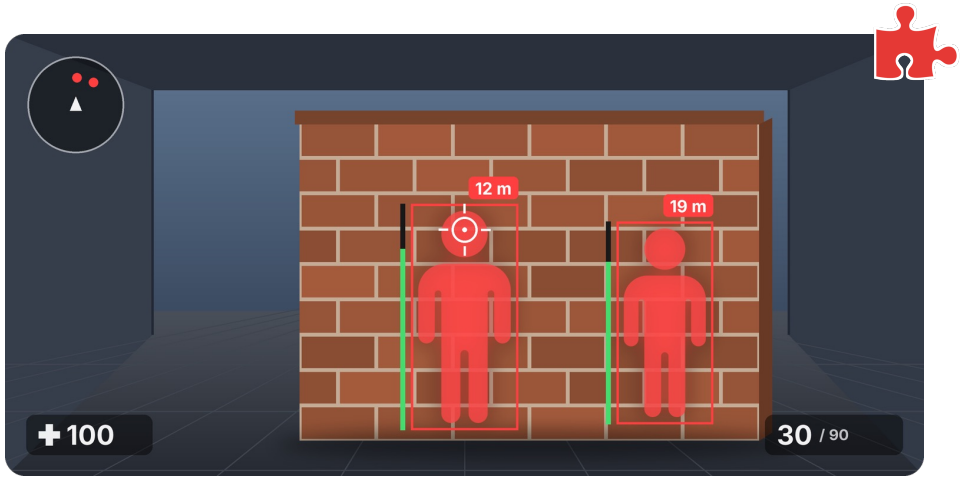
Changes a user makes to the program running on **their own device**

Client Modifications



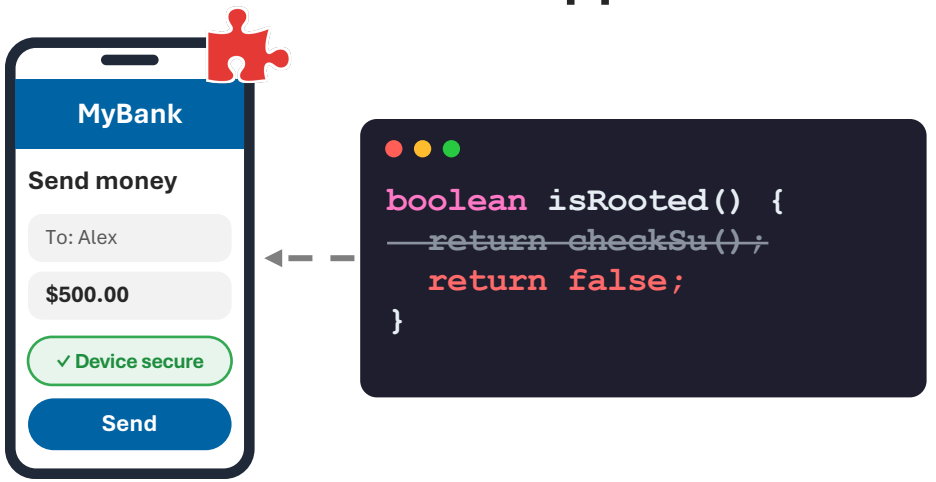
Changes a user makes to the program running on **their own device**

Online Games



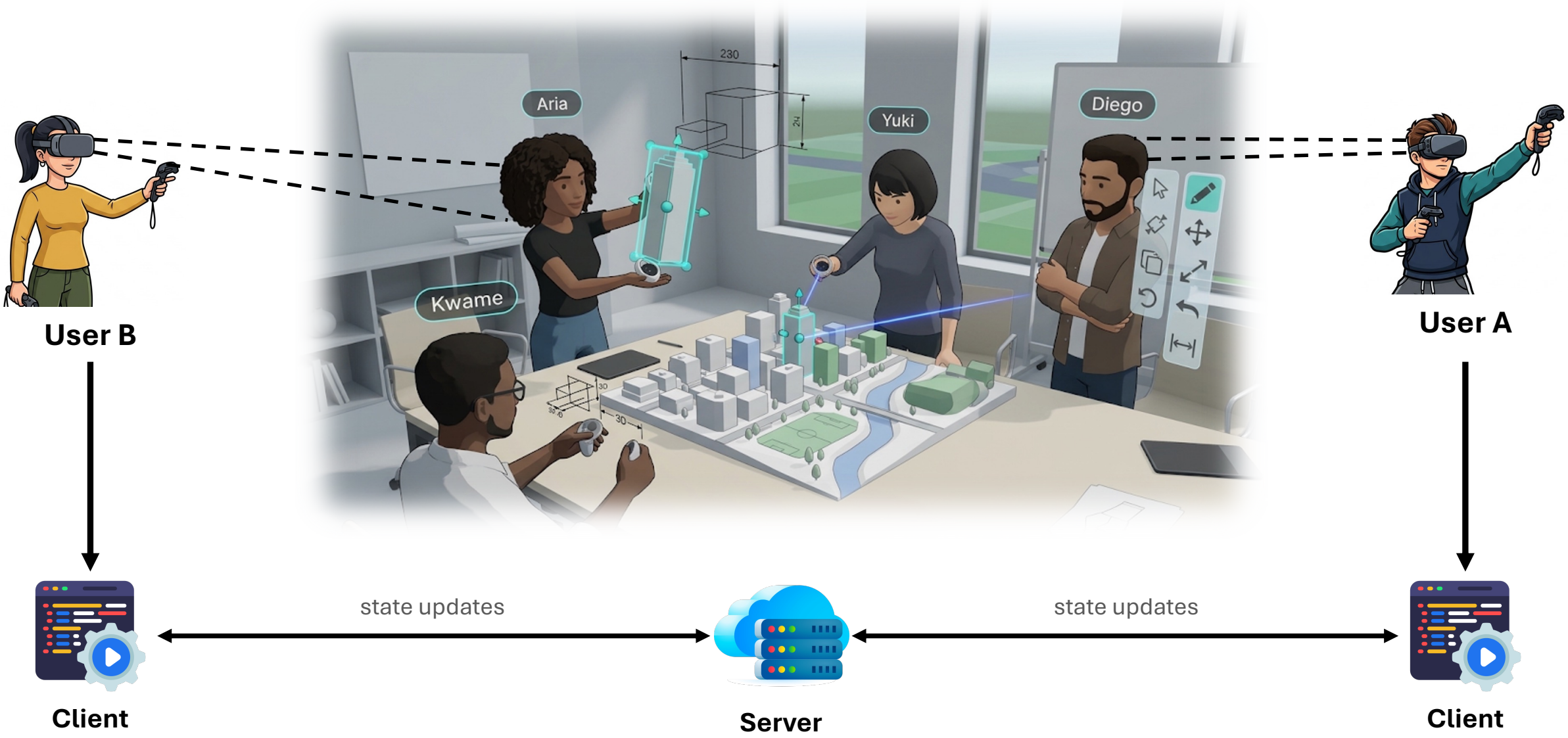
Seeing players through walls

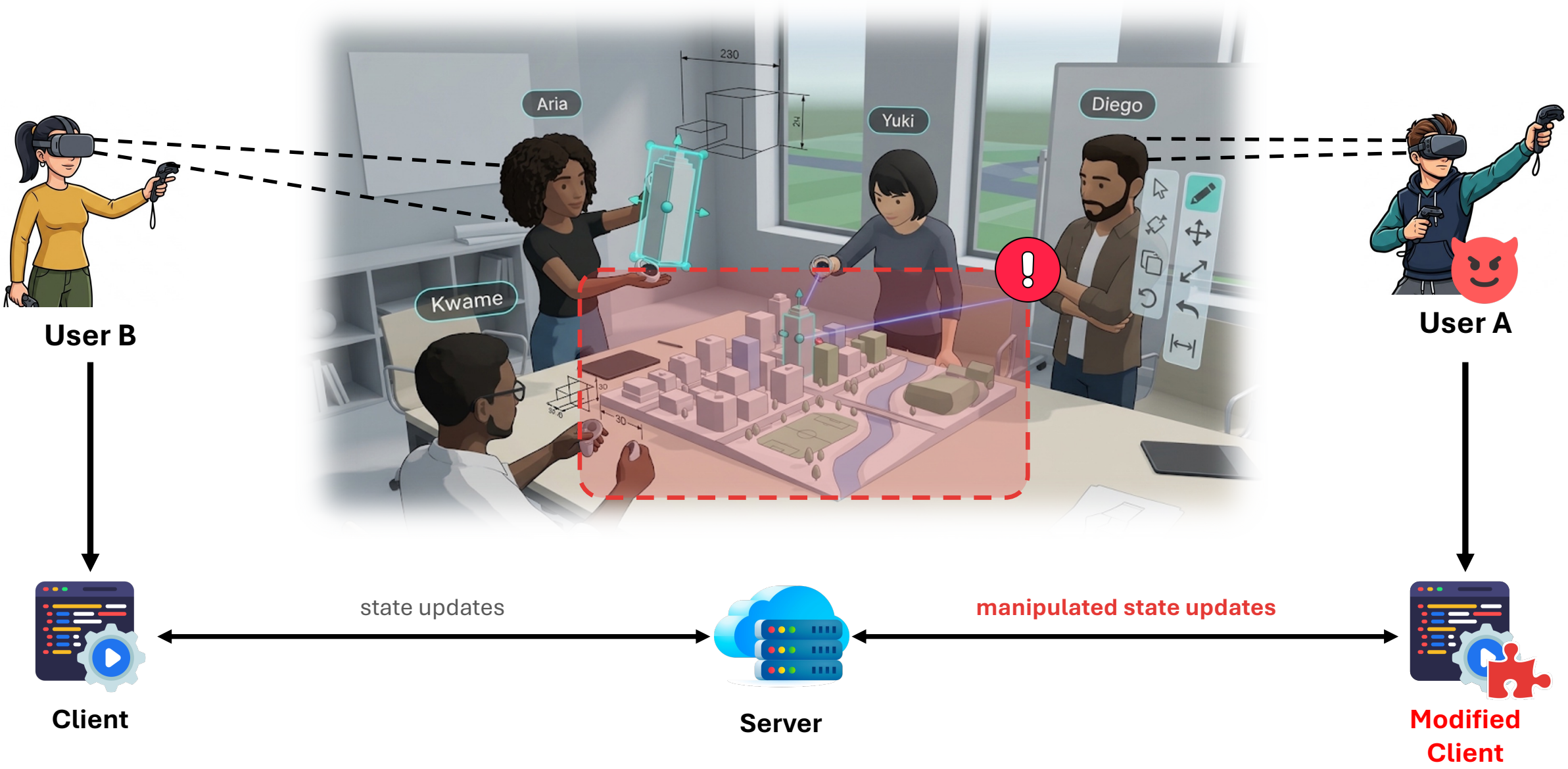
Financial Apps



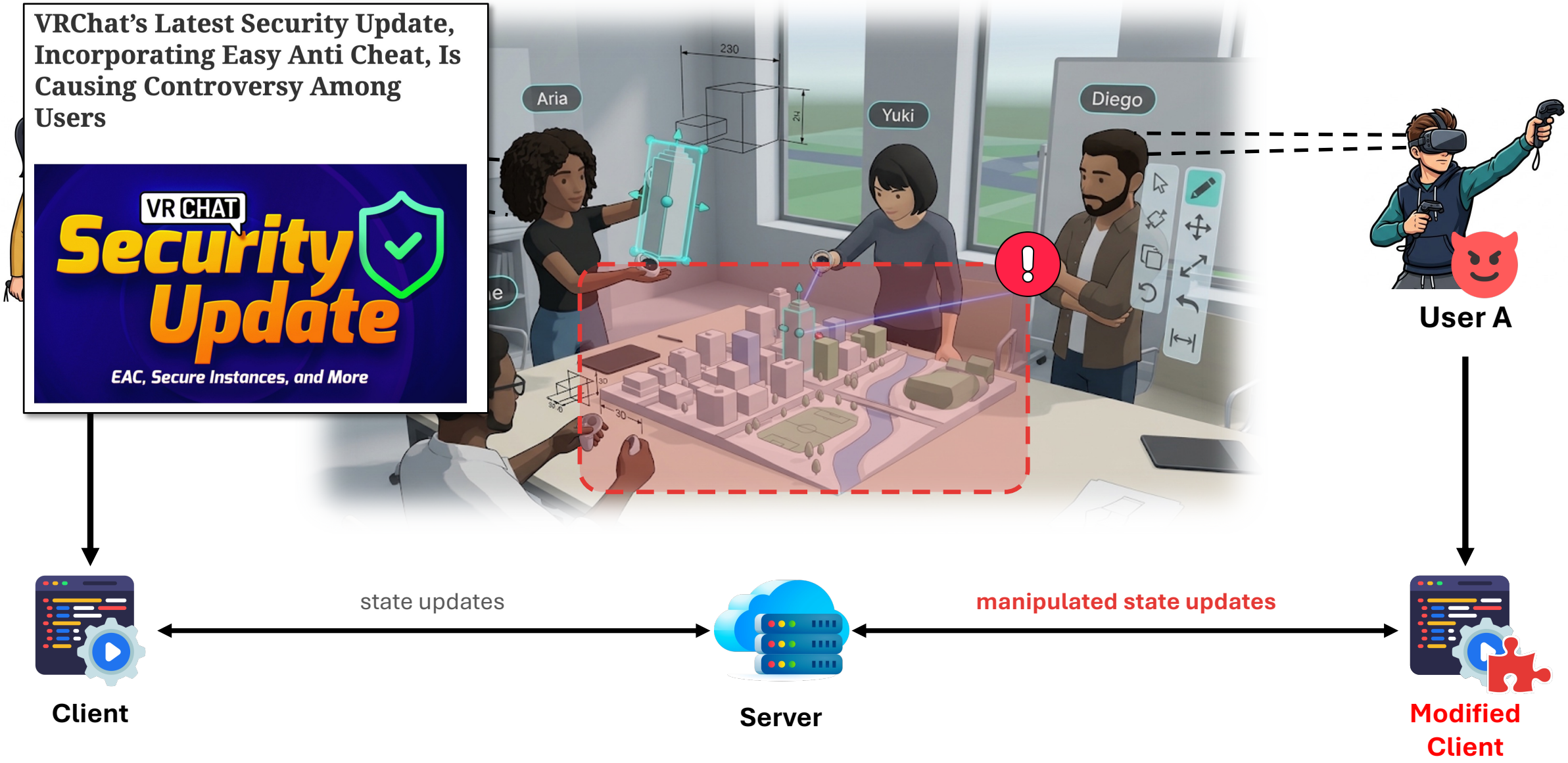
Bypassing the app's security checks

[1] J. Yan and B. Randell. A Systematic Classification of Cheating in Online Games. ACM NetGames 2005.
[2] T. Kim et al. Breaking Ad-hoc Runtime Integrity Protection Mechanisms in Android Financial Apps. ACM AsiaCCS 2017.

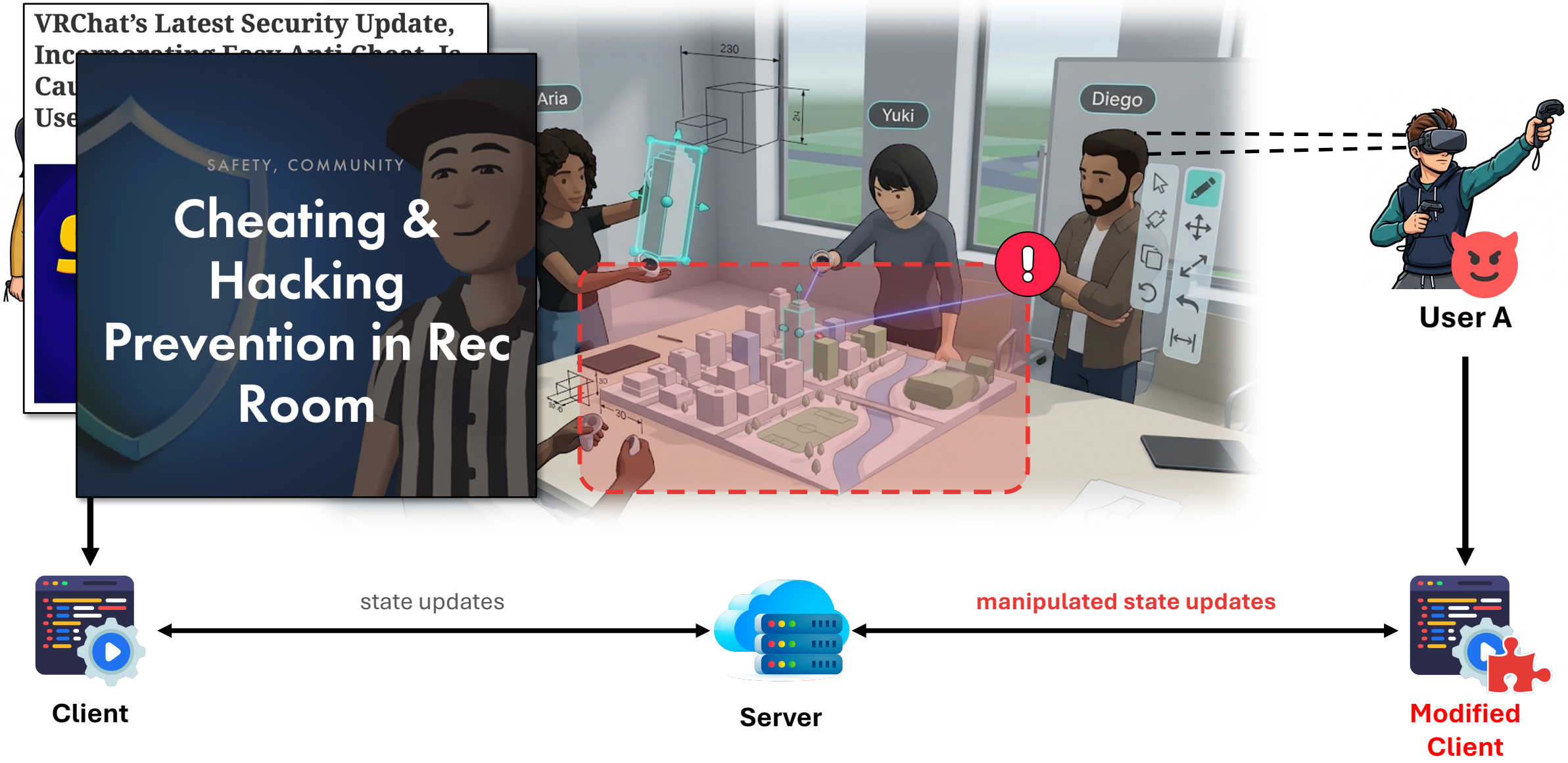

Aria
Yuki
Diego
Kwame
User B
User A
state updates
state updates
Client
Server
Client



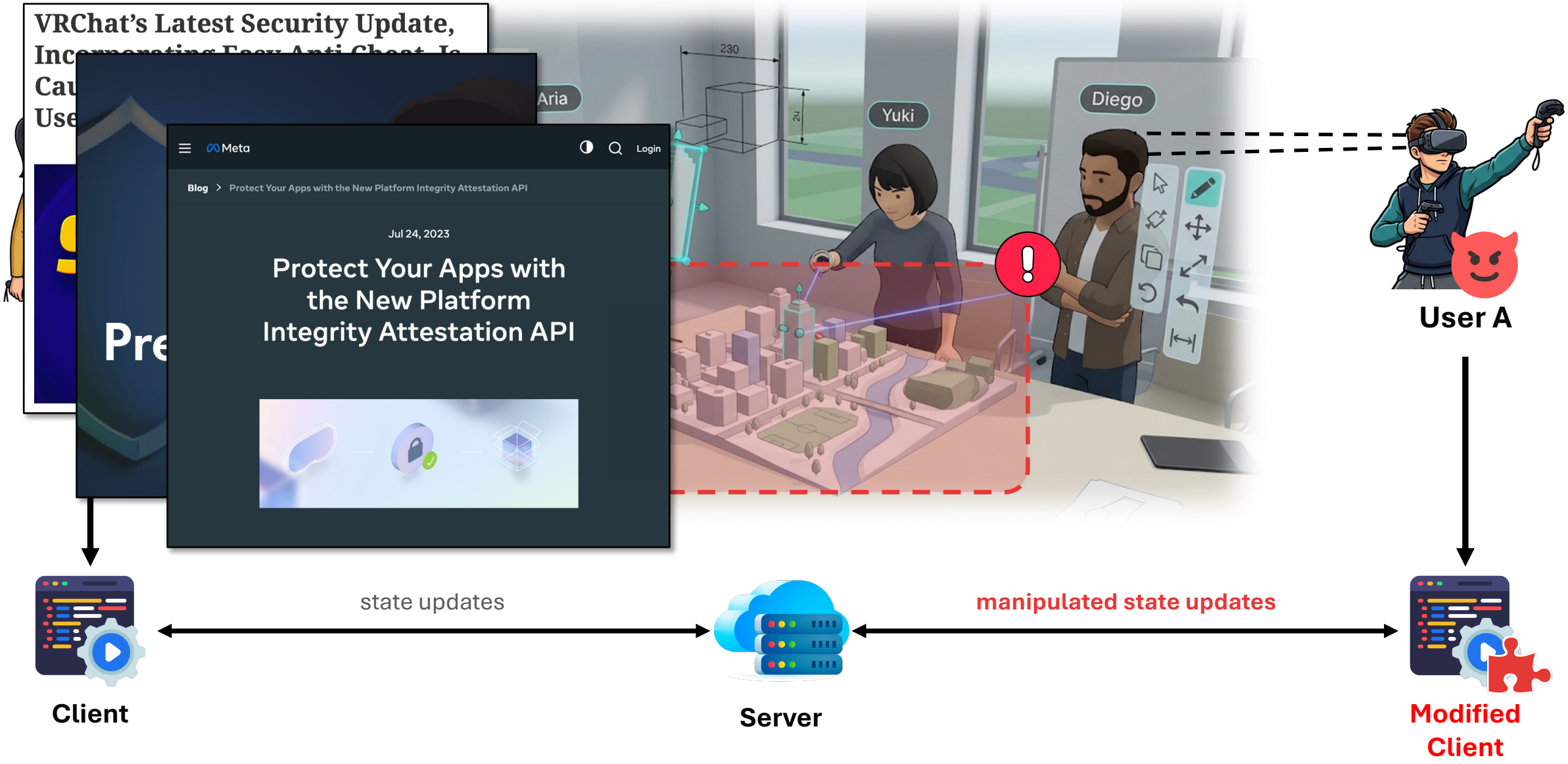
[1] A. Mengascini, R. Aurelio, and G. Pellegrino. The Big Brother's New Playground: Unmasking the Illusion of Privacy in Web Metaverses from a Malicious User's Perspective. ACM CCS 2024.
[2] M. Ali and H. Farrukh. Relay and Betray: Exploiting Client-Side Authority in Multi-User Mixed Reality. USENIX Security 2026.



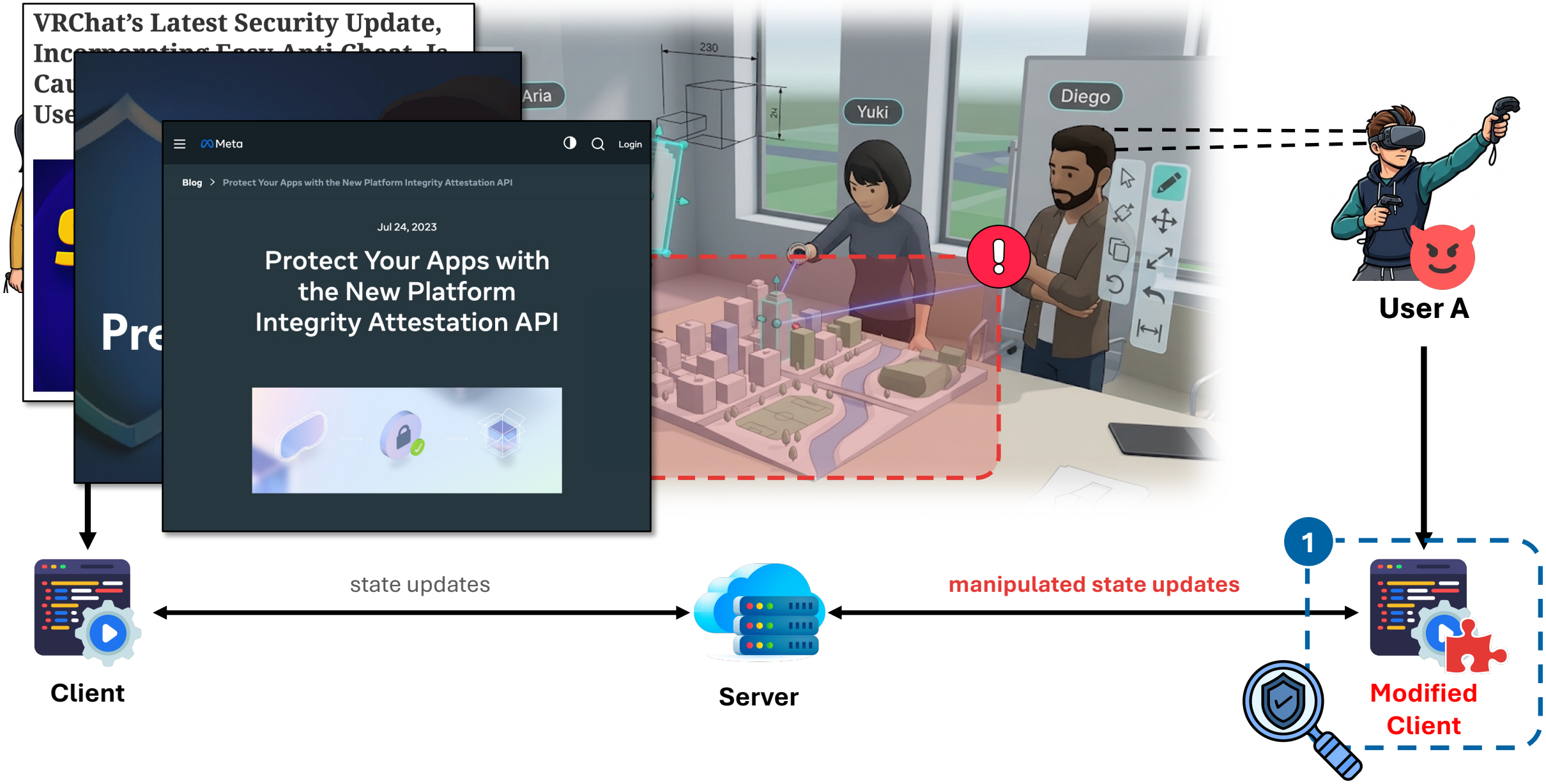
[1] A. Mengascini, R. Aurelio, and G. Pellegrino. The Big Brother's New Playground: Unmasking the Illusion of Privacy in Web Metaverses from a Malicious User's Perspective. ACM CCS 2024.
[2] M. Ali and H. Farrukh. Relay and Betray: Exploiting Client-Side Authority in Multi-User Mixed Reality. USENIX Security 2026.



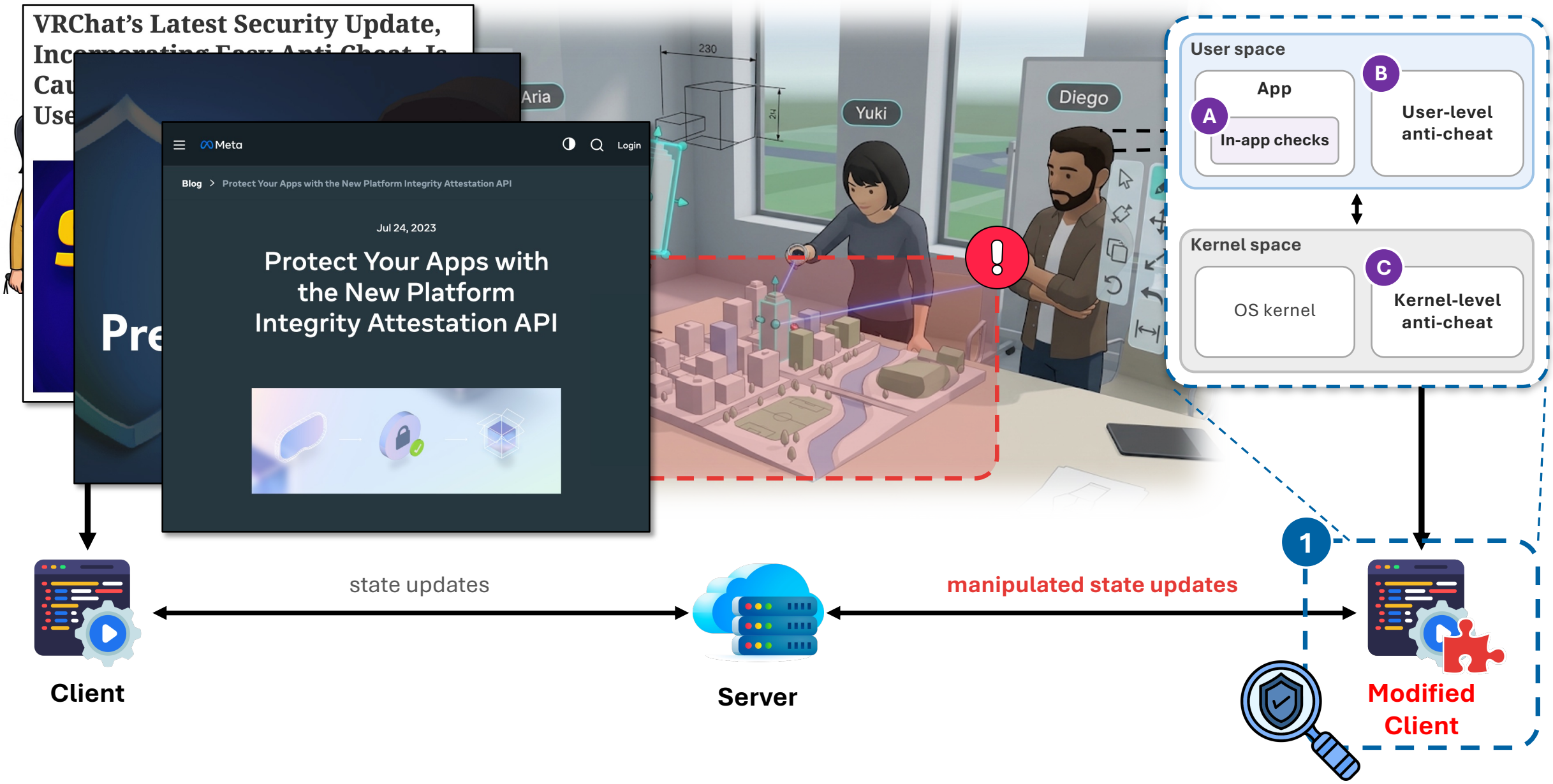
[1] A. Mengascini, R. Aurelio, and G. Pellegrino. The Big Brother's New Playground: Unmasking the Illusion of Privacy in Web Metaverses from a Malicious User's Perspective. ACM CCS 2024.
[2] M. Ali and H. Farrukh. Relay and Betray: Exploiting Client-Side Authority in Multi-User Mixed Reality. USENIX Security 2026.



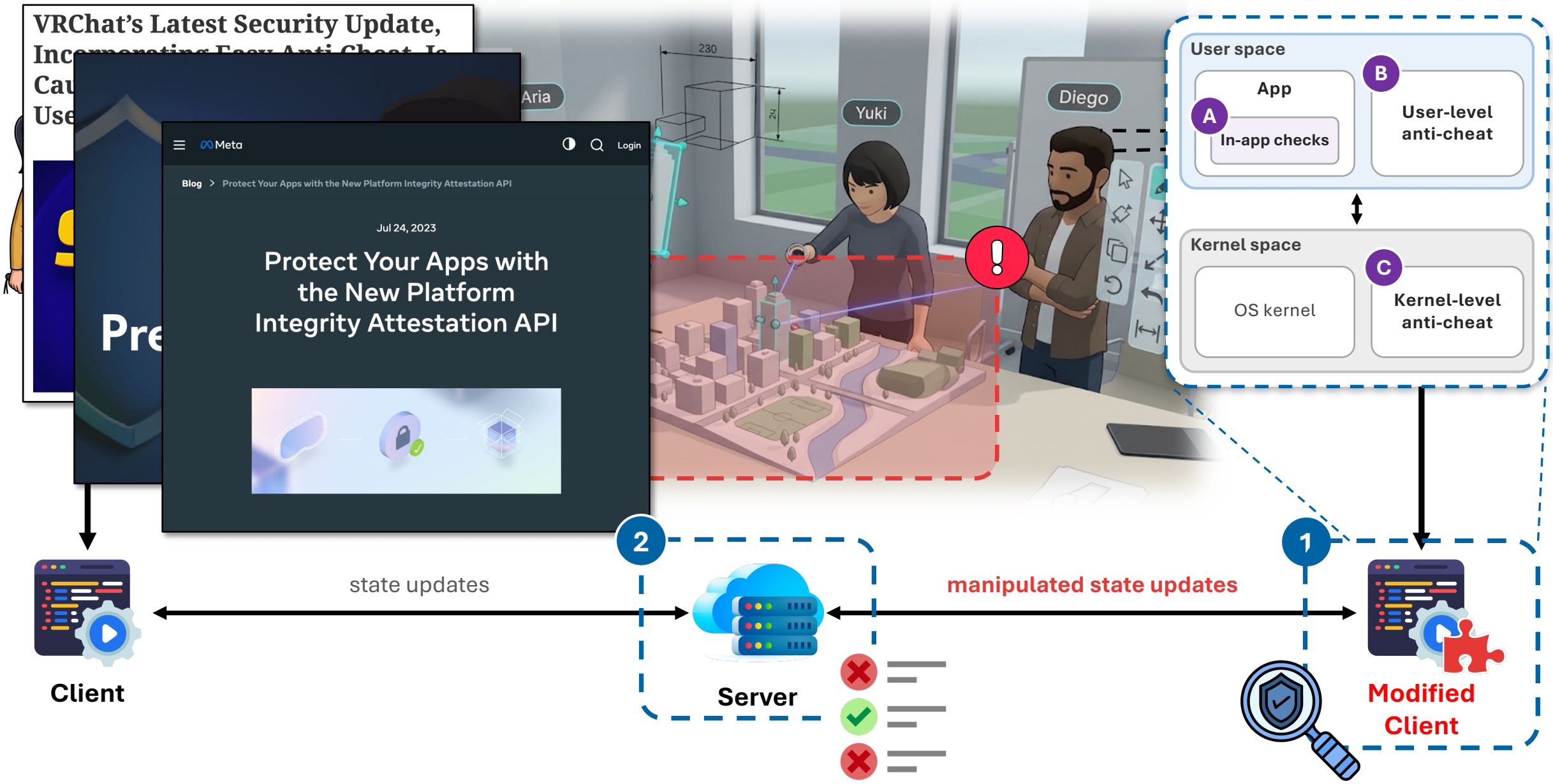
[1] A. Mengascini, R. Aurelio, and G. Pellegrino. The Big Brother's New Playground: Unmasking the Illusion of Privacy in Web Metaverses from a Malicious User's Perspective. ACM CCS 2024.
[2] M. Ali and H. Farrukh. Relay and Betray: Exploiting Client-Side Authority in Multi-User Mixed Reality. USENIX Security 2026.



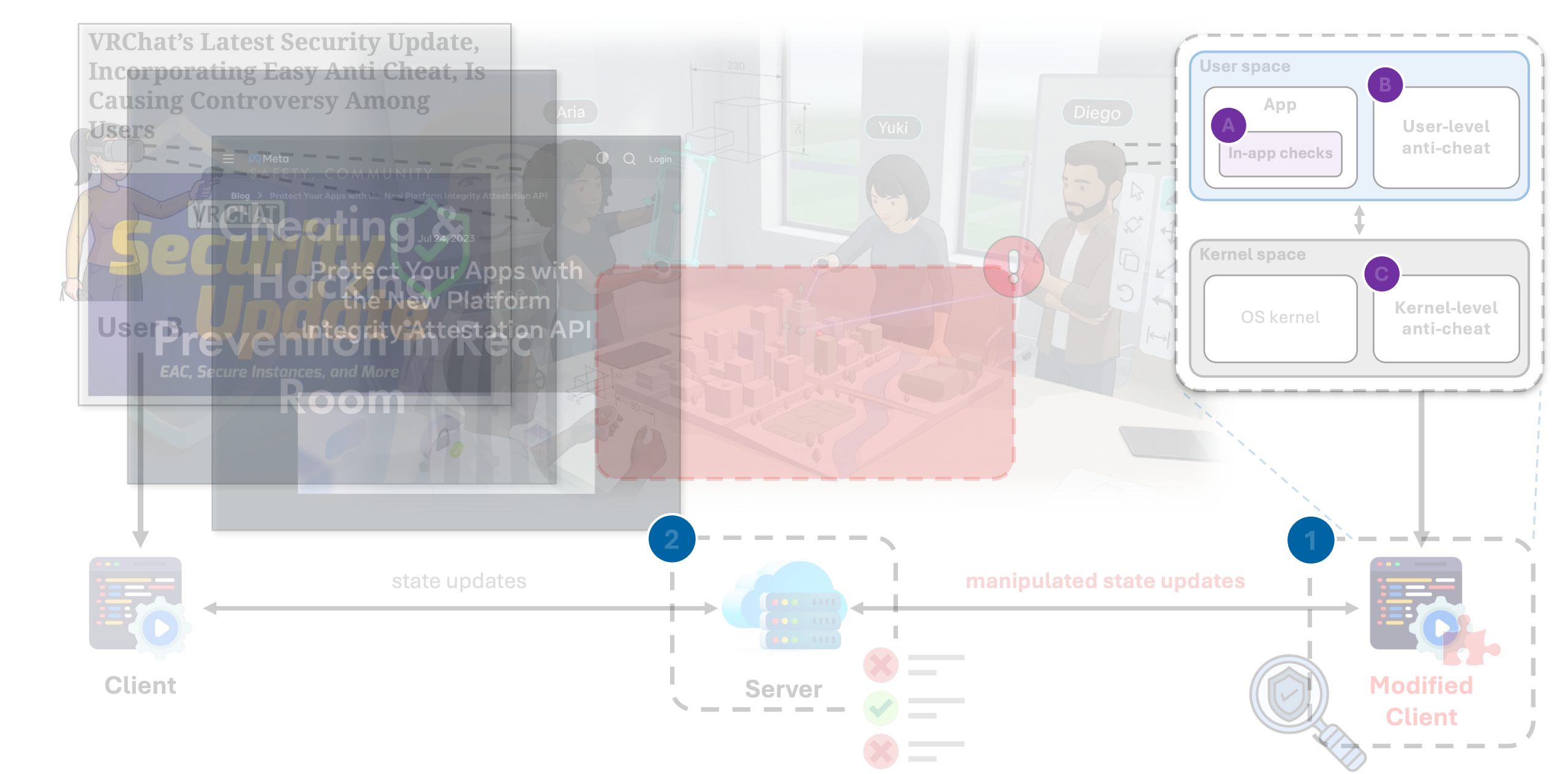
[1] A. Mengascini, R. Aurelio, and G. Pellegrino. The Big Brother's New Playground: Unmasking the Illusion of Privacy in Web Metaverses from a Malicious User's Perspective. ACM CCS 2024.
[2] M. Ali and H. Farrukh. Relay and Betray: Exploiting Client-Side Authority in Multi-User Mixed Reality. USENIX Security 2026.



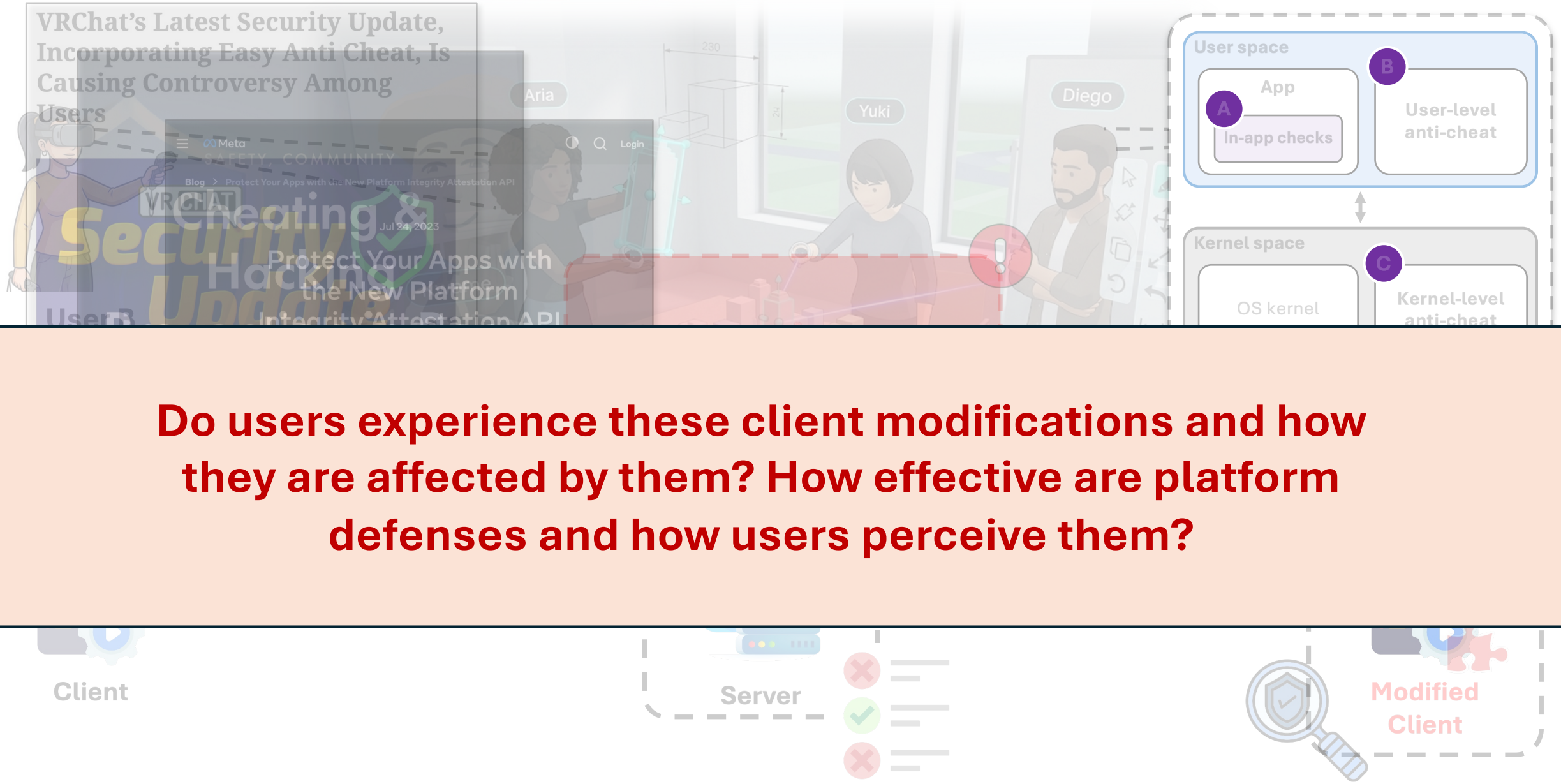
[1] A. Mengascini, R. Aurelio, and G. Pellegrino. The Big Brother's New Playground: Unmasking the Illusion of Privacy in Web Metaverses from a Malicious User's Perspective. ACM CCS 2024.
[2] M. Ali and H. Farrukh. Relay and Betray: Exploiting Client-Side Authority in Multi-User Mixed Reality. USENIX Security 2026.



[1] A. Mengascini, R. Aurelio, and G. Pellegrino. The Big Brother's New Playground: Unmasking the Illusion of Privacy in Web Metaverses from a Malicious User's Perspective. ACM CCS 2024.
[2] M. Ali and H. Farrukh. Relay and Betray: Exploiting Client-Side Authority in Multi-User Mixed Reality. USENIX Security 2026.



[1] A. Mengascini, R. Aurelio, and G. Pellegrino. The Big Brother's New Playground: Unmasking the Illusion of Privacy in Web Metaverses from a Malicious User's Perspective. ACM CCS 2024.
[2] M. Ali and H. Farrukh. Relay and Betray: Exploiting Client-Side Authority in Multi-User Mixed Reality. USENIX Security 2026.



Do users experience these client modifications and how they are affected by them? How effective are platform defenses and how users perceive them?

[1] A. Mengascini, R. Aurelio, and G. Pellegrino. The Big Brother's New Playground: Unmasking the Illusion of Privacy in Web Metaverses from a Malicious User's Perspective. ACM CCS 2024.
[2] M. Ali and H. Farrukh. Relay and Betray: Exploiting Client-Side Authority in Multi-User Mixed Reality. USENIX Security 2026.

Research Questions

Research Questions

RQ1 What concerns do users articulate about client modifications in social XR?

Research Questions

RQ1 What concerns do users articulate about client modifications in social XR?

RQ2 What are users' perceptions of the platform defenses deployed against client modifications?

Research Questions

RQ1 What concerns do users articulate about client modifications in social XR?

RQ2 What are users' perceptions of the platform defenses deployed against client modifications?

RQ3 How do users' concerns and perceptions evolve over time, and how do major events in the social XR ecosystem influence them?

User Discourse





Longitudinal View



Global User Perspectives and Scale



Real-World Reactions

User Discourse



Subreddit	Size
r/VRChat	213K
r/RecRoom	63K
r/VirtualReality	2.1M
r/VRGaming	159K



Longitudinal View



Global User Perspectives and Scale



Real-World Reactions

User Discourse





Longitudinal View



Global User Perspectives and Scale



Real-World Reactions

Subreddit	Size
r/VRChat	213K
r/RecRoom	63K
r/VirtualReality	2.1M
r/VRGaming	159K



Most popular social XR platforms

VRChat: **60K+** concurrent users [1]

Rec Room: **3M+** monthly active users [2]



Both have deployed defenses against client mods, including anti-cheat engines

[1] SteamDB. VRChat · SteamDB. steamdb.info/app/438100, 2026.
[2] S. Hayden. Virtual Social Platform ‘Rec Room’ Hits 3 Million Monthly Active VR Users. Road to VR, 2022.

User Discourse

Subreddit	Size
r/VRChat	213K
r/RecRoom	63K
r/VirtualReality	2.1M
r/VRGaming	159K

Longitudinal View

Global User Perspectives and Scale

Real-World Reactions

Most popular social XR platforms

VRChat: **60K+** concurrent users [1]

Rec Room: **3M+** monthly active users [2]

Both have deployed defenses against client mods, including anti-cheat engines

Largest general-purpose XR communities

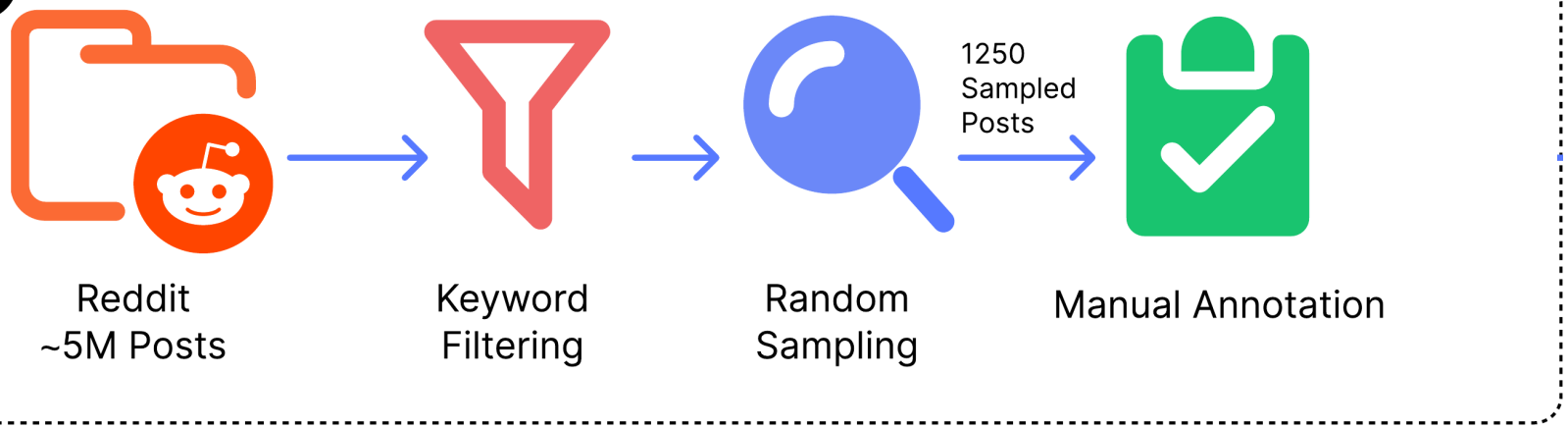
Users compare experiences across platforms

[1] SteamDB. VRChat · SteamDB. steamdb.info/app/438100, 2026.

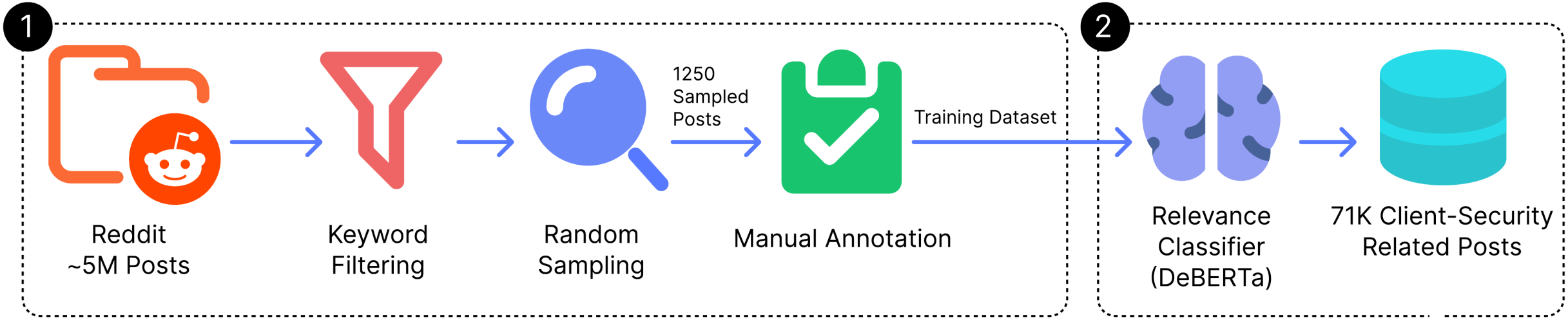
[2] S. Hayden. Virtual Social Platform ‘Rec Room’ Hits 3 Million Monthly Active VR Users. Road to VR, 2022.

Methodology

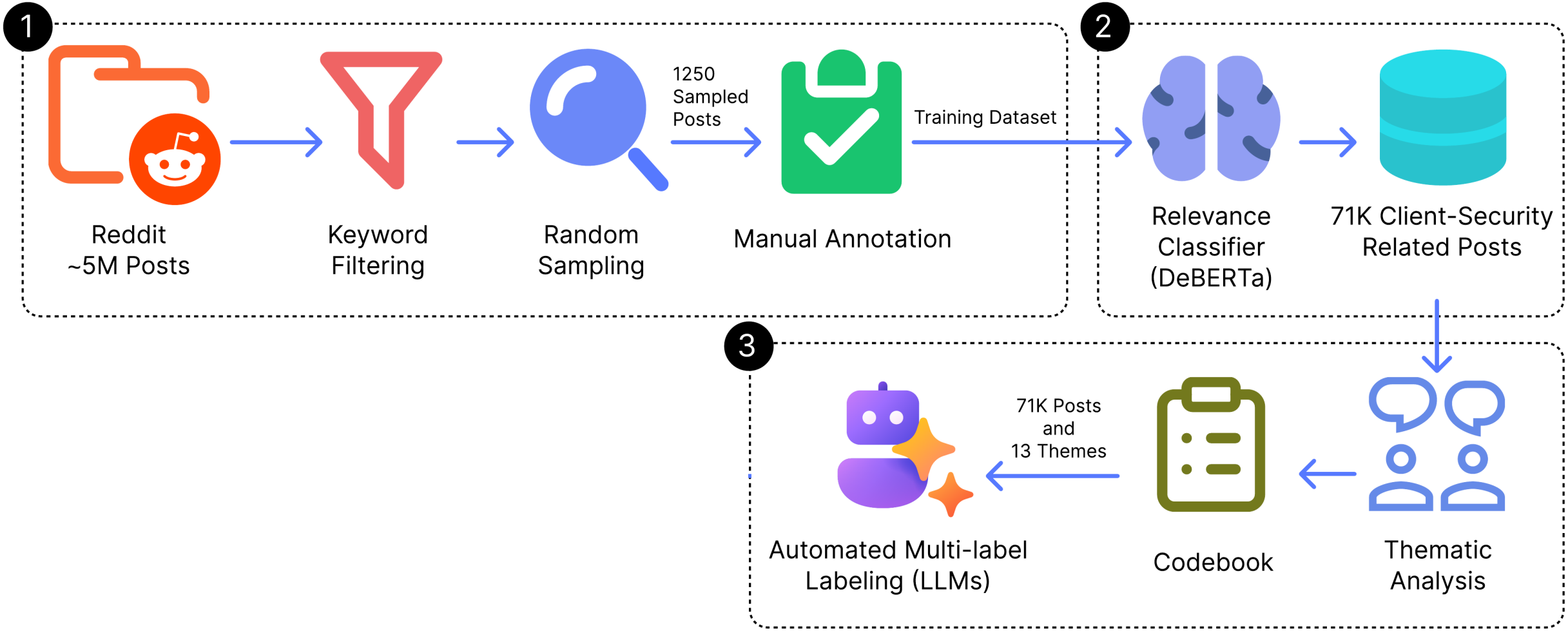
1



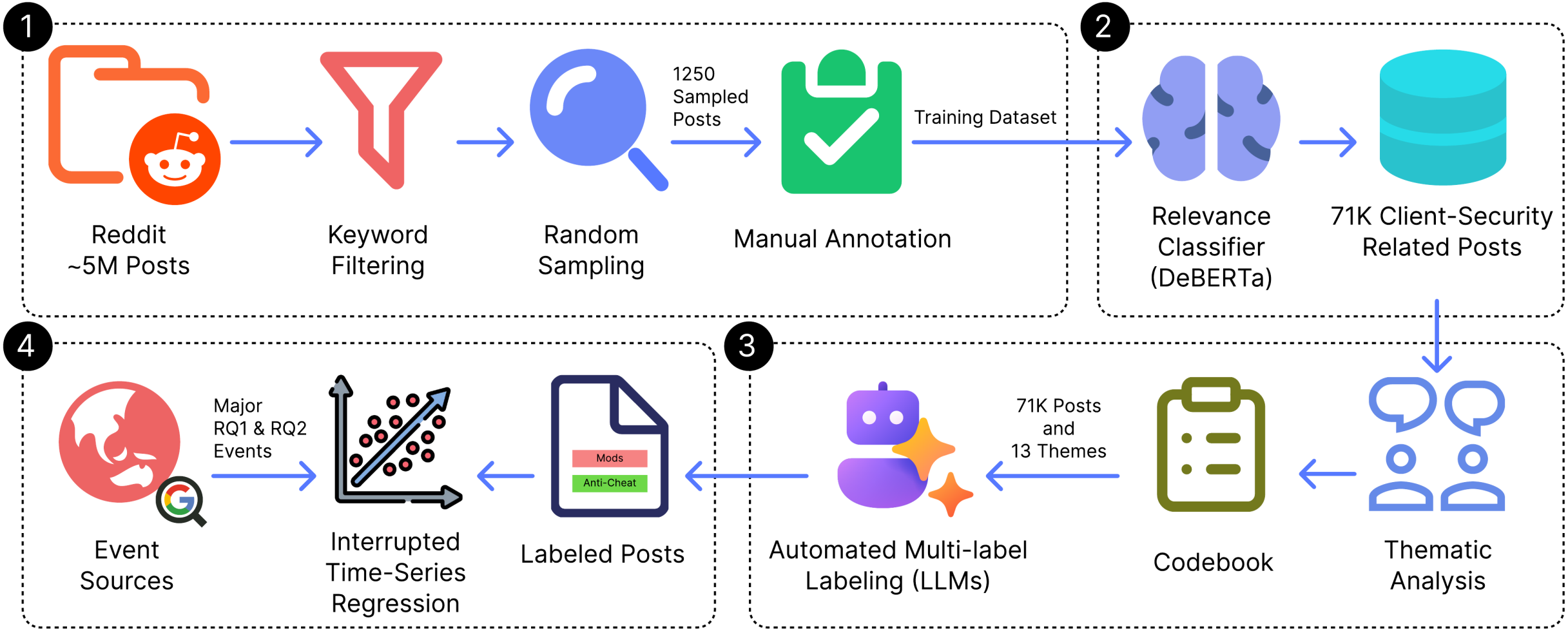
Methodology



Methodology



Methodology



RQ1: Client Modification



Asset Theft

- Avatar & world ripping
- Identity theft & impersonation
- IP & creativity theft



Safety Evasion

- Block evasion
- Votekick evasion
- Forced entry into private instances



Disruption

- Crashing
- Inducing lag
- Forced teleportation
- Object manipulation



Private Info Access

- Who is in private instances
- Friend lists & blocked status
- IP addresses



Mod Side-Effects

- Malware & keyloggers
- Auth-token stealers
- Account hijacking

RQ1: Client Modification



Asset Theft

- Avatar & world ripping
- Identity theft & impersonation
- IP & creativity theft



Safety Evasion

- Block evasion
- Votekick evasion
- Forced entry into private instances



Disruption

- Crashing
- Inducing lag
- Forced teleportation
- Object manipulation



Private Info Access

- Who is in private instances
- Friend lists & blocked status
- IP addresses



Mod Side-Effects

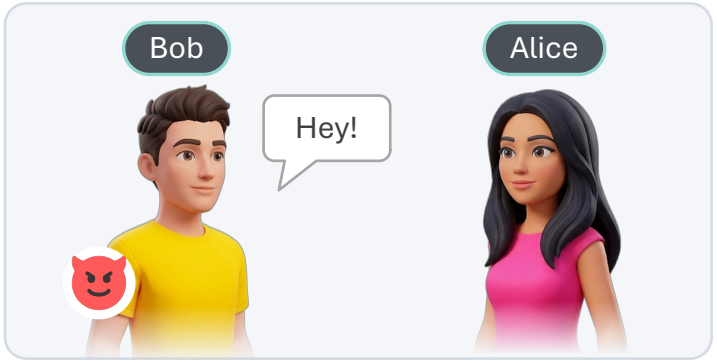
- Malware & keyloggers
- Auth-token stealers
- Account hijacking

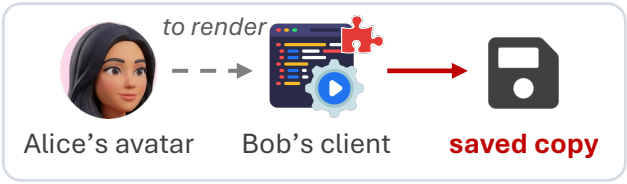
Asset Theft



Avatar Ripping

> *"When you equip your avatar, the package … is downloaded on everyone else's device … **a modified client just grabs that package and saves it**"*





Asset Theft

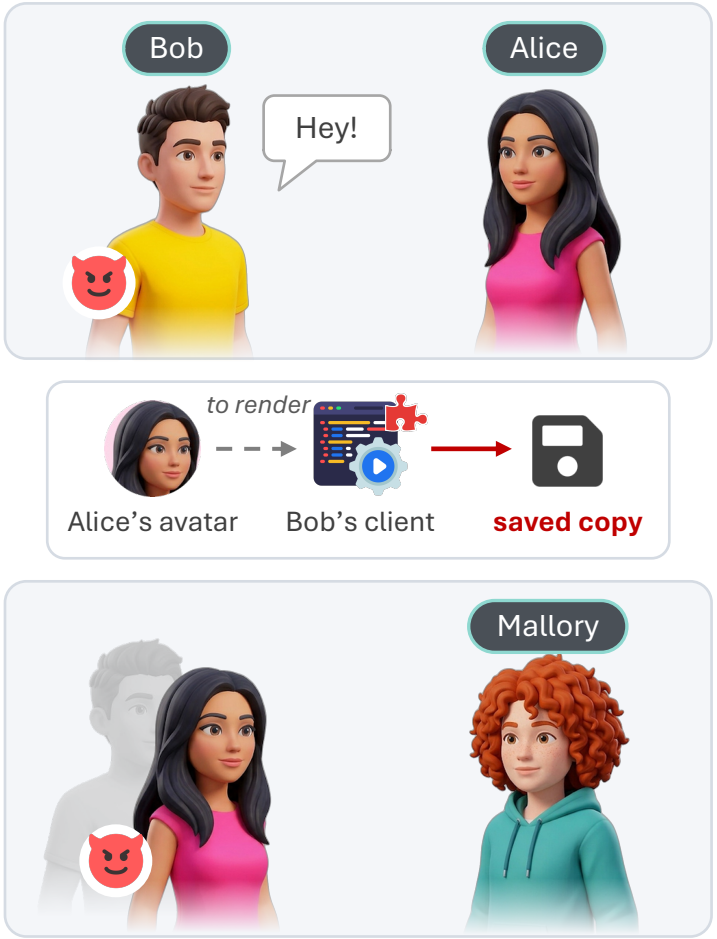
Avatar Ripping

> *"When you equip your avatar, the package … is downloaded on everyone else's device … **a modified client just grabs that package and saves it**"*

Identity Theft & Impersonation

> *"My avatar has been **my face and my identity in VR** … losing it would feel like **having my identity stolen** and someone parading around as me in real life"*

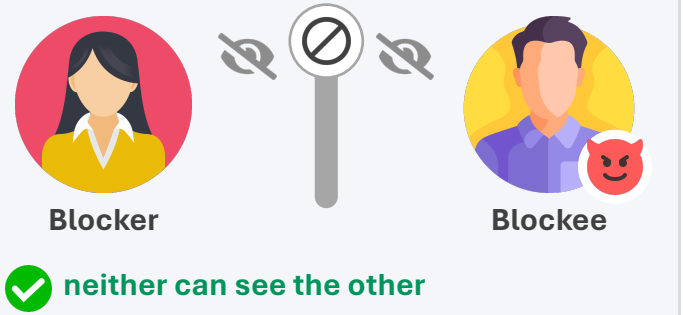
> *"Personal avatars are a form of self-expression as well, so taking one is **basically identity theft** … Picture walking down the block and coming face to face with a copy of yourself"*



Bob impersonates Alice in front of Mallory

Safety Evasion

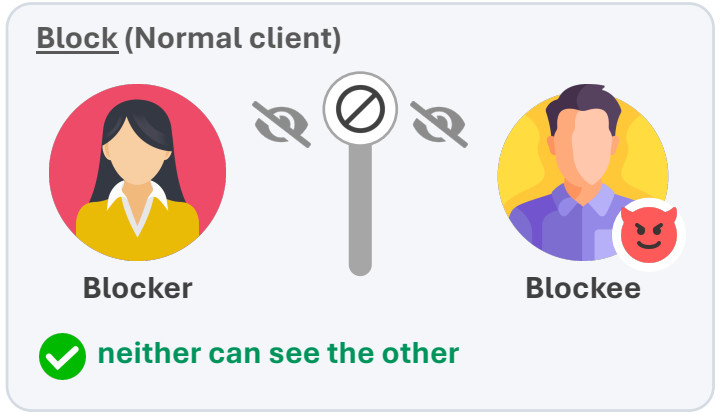
Block (Normal client)

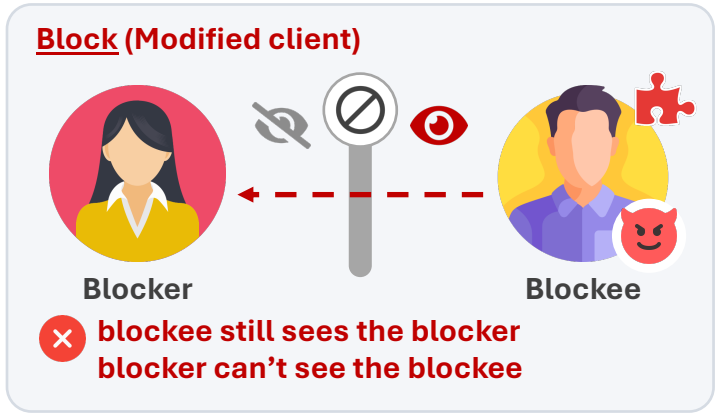


neither can see the other

[1] Harassment in Social Virtual Reality: Challenges for Platform Governance (CSCW'19)
[2] Disturbing the Peace: Experiencing and Mitigating Emerging Harassment in Social Virtual Reality (CSCW'22)
[3] Understanding Safety Risks and Safety Design in Social VR Environments (CSCW'23)

Safety Evasion



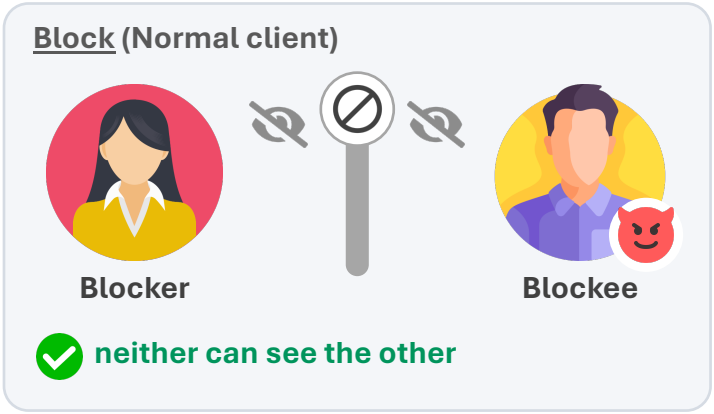


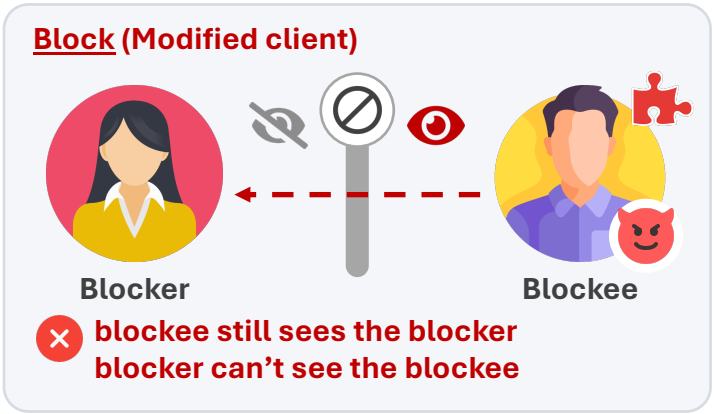
Safety Tools Fail Against Mods

"The trouble with blocking [modified clients] is that it doesn't always work ... ***the administrative powers sit on the client side"***

[1] Harassment in Social Virtual Reality: Challenges for Platform Governance (CSCW'19)
[2] Disturbing the Peace: Experiencing and Mitigating Emerging Harassment in Social Virtual Reality (CSCW'22)
[3] Understanding Safety Risks and Safety Design in Social VR Environments (CSCW'23)

Safety Evasion





Safety Tools Fail Against Mods

> *"The trouble with blocking [modified clients] is that it doesn't always work ...* ***the administrative powers sit on the client side"***

Persistent Stalking & Harassment

> *"What gets to me is that a user I already blocked* ***can still somehow track me down*** *and there's nothing I can do about it"*

> *"A friend of mine got harassed and stalked in VRC by someone running a mod that let him* ***sneak into invite-only world instances"***

[1] Harassment in Social Virtual Reality: Challenges for Platform Governance (CSCW'19)
[2] Disturbing the Peace: Experiencing and Mitigating Emerging Harassment in Social Virtual Reality (CSCW'22)
[3] Understanding Safety Risks and Safety Design in Social VR Environments (CSCW'23)

RQ2: Platform Defenses



- Server-Side Validation
- Anti-Cheat Engines
- Client Integrity and Attestation

RQ2: Platform Defenses



- Server-Side Validation
- Anti-Cheat Engines
- Client Integrity and Attestation



RQ2: Platform Defenses



- Server-Side Validation
- Anti-Cheat Engines
- Client Integrity and Attestation





AC Effectiveness

- Seen as effective (deterrence)
- Seen as ineffective (bypassable)
- Limited platform coverage
- User- vs. kernel-level



AC Tradeoffs

- Performance overhead
- Usability issues
- Loss of useful mods
- Privacy (kernel-level)



User Recommendations

- Official mod support
- Account-level enforcement
- Server-side validation



Financial Motives

- Features behind a paywall
- Investor demands

RQ2: Platform Defenses



- Server-Side Validation
- Anti-Cheat Engines
- Client Integrity and Attestation





AC Effectiveness

- Seen as effective (deterrence)
- Seen as ineffective (bypassable)
- Limited platform coverage
- User- vs. kernel-level



AC Tradeoffs

- Performance overhead
- Usability issues
- Loss of useful mods
- Privacy (kernel-level)



User Recommendations

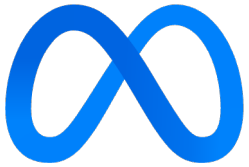
- Official mod support
- Account-level enforcement
- Server-side validation



Financial Motives

- Features behind a paywall
- Investor demands

Limited Platform Coverage













Limited Platform Coverage



Anti-Cheats Do Not Cover All Platforms

*“Modding hasn’t gone anywhere, since **Easy Anti- Cheat doesn’t run on Android**; you can just run the Android build on PC through an emulator ”*

Tradeoffs

Loss of Accessibility Mods

“Some players with disabilities relied on mods for accessibility reasons and after the update, ***they cannot play at all****”*





Tradeoffs

Loss of Accessibility Mods

“Some players with disabilities relied on mods for accessibility reasons and after the update, ***they cannot play at all****”*



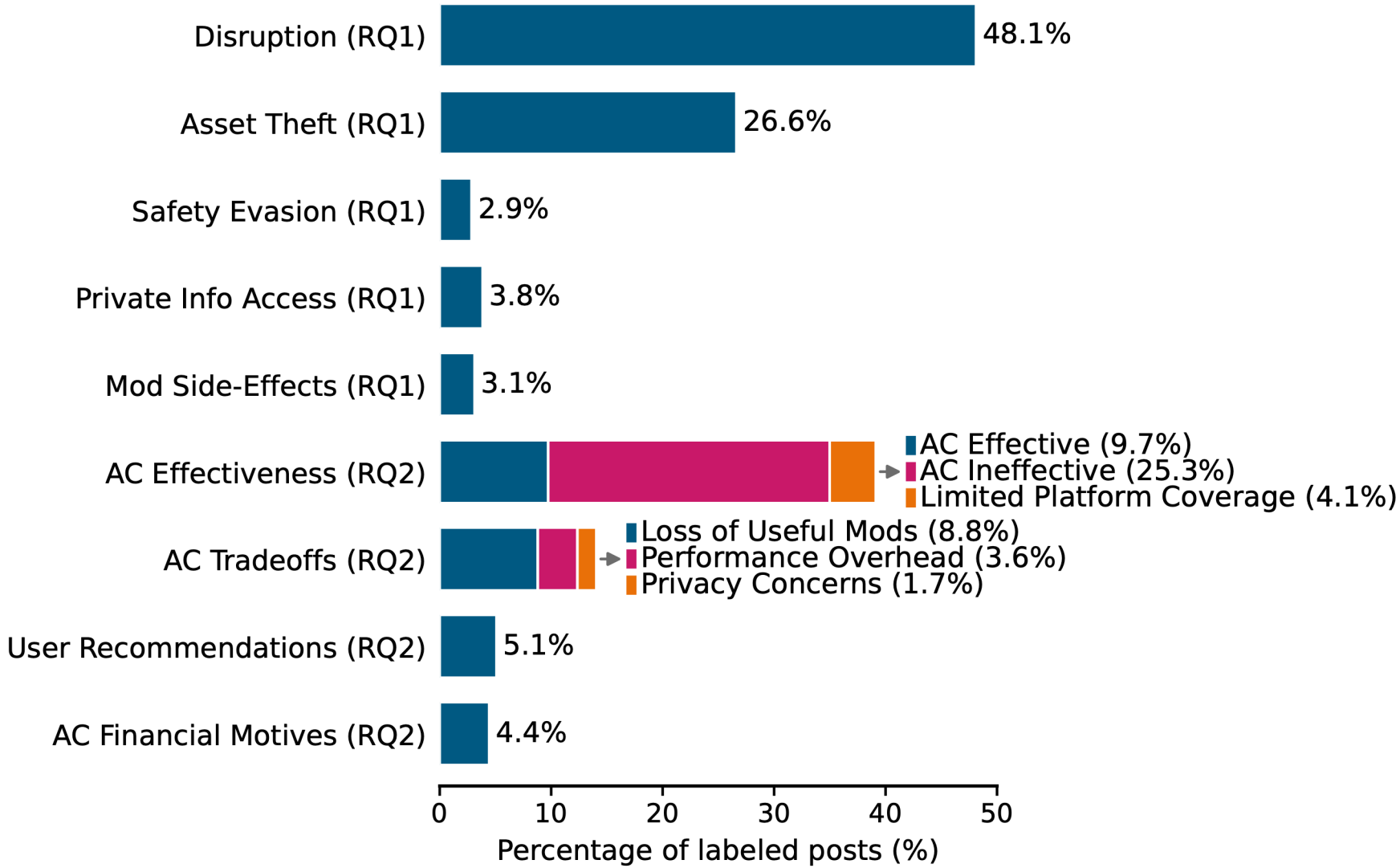


Privacy Concerns About Kernel-level ACs

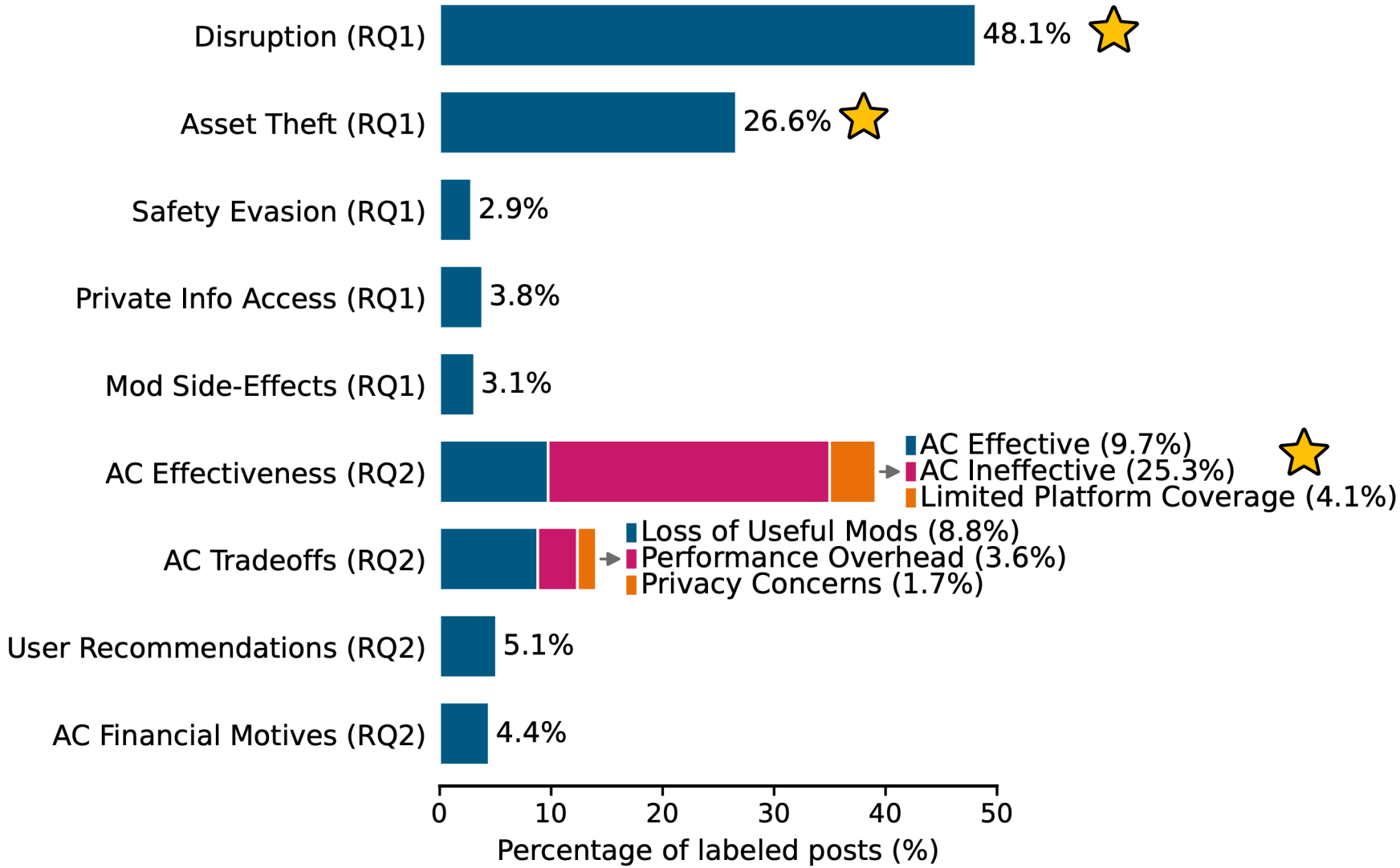
“Is EAC actually spying on me? This is straight from the EAC EULA: … you give your consent that Easy Anti-Cheat may ***gather, store, and publish data*** *…”*

“There’s no reason a ***social chat app*** *should require a* ***surveillance rootkit****”*

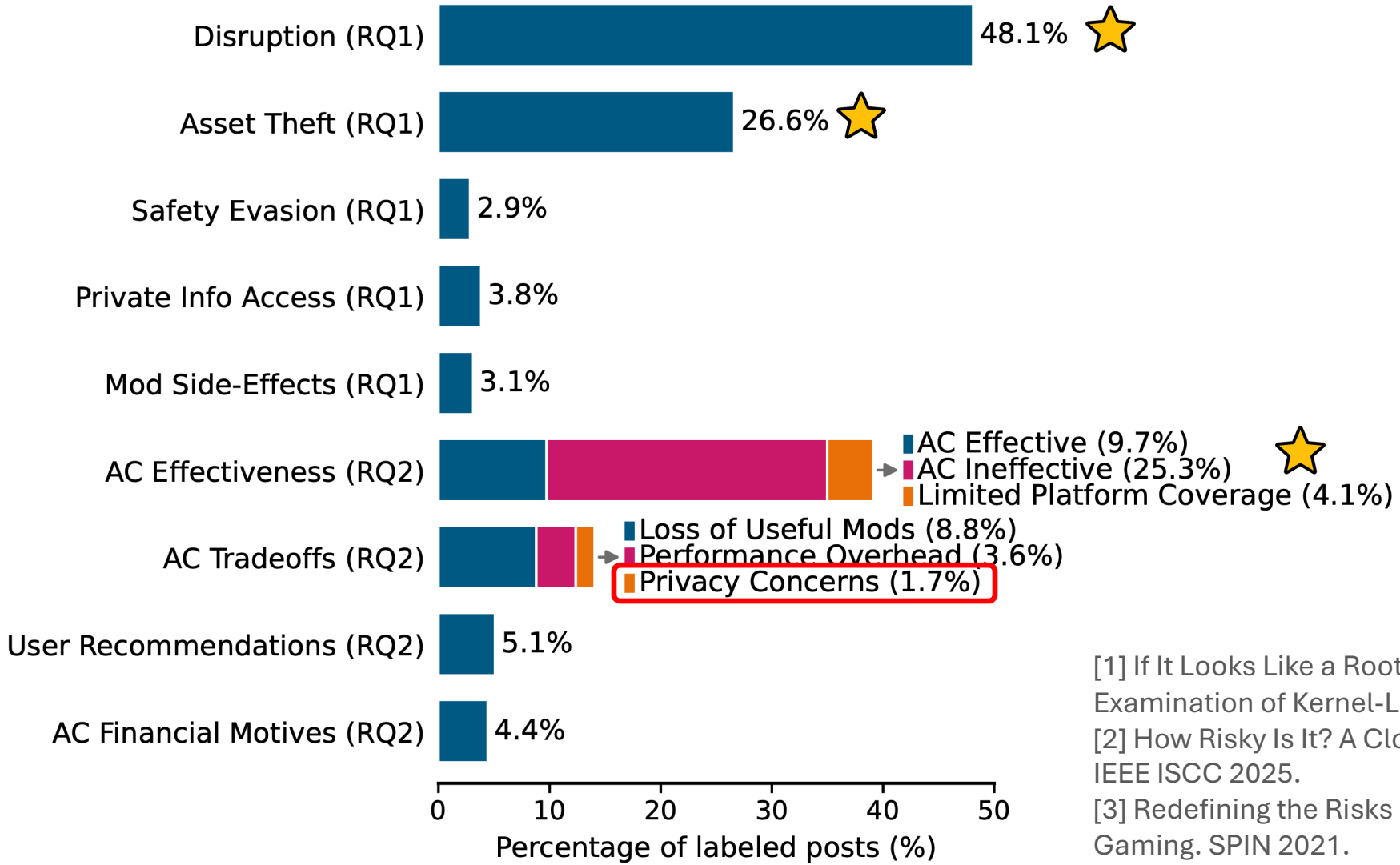
Prevalence


Disruption (RQ1)
48.1%
Asset Theft (RQ1)
26.6%
Safety Evasion (RQ1)
2.9%
Private Info Access (RQ1)
3.8%
Mod Side-Effects (RQ1)
3.1%
AC Effectiveness (RQ2)
AC Effective (9.7%)
AC Ineffective (25.3%)
Limited Platform Coverage (4.1%)
AC Tradeoffs (RQ2)
Loss of Useful Mods (8.8%)
Performance Overhead (3.6%)
Privacy Concerns (1.7%)
User Recommendations (RQ2)
5.1%
AC Financial Motives (RQ2)
4.4%
0
10
20
30
40
50
Percentage of labeled posts (%)

Prevalence

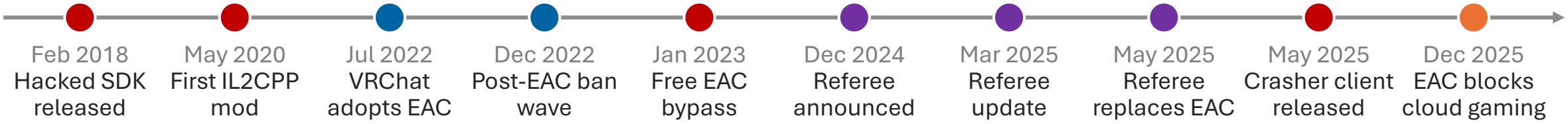

Disruption (RQ1)
48.1%
Asset Theft (RQ1)
26.6%
Safety Evasion (RQ1)
2.9%
Private Info Access (RQ1)
3.8%
Mod Side-Effects (RQ1)
3.1%
AC Effectiveness (RQ2)
AC Effective (9.7%)
AC Ineffective (25.3%)
Limited Platform Coverage (4.1%)
AC Tradeoffs (RQ2)
Loss of Useful Mods (8.8%)
Performance Overhead (3.6%)
Privacy Concerns (1.7%)
User Recommendations (RQ2)
5.1%
AC Financial Motives (RQ2)
4.4%
0
10
20
30
40
50
Percentage of labeled posts (%)

Prevalence



[1] If It Looks Like a Rootkit and Deceives Like a Rootkit: A Critical Examination of Kernel-Level Anti-Cheat Systems. ARES 2024.
[2] How Risky Is It? A Closer Look at Game Anti-Cheat Software. IEEE ISCC 2025.
[3] Redefining the Risks of Kernel-Level Anti-Cheat in Online Gaming. SPIN 2021.

RQ3: Evolution Over Time

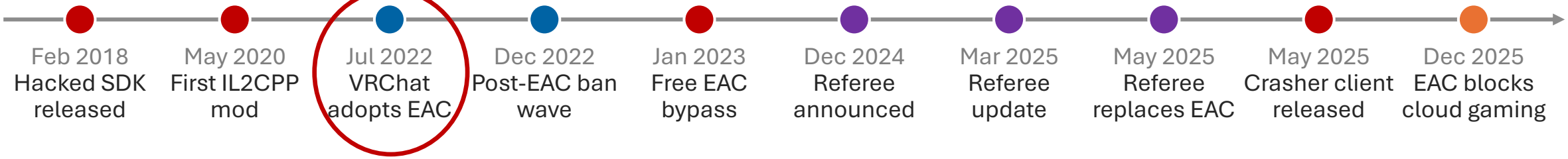


Mod & bypass releases AC adoption & enforcement Migration to in-house AC AC updates

RQ3: Evolution Over Time

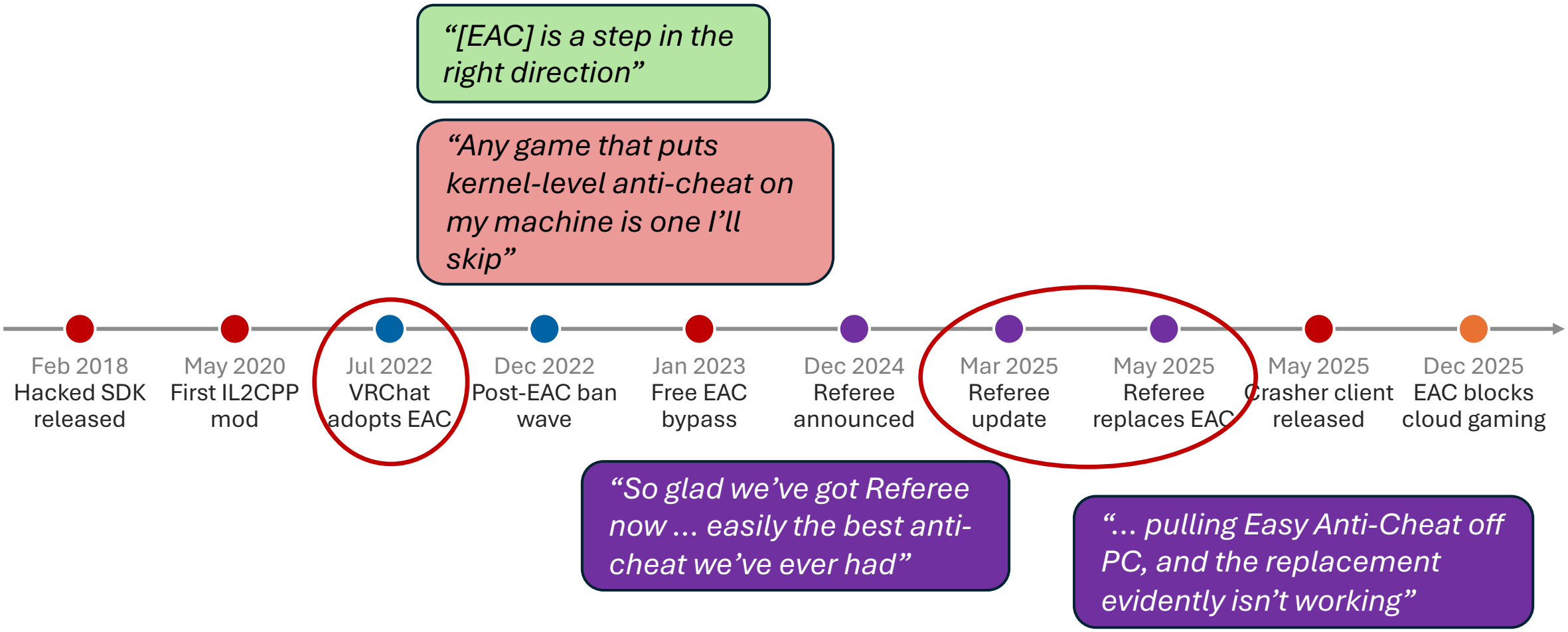
“[EAC] is a step in the right direction”

“Any game that puts kernel-level anti-cheat on my machine is one I’ll skip”

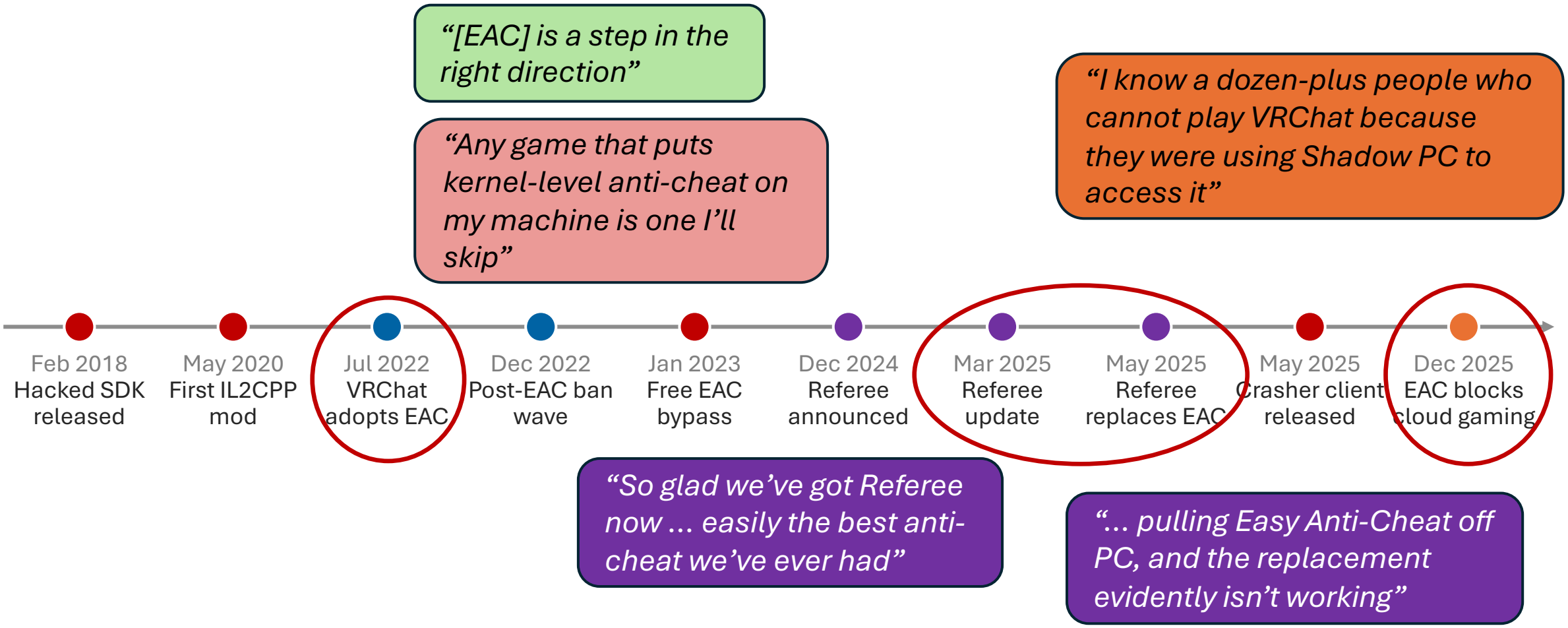


Mod & bypass releases AC adoption & enforcement Migration to in-house AC AC updates

RQ3: Evolution Over Time



RQ3: Evolution Over Time



Recommendations

For Platforms



Official mod support

Build popular safety & accessibility mods in as first-party features



Stronger account enforcement

Hardware-ID & IP bans raise the cost of modding



Defense in depth

AC + integrity checks + attestation, with server-side checks for safety features



Transparency

Have transparency around the reasons for AC adoption (e.g., financial motives or IP theft)

Recommendations

For Platforms



Official mod support

Build popular safety & accessibility mods in as first-party features



Stronger account enforcement

Hardware-ID & IP bans raise the cost of modding



Defense in depth

AC + integrity checks + attestation, with server-side checks for safety features



Transparency

Have transparency around the reasons for AC adoption (e.g., financial motives or IP theft)

For Users



Use private, unlisted instances

Trades community size and usability for safety

For Policymakers



Set platform guidelines for sensitive uses

e.g., K-12 education, workplaces

Conclusion



Analysis of ~5M Reddit posts on client mods and defenses in social XR



Client mods worsen harms in social XR



Anti-cheat is partially effective, but its costs fall on users who never modded



Sentiment toward anti-cheat shifts with events in the ecosystem



Recommendations for platforms, users, and policymakers

Conclusion

- Analysis of ~5M Reddit posts on client mods and defenses in social XR
- Client mods worsen harms in social XR
- Anti-cheat is partially effective, but its costs fall on users who never modded
- Sentiment toward anti-cheat shifts with events in the ecosystem
- Recommendations for platforms, users, and policymakers



Thank You!