Northeastern University

From Perception to Protection: A Developer-Centered Study of Security and Privacy Threats in Extended Reality (XR)

Kunlin Cai, Jinghuai Zhang, Ying Li, Zhiyuan Wang, Xun Chen, Tianshi Li, Yuan Tian

NDSS 2026

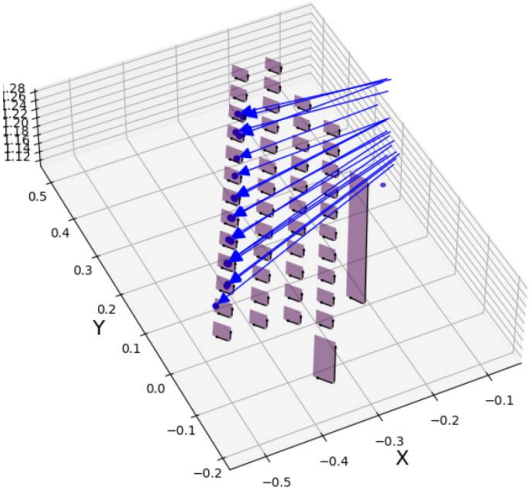
Background

The Rise of XR:

- Rapid adoption across critical sectors
  - e.g., Education, Healthcare, Social Interaction, and Retail
- Unprecedented user interactions & data collection
  - e.g., gaze, gestures, biometric data

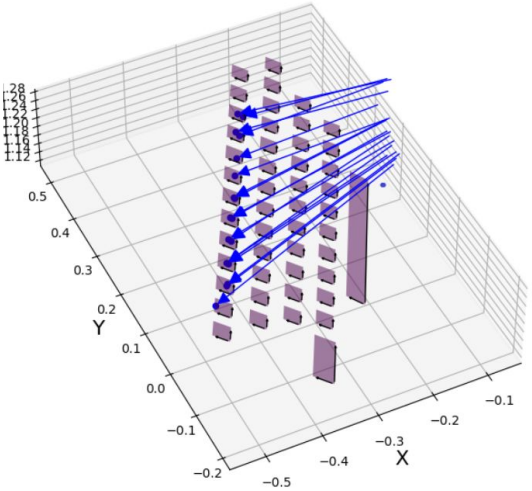
Extended Reality (XR)

Background

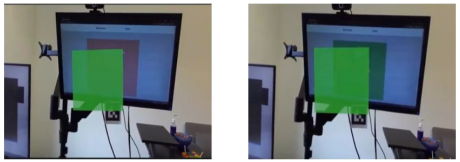


Keylogging Attacks

Background

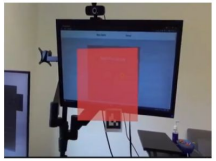


Keylogging Attacks

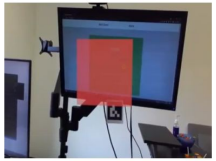


(a) FalseGreen Attack

(b) DoubleGreen Attack



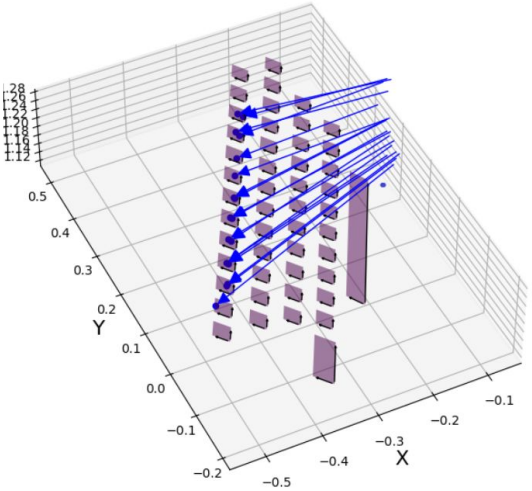
(c) DoubleRed Attack



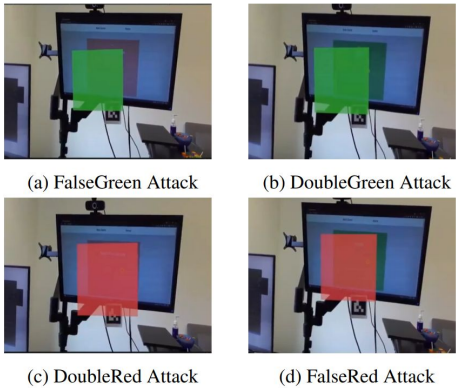
(d) FalseRed Attack

Perception Manipulation

Background



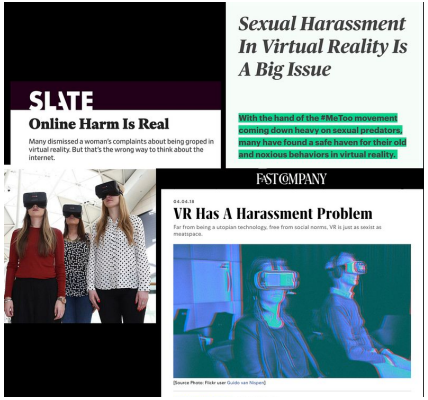
Keylogging Attacks



(a) FalseGreen Attack (b) DoubleGreen Attack

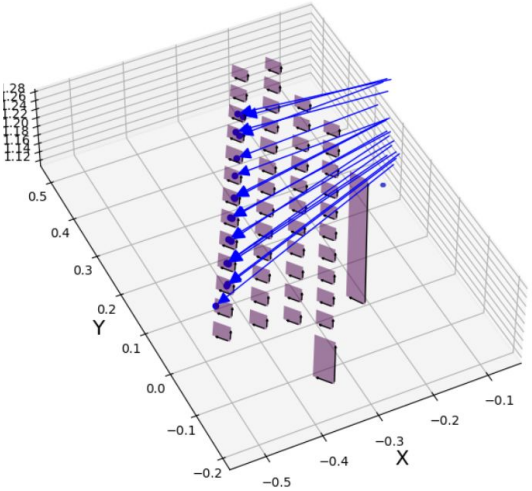
(c) DoubleRed Attack (d) FalseRed Attack

Perception Manipulation

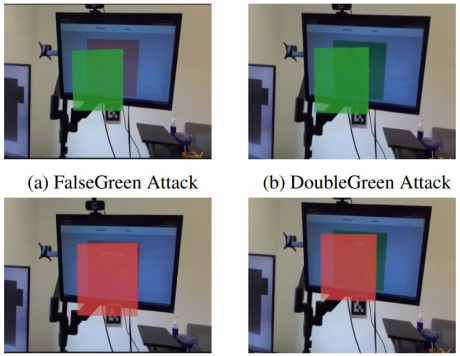


Social Harassment

Background



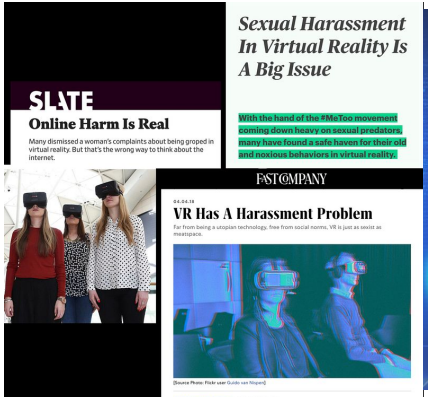
Keylogging Attacks



(a) FalseGreen Attack (b) DoubleGreen Attack

(c) DoubleRed Attack (d) FalseRed Attack

Perception Manipulation



Social Harassment

Privacy Leakage

Background

The Prevalence of S&P Issues in XR

Metaverse poses serious privacy risks for users, report warns

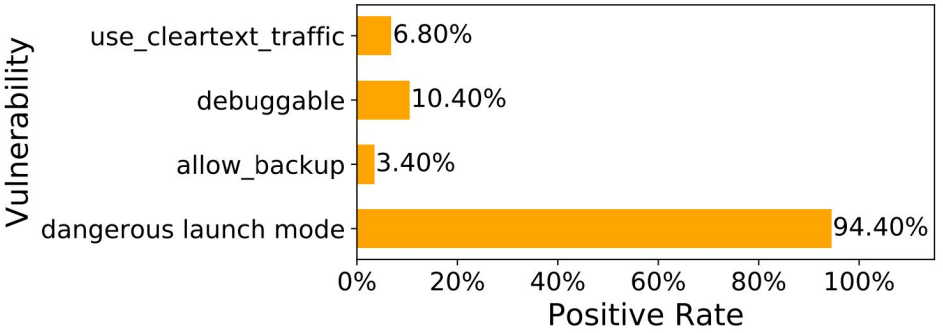
The immersive internet experience known as the metaverse will erode users' privacy unless significant steps are taken to improve and regulate how the technology captures and stores personal data, a new report from New York University argues.

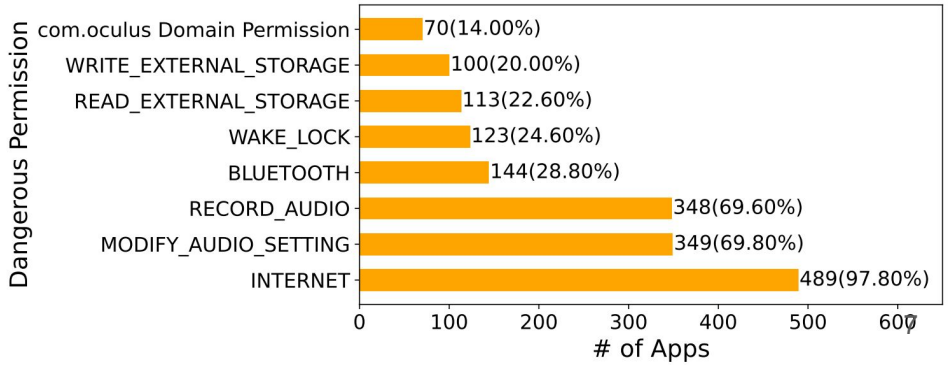
Metaverse or Metaworse? How the Apple Vision Pro Stacks Up Against Predictions

In 2022, Trend Micro conducted extensive research to understand potential cyber threats to the metaverse amid significant global changes and a growing focus on AI technologies. The release of Apple's Apple Vision Pro headset a year later provided an opportunity to evaluate these predictions, highlighting both advancements and persistent challenges in areas such as data privacy, biometric security, and multi-vendor interoperability.

Youth Face Rising Risks of Harassment and Exploitation in the Metaverse

Featured Neuroscience Psychology · October 23, 2024



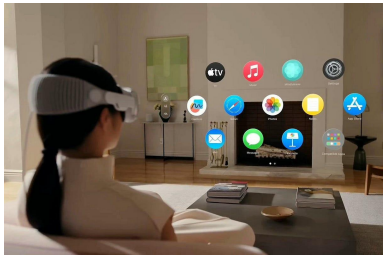


Background

Understanding Developers – The Primary Architects:

- Identifying new XR threats does not necessarily lead to their prevention in practice
- Research is mostly user-centered or system-centered
- Lack of in-depth studies from the developer's perspective and of realistic threats in XR

Research Questions



- **RQ1:** What are developers' perceptions of emerging S&P threats in XR?
- **RQ2:** What are developers' perceptions of current mitigation practices and community support?

Methodology

Q: How should we access developers' perceptions of threats/mitigations?

1. XR developers are difficult to recruit
2. Threat demonstration is required
3. Need in-depth understanding for analysis, not high-level descriptions

Methodology

Q: How should we access developers' perceptions of threats/mitigations?

1. XR developers are difficult to recruit
2. Threat demonstration is required
3. Need in-depth understanding for analysis, not high-level descriptions

Study Design: Semi-Structured interviews (approx. 90 mins).

- Explain threats and ask in-depth follow-up questions

Semi-Structured Interview

50+ XR S&P papers

Collect demographic information

Developer background and practices in XR development

Developers' perspectives on S&P threats in XR

Developers' perspectives on tools in XR and responsibilities

Future challenges in XR S&P and feedback on our study

Prestudy Survey

Background Questions

Threat in XR

Mitigation and Best Practices

Feedback

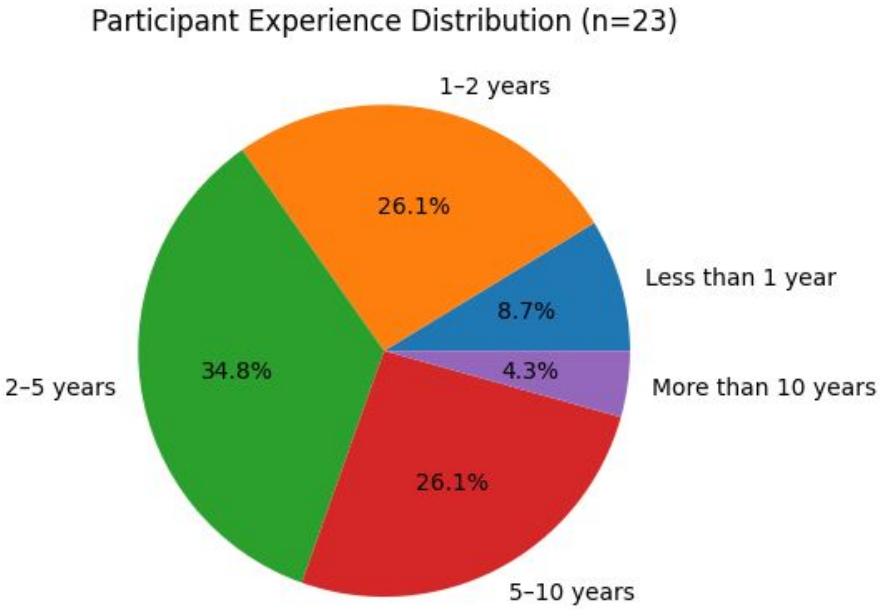
Qualtrics Survey (10 Minutes)

Semi-structured Interview (90 Minutes)

Participant Overview

Participants recruited from LinkedIn:

- **N = 23** professional XR developers.
  a. Have published at least one XR application
  b. Currently working in XR development
- **15 Types** of XR applications
- Spanning **12** different XR platforms



RQ1 Findings: Awareness Gaps

Limited Awareness

- Identified only **2.1/9.0** XR-sensitive data types (before the demonstration).
- **4.8/9.0** types were collected in their apps (after demonstration).
- Identified only **0.9/7.0** attacks (before the demonstration).
- **3.7/7.0** attacks were **new to them** (after demonstration).

Developers agreed that this knowledge is important for S&P in XR development

RQ1 Findings: Why Does Data Leakage Occur in XR?

- Development misoperations due to technological immaturity
- Immersive interaction reduces awareness of data leakage
  - Need better notification systems

When it comes to the AR/VR set of things. It's still a **maturing technology** where a lot of freelancers, small agencies, people from all sizes of teams, and backgrounds are coming in. So, as I mentioned, no matter what the protocols we bring in, <u>at the end of the day. It's a responsibility of the developing team.</u>

- P13 on XR immaturity

RQ1 Findings: Why Are Attacks More Critical in XR?

- Immersive technology is personal; negative experiences can harm the industry.
- Encouraging user-generated content in XR may enable adversaries.
- Mitigations in XR applications remain challenging.

That's actually one of the things we tried to prevent when we're doing an event on Horizon, because the user can just jump on stage or show models or images that's not great.

- P4 on user-generated content risks

I think it's difficult to moderate. You probably aren't able to do real-time voice detection.

- P6 on mitigation challenges

RQ1 Findings: Developer Misconceptions

- Overreliance on user responsibility
- Underestimation of XR attacks

I think it's too easy to just take off the headset. It's not like I'm holding you hostage or anything.

- P8 on user responsibility

You can't really gain anything from this. Aside from harming people, basically like you can't earn money from it right?

- P6 on attack motivation

RQ2 Findings: Perceptions of Current Mitigations

- Existing mitigations may sacrifice utility in exchange for S&P (e.g., camera blockage)
- The app review process lacks consideration of S&P
- Documents for XR S&P are impractical or outdated

> They don’t provide any access to the camera and information at all, it really limits what you can develop as a developer.
>
> - P6 on S&P vs. utility trade-offs

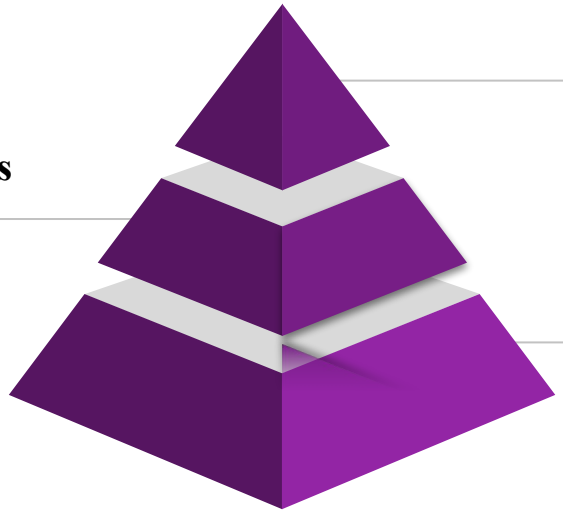
RQ2 Findings: Support Needed from the XR Community

Technical

1. **Moderation tools.**
2. **Notification systems**

Communication

1. **Communication channels**
2. **Knowledge sharing**



Strategic

1. **Economic and utility concerns.**
2. **Best XR S&P practices.**

Security is definitely something we want to consider sooner rather than later, but it's essential to have more cost-effective solutions.

- P7 on needed support

Why XR Threats Evade Current Security Practices

- **Developer awareness lags behind XR evolution**
  - Rapid evolution makes it difficult to recognize emerging threat patterns
- **Threats often blend with UX issues**
  - XR S&P issues often look like UX or hardware issues, making them easy to overlook
- **Diffuse ownership in XR ecosystems**
  - No clear roles or guidelines for who should address emerging XR threats

Why XR Threats Evade Current Security Practices

- **Developer awareness lags behind XR evolution**
  - Rapid evolution makes it difficult to recognize emerging threat patterns
- **Threats often blend with UX issues**
  - XR S&P issues often look like UX or hardware issues, making them easy to overlook
- **Diffuse ownership in XR ecosystems**
  - No clear roles or guidelines for who should address emerging XR threats

Beyond discovering new threats/solutions, XR S&P often fails when risks go unrecognized and deprioritized. Researchers should act as community advocates by actively sharing knowledge to foster robust best practices and actionable security policies.

Thank You