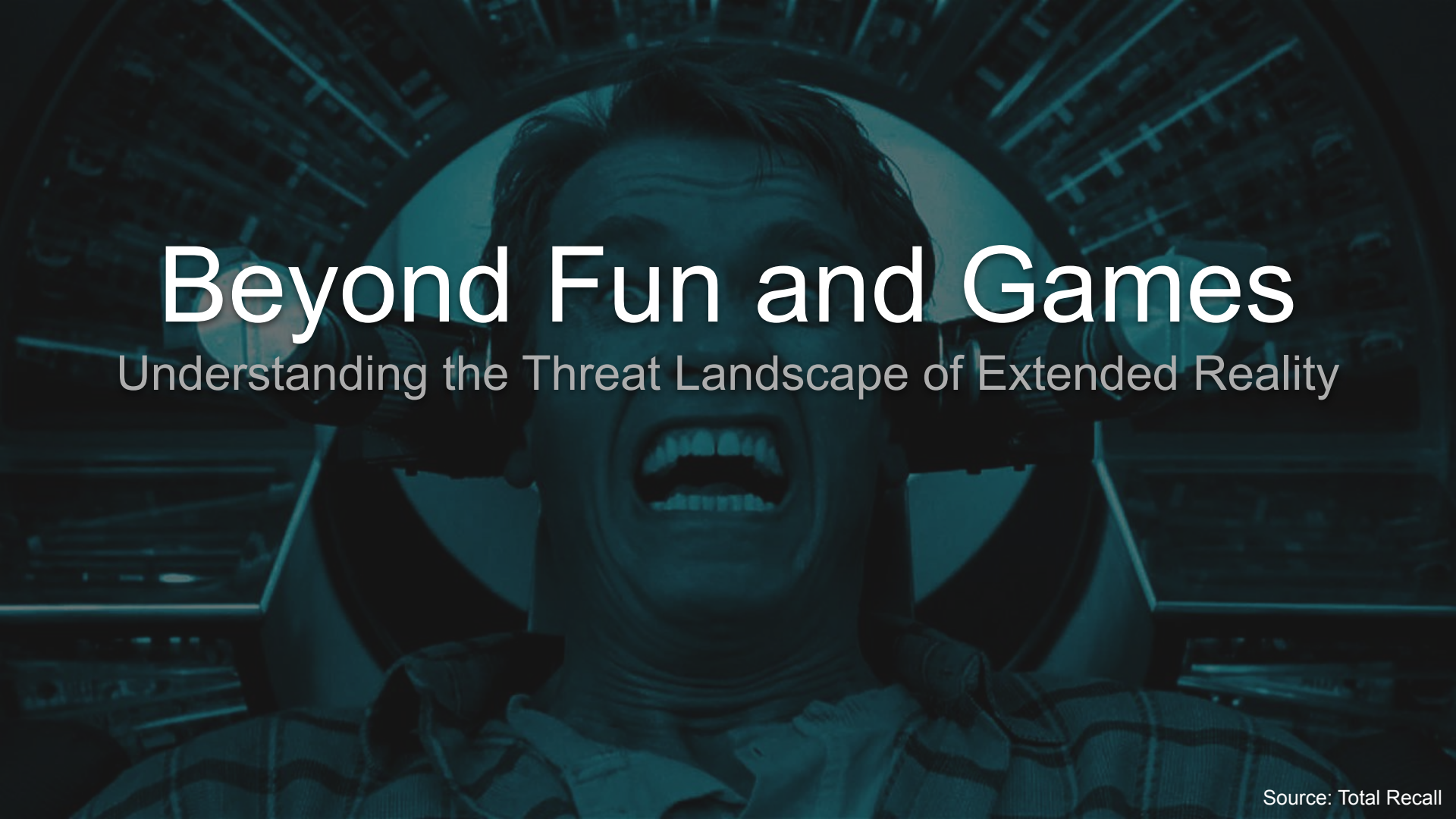
Beyond Fun and Games

Understanding the Threat Landscape of Extended Reality



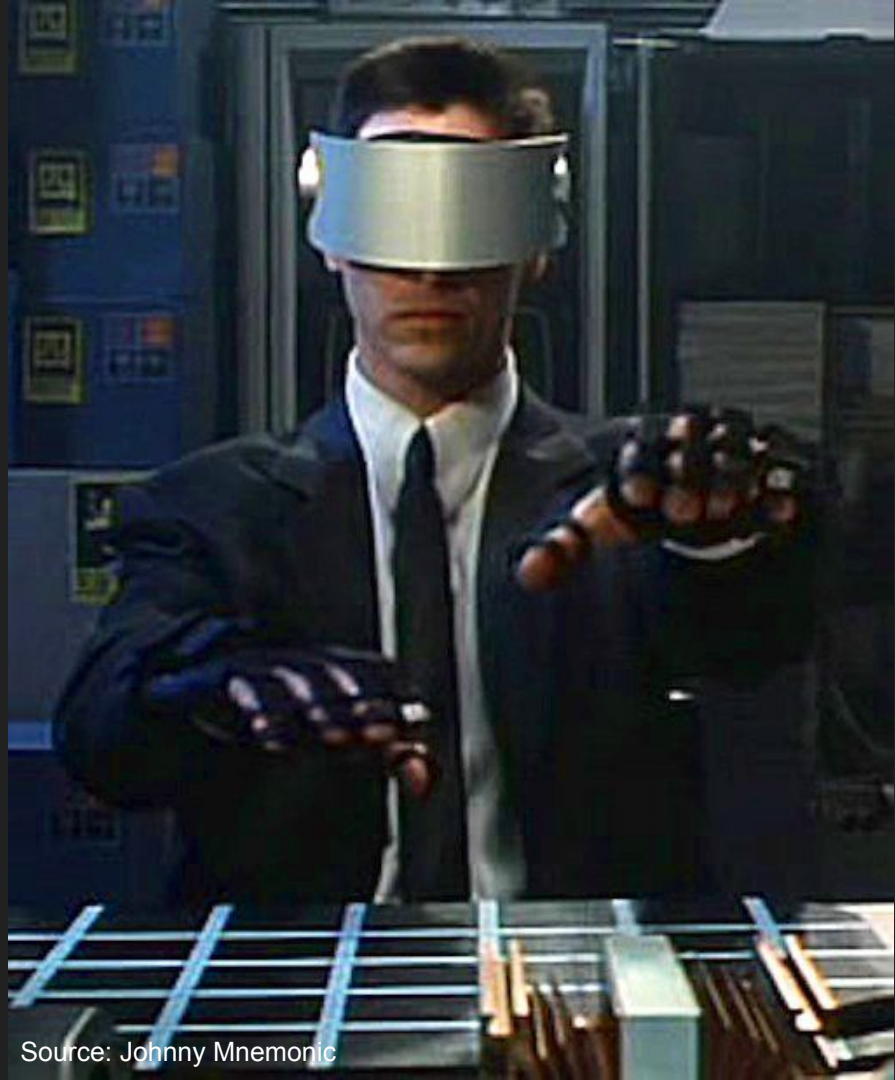
Source: Total Recall

Who am I?

- Security Architect
- Hacker / early adopter / tech evangelist
- Tinkering with '*puters* since age of 6
- Working in tech for 10+ years

Overview

- What is XR
- Common XR Devices
- Technical Overview
- Key Threats
- Security Controls

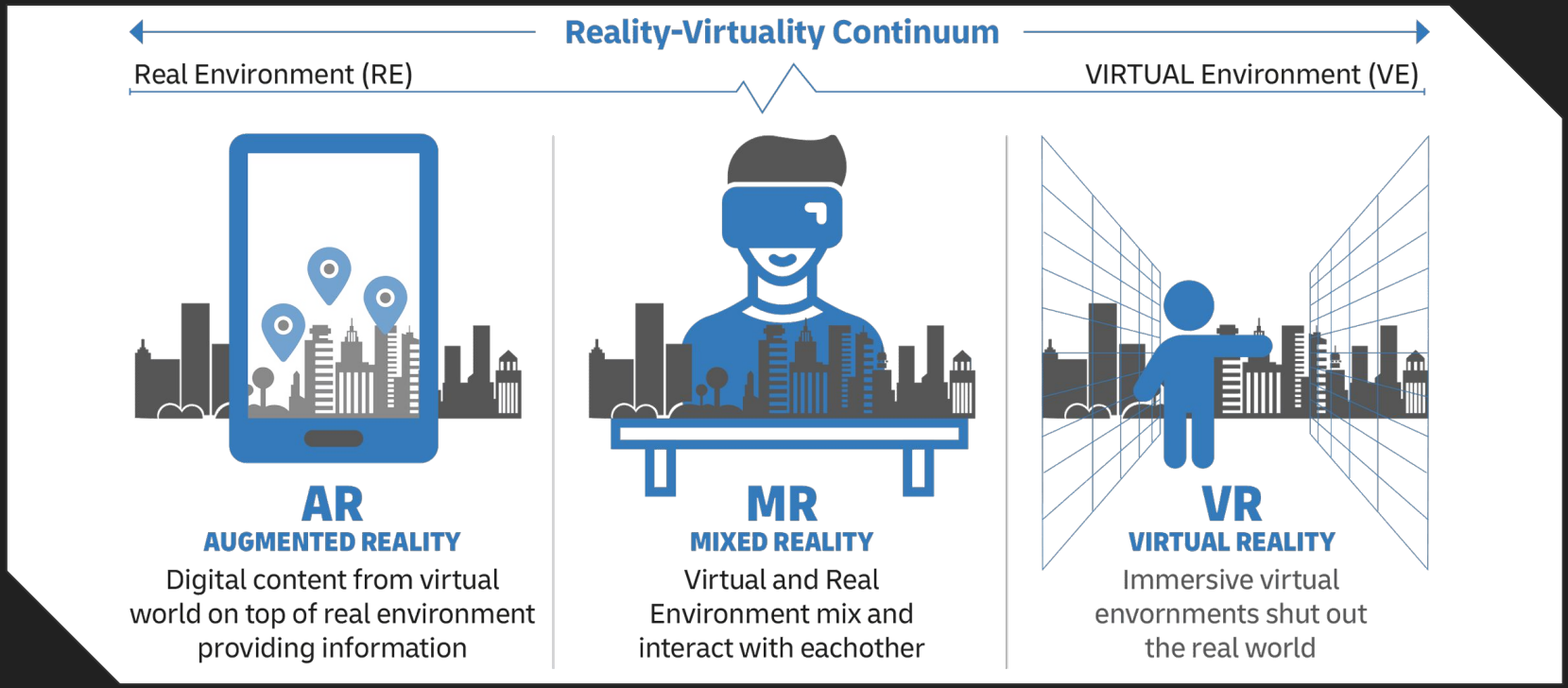


Source: Johnny Mnemonic

Why this talk?

- XR is the future (not the present)
- Media approaches XR mostly from a consumer perspective (gaming)
- Security/safety is a key component in XR
- Complex cyber-physical systems with very sensitive access
- Raise awareness about this exciting area

AR/MR/VR/XR?



Source: DHL

https://www.dhl.com/de-en/home/insights-and-innovation/thought-leadership/trend-reports/augmented-and-extended-reality.html

XR Devices

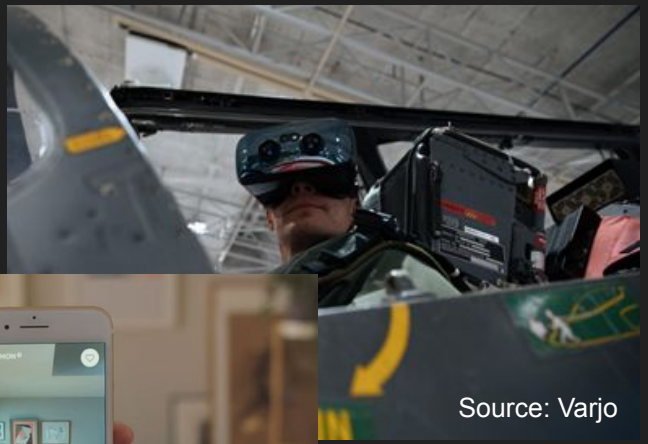
Augmented Reality

Virtual Reality

Sources: Apple, Sony, Mechdyne, Microsoft, Apple, Meta,

Use Cases

- Education and Training
- Retail & Entertainment
- Healthcare
- Real Estate
- Manufacturing and R&D
- Remote Support


Source: Varjo

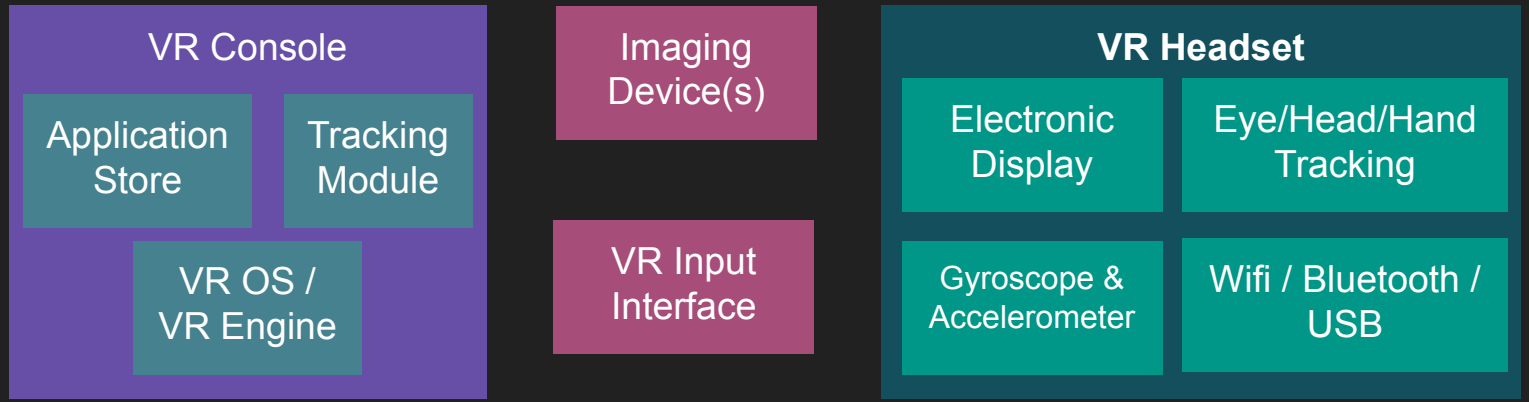

Source: IKEA


Source: MediView

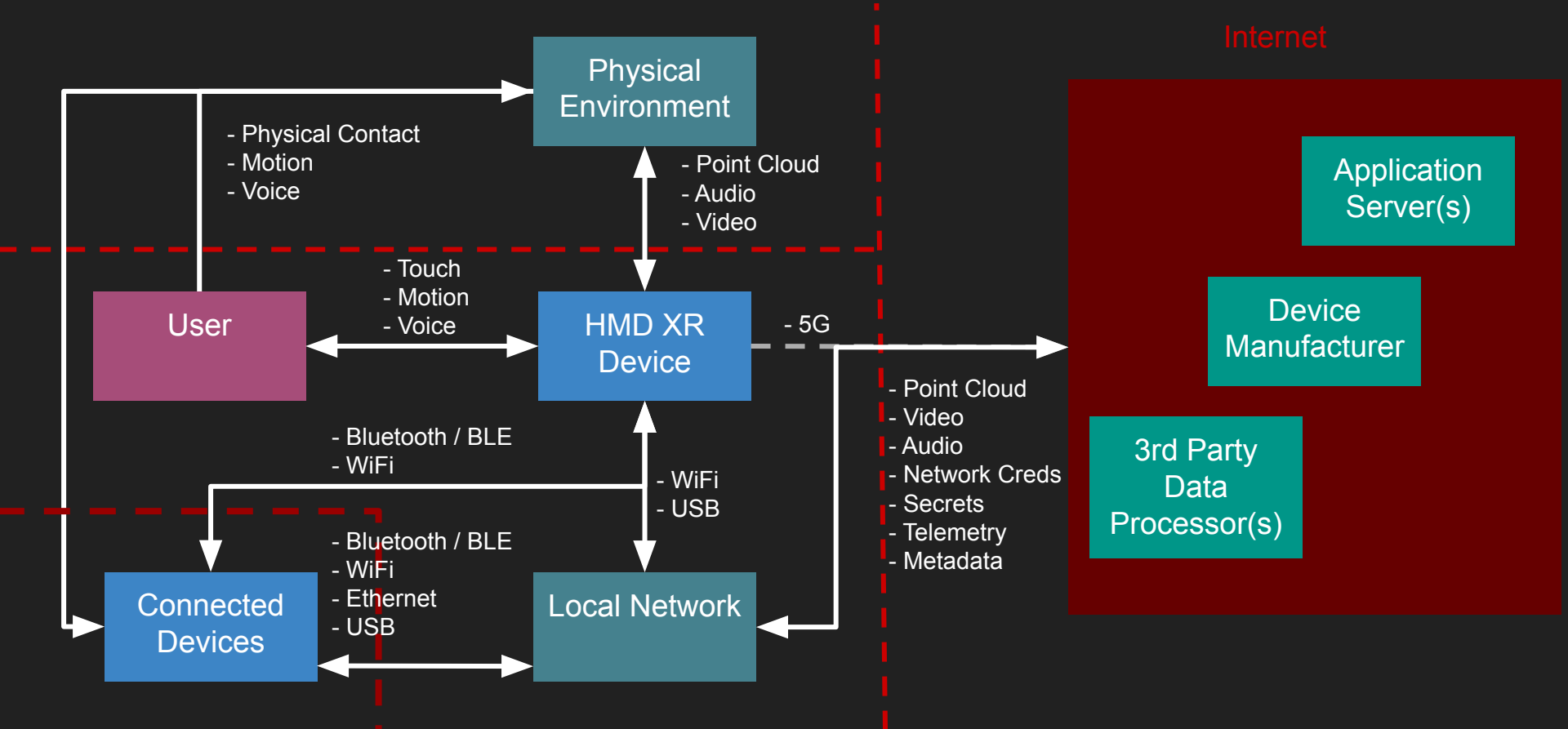
HMD Device Model

- HMDs are mobile devices on steroids
- ARM based SoC (Qualcomm or M2 for Vision Pro)
- Fork of commonly used OS (AOSP / Windows Holographic / visionOS)
- Attack surface: Apps, USB, cameras, sensors, WiFi, Bluetooth, 5G
- App development with Unreal, Unity, OpenXR

Loosely based on Oculus Autofocus Virtual Reality Patent



HMD XR Environment



Notable Threats

- Physical damage to user and/or environment
- Altering user senses to trick them into taking action
- User/Environment surveillance
- Weaker security controls
- Massive privacy risks
- Data leakage
- Other common security problems
  - Application/OS vulnerabilities
  - Supply chain risks

Security Controls

- Built-in OS controls and hardening
- FIDO2, biometric authentication, PIN
- Mobile device management
- Locked bootloader, code signing
- Little information about Vision Pro
- **Hololens 2 is King!** 👑

Source: Ghost in the Shell

Recommended Reading

- Microsoft Hololens 2 - Deploying Hololens 2
- META Engineering Blog - Meta Quest 2: Defense through offense
- Abraham, Melvin & Saeghe, Pejman & Mcgill, Mark & Khamis, Mohamed. (2022) - Implications of XR on Privacy, Security and Behaviour: Insights from Experts


Slides available on Github
Thank you
for your cooperation!
Source: Robocop: Rogue City