

# Trusted Inter-Reality Infrastructure: Building Trust within Entities (Digest)

Akira Kanaoka  
Toho University

Takuro Yonezawa  
Nagoya University

## Abstract

As the development of information technology extends reality from physical space to cyber virtual space and people's use of the Internet increases rapidly, providing connectivity between different realities and promoting mutual collaboration is essential for the stability of the next generation of society. In this paper, we focus on establishing trust among user entities in the cyber virtual space opened up by the evolution of information technology. Specific approaches to establishing a Trusted Inter-Reality infrastructure are discussed. In addition to the fact that trust in the components of each reality is indispensable for providing safe and secure services and that by-design security and privacy protection are necessary, we also indicated the importance of research and development to clarify the requirements for a new trust infrastructure, taking into account the attributes of users in the extended realities. Specifically, it will be necessary to discuss the identity assurance of user entities, authentication, and application of cryptographic methods. Through the "Trusted Inter-Reality Infrastructure" provided by the establishment of trust described in this paper, we aim to provide safe and secure services in the next generation and contribute to the establishment of trust for user entities in the extended realities.

## 1 Introduction

The evolution of information technology has expanded our reality from physical to cyber virtual spaces. Last year, for the first time, the average time spent on the Internet (including SNS (Social Networking Service) and online games) ex-

ceeded that of watching television<sup>1</sup>. This shift signifies the transition of society's focus towards virtual spaces. However, this expansion brings risks such as social fragmentation due to selective exposure. Therefore, providing connectivity between different realities and enhancing opportunities for mutual understanding and emergence is crucial for a stable next-generation society. VR (Virtual Reality), exemplified by digital twins and the metaverse, provides new communication and workspaces free from physical constraints and is significant in the age of integrated digital and physical spaces. Future VR developments, including continuous biometric data input via wearables, will heighten security and privacy risks. Consequently, it is essential to trust the elements that constitute each reality and ensure security and privacy protection from the design stage.

Our research project, the Internet of Realities<sup>2</sup>, supported by JST CREST, aims to establish information infrastructure technology that integrates various physical and virtual spaces and their entities securely. We clarify the requirements for a new trust infrastructure, considering the nature of spaces and user attributes in extended realities, and develop methods for constructing and connecting diverse modalities of reality. This includes not only technological extensions in information security, such as identity assurance, authentication, and adaptive cryptographic methods but also medical verification of physical and mental impacts through wearable devices. The integrated infrastructure is named the Trusted Inter-Reality Infrastructure, and we evaluate its convenience, safety, and availability through demonstration experiments. This paper discusses new trust requirements for connecting diverse realities and constructing various services, indicating future research directions.

This is an English-language digest of a paper originally published in Journal of Information Processing (JIP) in Japanese [13].

Copyright is held by the author/owner. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2024.  
August 11–13, 2024, Philadelphia, PA, United States.

<sup>1</sup><https://www.soumu.go.jp/johotsusintokei/whitepaper/r03.html>

<sup>2</sup><https://internet-of-realities.org>

## 2 Necessity of a Trusted Inter-Reality Framework

### 2.1 Connecting Realities

Defining reality precisely is challenging. For convenience, we define reality as a certain space-time and its entities, considering technologies such as VR, AR, MR, collectively known as XR, and digital twins. Connected realities are states where elements of one reality can interact with those of another, synchronously or asynchronously. Examples include synchronous movement of physical furniture based on VR space [27] or blocking sensory input in physical space while a user concentrates in VR [9].

Advanced IoT technologies integrate sophisticated sensing and actuating functions into living spaces, allowing entire spaces and their entities to be incorporated into digital twins or mapped to different information spaces (metaverse). While extending current computing environments, these connections bring unique security and privacy threats due to spatial and temporal expansion and sophisticated functions.

### 2.2 Towards Framework Construction

To connect realities, an interoperable infrastructure is required, both semantically and syntactically. User management must allow participation in other realities under real names, pseudonyms, or anonymously, ensuring identity protection. In environments with constant wearable device use, strict design regarding biometric information linkage, data disclosure, and storage is essential. Interaction with other users must consider malicious entities or programs. When spaces become fully interactive, actions in one space can affect all users, necessitating measures to prevent unexpected or dangerous controls.

These considerations are part of connecting realities. Our project concurrently researches specific methodologies, such as constructing semantically synchronized virtual spaces [12] and connecting immersive realities [30]. From these activities, we extract and organize requirements and design the architecture. We aim to build a framework that applies appropriate trust to each layer, enabling secure reality connections and services, ultimately achieving the Trusted Inter-Reality Infrastructure.

## 3 Threats to Trust

### 3.1 Security and Privacy Threats Similar to Existing Computing Environments

In XR, multiple academic studies on security and privacy are being conducted. There are not many studies broadly considering XR technologies, devices, computing environments, and virtual spaces. We explain elements mentioned in papers by Abraham et al. [1].

Threats in XR can be divided into those similar to existing computing environments and those unique to XR. We first organize threats similar to existing environments.

#### 3.1.1 Unauthorized Information Acquisition

In XR, user or service provider information can be maliciously acquired, similar to existing computing environments. Examples include keylogger technology recording interface actions without user permission and the threat of unintended information leakage due to space recording.

Communication eavesdropping is also a threat, as XR devices communicate similarly to PCs and smartphones. Improperly protected communication can be intercepted between devices and servers or by the OS layer or other apps.

Security and privacy measures for XR device OSs are essential. Standalone VR and MR devices use unique OSs, presenting risks such as unintended data access and user information acquisition [8, 14, 17, 25]. Smart glasses providing AR often use smartphone OSs, offering similar security and privacy levels.

#### 3.1.2 User Impersonation and Authentication Bypass

User authentication for XR devices (local and remote) is necessary, similar to PCs and smartphones. New authentication threats may arise due to the specificity of input devices.

#### 3.1.3 Unauthorized Manipulation

Unauthorized control is a threat in XR, similar to PCs and smartphones. In XR, users recognize only part of the space, making unauthorized operations less noticeable.

#### 3.1.4 Impersonation of Services, Content, and Other Users (Phishing)

In XR, malicious entities can impersonate legitimate services, content, or other users, posing a phishing threat. The high immersion and easy mimicry of digital data make phishing a significant threat.

#### 3.1.5 Denial of Service (DoS) Attacks

XR services are likely provided via the Internet, similar to current services, making them vulnerable to DoS attacks. Specific data formats can also stop OSs or applications.

### 3.2 Security and Privacy Threats Unique to XR

We previously discussed threats similar to existing environments and now examine unique XR threats.

### 3.2.1 User Perception Manipulation

XR provides unique visual and auditory experiences, significantly impacting users. High immersion makes it easier to guide user cognition compared to PC or smartphone services. Threats include unauthorized acquisition of private or confidential information in physical spaces using AR or MR devices and inducing erroneous operations.

### 3.2.2 Security and Privacy of Bystanders

Various sensors in XR devices can collect information about users around the device user, violating bystanders' privacy. Studies on AR by Roesner and Kohno [15, 16, 23, 24, 24] indicate similar threats for other technologies.

### 3.2.3 Impact on Users in the Physical Space due to Shocks in the Virtual Space

High immersion increases the user's awareness of physical space. Events in virtual spaces can flow back and impact users physically or psychologically. Visual manipulations can impair vision, and feedback affecting senses other than sight and hearing can strongly impact users without prior recognition or experience.

## 3.3 Awareness of XR Device Users

User awareness of XR threats and risks is crucial. XR devices collect and analyze surrounding information more extensively than PCs and smartphones, but users are not fully aware of how this impacts security and privacy.

Developers creating applications and services using XR devices must also consider whether extensive data collection is necessary and appropriate.

## 4 Concept of Trust

### 4.1 Extending the Three Elements of Security

Inter-Reality can expand user experiences and create new value, but appropriate trust between spaces and entities is crucial. Entities refer to users and objects in XR-built service spaces and applications. Inter-Reality requires connections and interactions among users and objects, making trust crucial.

For example, in a digital twin, physical objects are expanded into the virtual space, requiring assurance that the data reflects the physical space. Security measures are needed to prevent data tampering. Inter-Reality must consider how entities interact across realities.

Security elements (CIA: Confidentiality, Integrity, Availability) must be expanded in Inter-Reality. An entity in one reality may appear as a different entity in another. Ensuring

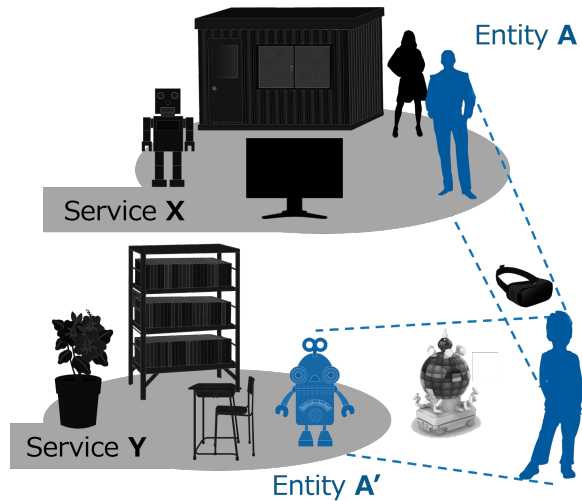


Figure 1: Different entity usage for each service

that these entities are linked to the same individual is crucial, differing from conventional integrity.

Interactions with entities in Inter-Reality require expanding "Integrity" to "Consistency", including existentiality and reflexivity. Building a trust infrastructure based on the new three elements (CCA: Confidentiality, Consistency, Availability) can establish trust in Inter-Reality. Achieving this requires research and development, focusing on "bidirectional entity consistency assurance."

## 4.2 Technologies Crucial for Ensuring Integrity

### 4.2.1 Assurance Levels of Entities

Trust in Inter-Reality requires varying assurance levels for entities across realities. For example, a public service A using VR for administrative services may require strict identity verification, while a social service B with email authentication allows free object creation. Interactions must consider these assurance levels (Figure 2).

Digital identity assurance can reference NIST SP 800-63-3. Defining assurance levels for users and objects, and determining mutual use, provides appropriate trust in Inter-Reality.

### 4.2.2 Techniques for Verifying Assurance Levels

Defining assurance levels is insufficient; verification technologies are required. These include electronic signatures and hardware security technologies for reliable assurances. Verification may involve checking certificates, user identity, and object authenticity.

Combining adaptive authentication methods and verification through probes of surrounding objects can provide as-

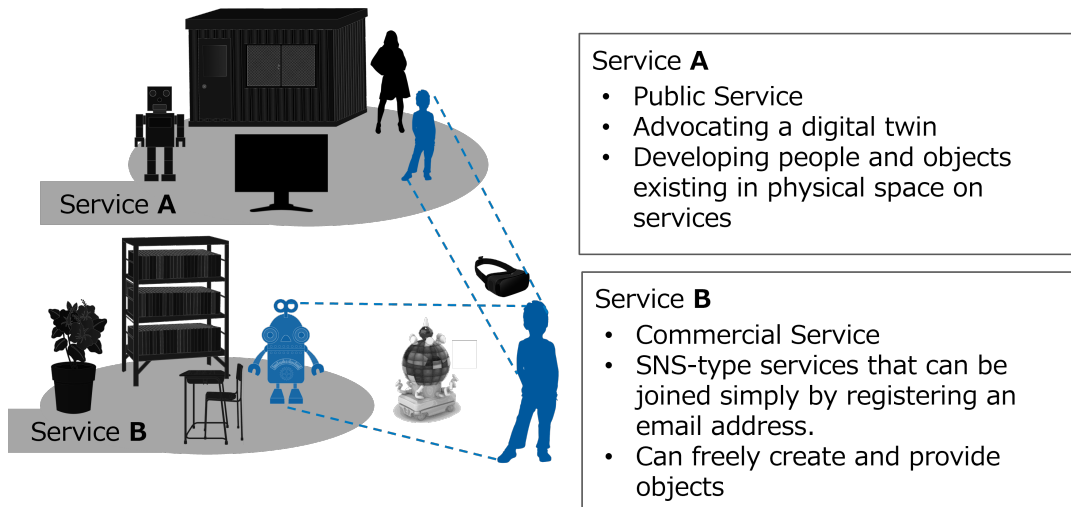


Figure 2: Services with different assurance levels

assurance. An overview of necessary technologies is shown in Figure 3.

## 5 Current State of Research on Security, Privacy, and Trust

Academic approaches to security and privacy in VR/AR/MR began around 2014 [7, 23]. Representative achievements include the work by Roesner and Kohno, focusing on privacy in AR glasses [15, 16, 24].

For example, Ruth et al. [24] focused on secure and private content sharing in multi-user AR environments, designing a corresponding module. Previous studies targeted AR devices used alone, but Ruth et al. addressed multi-user AR environments, indicating further research importance for Inter-Reality.

Research has become more active since the 2020s. IEEE VR 2022 and USENIX Security 2023 featured sessions on security and digital reality. However, most papers focused on XR-specific threats similar to existing computing environments.

Research on threats similar to existing environments includes unauthorized sensor and data access [8, 14, 17, 25], side-channel attacks estimating text input and user behavior [2, 10, 17, 19, 31], and user identification and authentication [20, 26, 32]. These studies clarify risks but do not consider trust structures for spaces and entities. Establishing trust in Inter-Reality can mitigate these risks.

Research on XR-specific security and privacy includes user operation investigations [3, 4, 28], security display proposals [29], shoulder surfing attacks [18], comprehensive surveys [5, 11, 21, 22], and user perception examinations by experts [6]. Cheng et al. [4] represents advanced XR-specific security research, but further experiments are needed as XR

technologies spread.

As XR technologies spread, research on XR security will become more active. However, sufficient discussions on trust for individual realities are lacking, and interactions between realities have not been addressed. Establishing a trust structure in Inter-Reality can efficiently address XR security and privacy issues.

## 6 Conclusion

Ensuring safe, secure, and free services requires trust in spaces and user entities constituting each reality, and implementing security and privacy protection from the design stage. This paper discussed trust concepts maintaining entity consistency, security, and privacy in extended realities. Threats undermining trust were divided into those similar to existing environments and new threats. Based on these considerations, security elements were expanded, and technologies important for ensuring consistency were discussed. Future research aims to design human-centered security architectures with usable security technologies, medical verification of impacts through wearable devices, and assumptions of actual usage and operation forms. The infrastructure, named Trusted Inter-Reality Infrastructure, is evaluated for convenience, safety, and availability through demonstration experiments.

## Acknowledgments

This work was supported by JST, CREST Grant Number JP-MJCR22M4, Japan

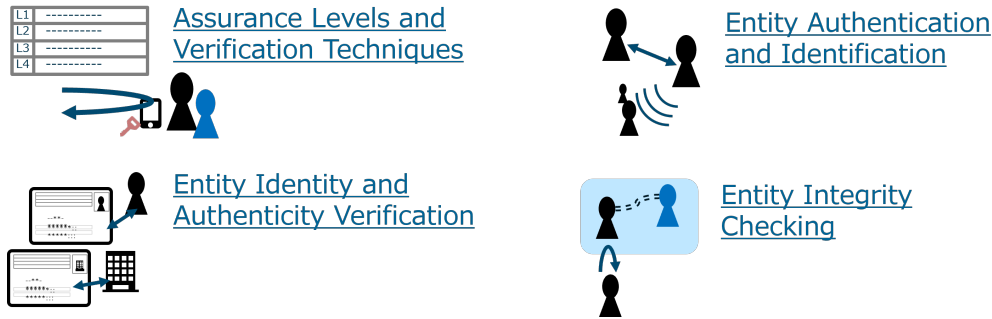


Figure 3: Overview of technologies required to ensure Consistency

## References

- [1] Melvin Abraham, Pejman Saeghe, Mark McGill, and Mohamed Khamis. Implications of xr on privacy, security and behaviour: Insights from experts. In *Nordic Human-Computer Interaction Conference, NordiCHI '22*, New York, NY, USA, 2022. Association for Computing Machinery.
- [2] Abdullah Al Arafat, Zhishan Guo, and Amro Awad. Vrspy: A side-channel attack on virtual key-logging in vr headsets. In *2021 IEEE Virtual Reality and 3D User Interfaces (VR)*, pages 564–572, 2021.
- [3] Elise Bonnail, Wen-Jie Tseng, Mark McGill, Eric Lecolinet, Samuel Huron, and Jan Gugenheimer. Memory manipulations in extended reality. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems, CHI '23*, New York, NY, USA, 2023. Association for Computing Machinery.
- [4] Kaiming Cheng, Jeffery F. Tian, Tadayoshi Kohno, and Franziska Roesner. Exploring user reactions and mental models towards perceptual manipulation attacks in mixed reality. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 911–928, Anaheim, CA, August 2023. USENIX Association.
- [5] Jaybie A. De Guzman, Kanchana Thilakarathna, and Aruna Seneviratne. Security and privacy approaches in mixed reality: A literature survey. *ACM Comput. Surv.*, 52(6), oct 2019.
- [6] Elmira Deldari, Diana Freed, Julio Poveda, and Yaxing Yao. An investigation of teenager experiences in social virtual reality from teenagers’, parents’, and bystanders’ perspectives. In *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*, pages 1–17, Anaheim, CA, August 2023. USENIX Association.
- [7] Tamara Denning, Zakariya Dehlawi, and Tadayoshi Kohno. In situ with bystanders of augmented reality glasses: Perspectives on recording and privacy-mediating technologies. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '14*, page 2377–2386, New York, NY, USA, 2014. Association for Computing Machinery.
- [8] Habiba Farrukh, Reham Mohamed, Aniket Nare, Antonio Bianchi, and Z. Berkay Celik. LocIn: Inferring semantic location from spatial maps in mixed reality. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 877–894, Anaheim, CA, August 2023. USENIX Association.
- [9] Andreas Rene Fender and Christian Holz. Causality-preserving asynchronous reality. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems, CHI '22*, New York, NY, USA, 2022. Association for Computing Machinery.
- [10] Sindhu Reddy Kalathur Gopal, Diksha Shukla, James David Wheelock, and Nitesh Saxena. Hidden reality: Caution, your hand gesture inputs in the immersive virtual world are visible to all! In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 859–876, Anaheim, CA, August 2023. USENIX Association.
- [11] Yan Huang, Yi Joy Li, and Zhipeng Cai. Security and privacy in metaverse: A comprehensive survey. *Big Data Mining and Analytics*, 6(2):234–247, 2023.
- [12] Kazuma Inokuchi, Jin Nakazato, Manabu Tsukada, and Hiroshi Esaki. Semantic digital twin for interoperability and comprehensive management of data assets. In *IEEE International Conference on Metaverse Computing, Networking and Applications (IEEE MetaCom 2023)*, Kyoto, Japan, 2023.
- [13] Akira Kanaoka and Takuro Yonezawa. Trusted inter-reality infrastructure: Building trust within entities. *Journal of Information Processing (JIP) written in Japanese*, 64(12):1590–1598, dec 2023.

- [14] Yoonsang Kim, Sanket Goutam, Amir Rahmati, and Arie Kaufman. Erebus: Access control for augmented reality systems. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 929–946, Anaheim, CA, August 2023. USENIX Association.
- [15] Kiron Lebeck, Kimberly Ruth, Tadayoshi Kohno, and Franziska Roesner. Securing augmented reality output. In *2017 IEEE Symposium on Security and Privacy (SP)*, pages 320–337, 2017.
- [16] Kiron Lebeck, Kimberly Ruth, Tadayoshi Kohno, and Franziska Roesner. Towards security and privacy for multi-user augmented reality: Foundations with end users. In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 392–408, 2018.
- [17] Shiqing Luo, Xinyu Hu, and Zhisheng Yan. Holologger: Keystroke inference on mixed reality head mounted displays. In *2022 IEEE Conference on Virtual Reality and 3D User Interfaces (VR)*, pages 445–454, 2022.
- [18] Florian Mathis, Joseph O’Hagan, Mohamed Khamis, and Kami Vaniea. Virtual reality observations: Using virtual reality to augment lab-based shoulder surfing research. In *2022 IEEE Conference on Virtual Reality and 3D User Interfaces (VR)*, pages 291–300, 2022.
- [19] Ülkü Meteriz-Yıldiran, Necip Fazıl Yıldiran, Amro Awad, and David Mohaisen. A keylogging inference attack on air-tapping keyboards in virtual environments. In *2022 IEEE Conference on Virtual Reality and 3D User Interfaces (VR)*, pages 765–774, 2022.
- [20] Vivek Nair, Wenbo Guo, Justus Mattern, Rui Wang, James F. O’Brien, Louis Rosenberg, and Dawn Song. Unique identification of 50,000+ virtual reality users from head & hand motion data. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 895–910, Anaheim, CA, August 2023. USENIX Association.
- [21] Blessing Odeleye, George Loukas, Ryan Heartfield, Georgia Sakellari, Emmanouil Panaousis, and Fotios Spyridonis. Virtually secure: A taxonomic assessment of cybersecurity challenges in virtual reality environments. *Computers & Security*, 124:102951, 2023.
- [22] Sara Qamar, Zahid Anwar, and Mehreen Afzal. A systematic threat analysis and defense strategies for the metaverse and extended reality systems. *Computers & Security*, 128:103127, 2023.
- [23] Franziska Roesner, Tadayoshi Kohno, and David Molnar. Security and privacy for augmented reality systems. *Commun. ACM*, 57(4):88–96, apr 2014.
- [24] Kimberly Ruth, Tadayoshi Kohno, and Franziska Roesner. Secure Multi-User content sharing for augmented reality applications. In *28th USENIX Security Symposium (USENIX Security 19)*, pages 141–158, Santa Clara, CA, August 2019. USENIX Association.
- [25] Carter Slocum, Yicheng Zhang, Nael Abu-Ghazaleh, and Jiasi Chen. Going through the motions: AR/VR keylogging from user head motions. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 159–174, Anaheim, CA, August 2023. USENIX Association.
- [26] Sophie Stephenson, Bijeeta Pal, Stephen Fan, Earlene Fernandes, Yuhang Zhao, and Rahul Chatterjee. Sok: Authentication in augmented and virtual reality. In *2022 IEEE Symposium on Security and Privacy (SP)*, pages 267–284, 2022.
- [27] Ryo Suzuki, Hooman Hedayati, Clement Zheng, James L. Bohn, Daniel Szafir, Ellen Yi-Luen Do, Mark D. Gross, and Daniel Leithinger. Roomshift: Room-scale dynamic haptics for vr with furniture-moving swarm robots. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, CHI ’20*, page 1–11. Association for Computing Machinery, 2020.
- [28] Samaikya Valluripally, Aniket Gulhane, Khaza Anuarul Hoque, and Prasad Calyam. Modeling and defense of social virtual reality attacks inducing cybersickness. *IEEE Transactions on Dependable and Secure Computing*, 19(6):4127–4144, 2022.
- [29] Maximiliane Windl, Anna Scheidle, Ceenu George, and Sven Mayer. Investigating security indicators for hyper-linking within the metaverse. In *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*, pages 605–620, Anaheim, CA, August 2023. USENIX Association.
- [30] Takuro Yonezawa, Nozomi Hayashida, Kenta Urano, Johannes Przybilla, Yutaro Kyono, and Nobuo Kawaguchi. Metapo: A robotic meta portal for interspace communication. In *ACM SIGGRAPH 2022 Posters, SIGGRAPH ’22*, New York, NY, USA, 2022. Association for Computing Machinery.
- [31] Yicheng Zhang, Carter Slocum, Jiasi Chen, and Nael Abu-Ghazaleh. It’s all in your head(set): Side-channel attacks on AR/VR systems. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 3979–3996, Anaheim, CA, August 2023. USENIX Association.
- [32] Huadi Zhu, Mingyan Xiao, Demoria Sherman, and Ming Li. Soundlock: A novel user authentication scheme for VR devices using auditory-pupillary response. In *30th Annual Network and Distributed System Security*

*Symposium, NDSS 2023, San Diego, California, USA,  
February 27 - March 3, 2023. The Internet Society, 2023.*