Securing BYOD in ZTA: Insights & Applications

Ian Bento

CyberSecurity Service Provider Internship Program, ITS 293, Fall 2023

Advisors: Dr. Curtis Arnold, Chief Scientist – Cyber, & Dr. Robert Adamove, Sr. Associate, (Core4ce)

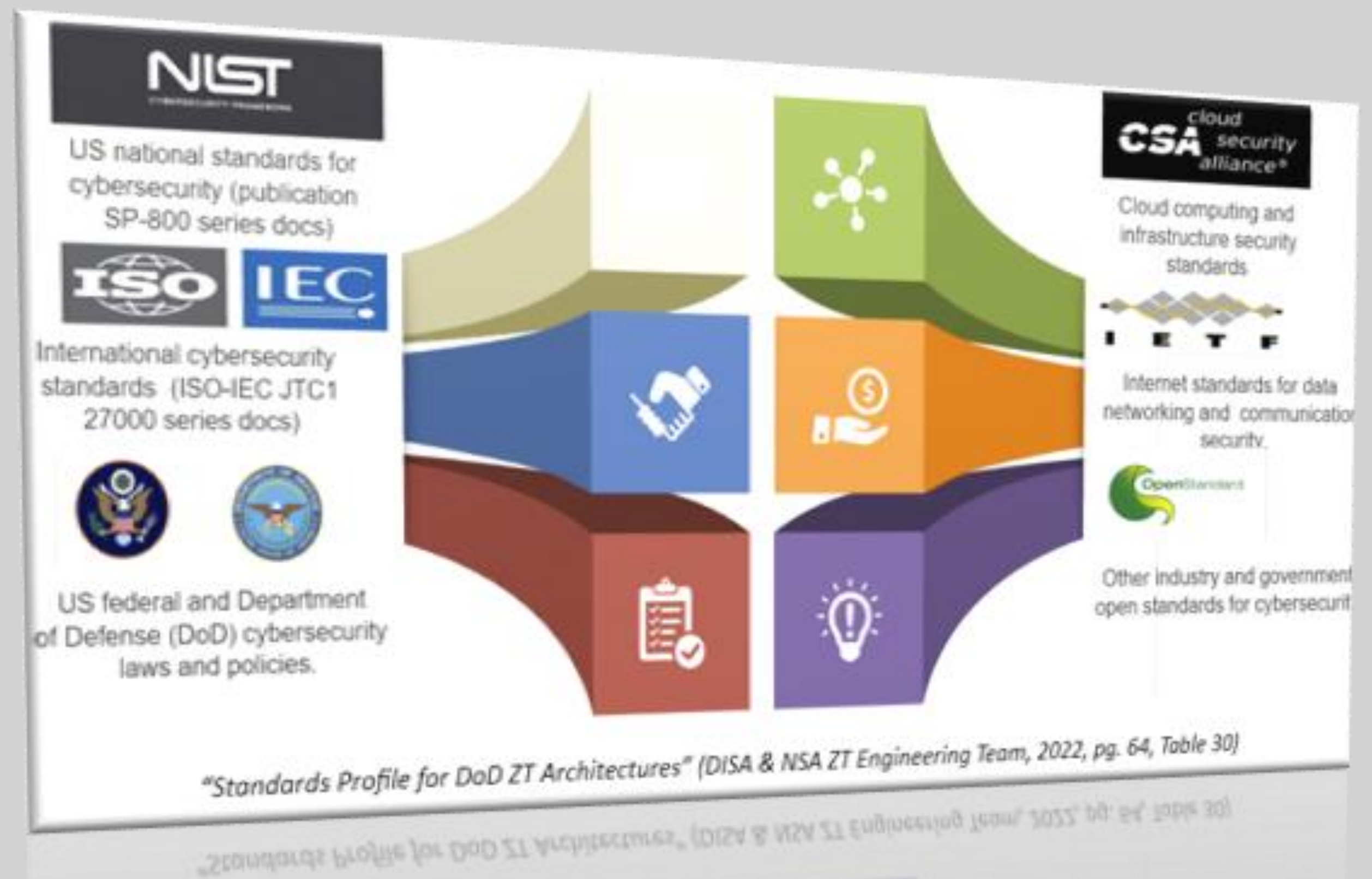
Problem Statement:

Recent high-profile cyber threats coupled with the COVID-19 pandemic have accelerated the meeting of two practices: Bring-your-own-device and zero-trust architecture. The problem is the sparse nature of the literature regarding securing BYOD devices in a ZT environment.

Purpose:

This study was poised to uncover various methods of securing mobile devices and the core components of ZTA in the face of mobile botnets and other threats with the goal of benefiting from both practices with little compromise.

Besides the primary objective, byproducts such as critical success factors (CSFs) of successful ZT implementations, ZT posture assessments, IoT solutions, interoperability potential, and privacy-preserving techniques were identified.



NIST
US national standards for cybersecurity (publication SP-800 series docs)
ISO
IEC
International cybersecurity standards (ISO-IEC JTC1 27000 series docs)
US federal and Department of Defense (DoD) cybersecurity laws and policies.
CSA cloud security alliance
Cloud computing and infrastructure security standards
IETF
Internet standards for data networking and communication security.
OpenStandard
Other industry and government open standards for cybersecurit

"Standards Profile for DoD ZT Architectures" (DISA & NSA ZT Engineering Team, 2022, pg. 64, Table 30)

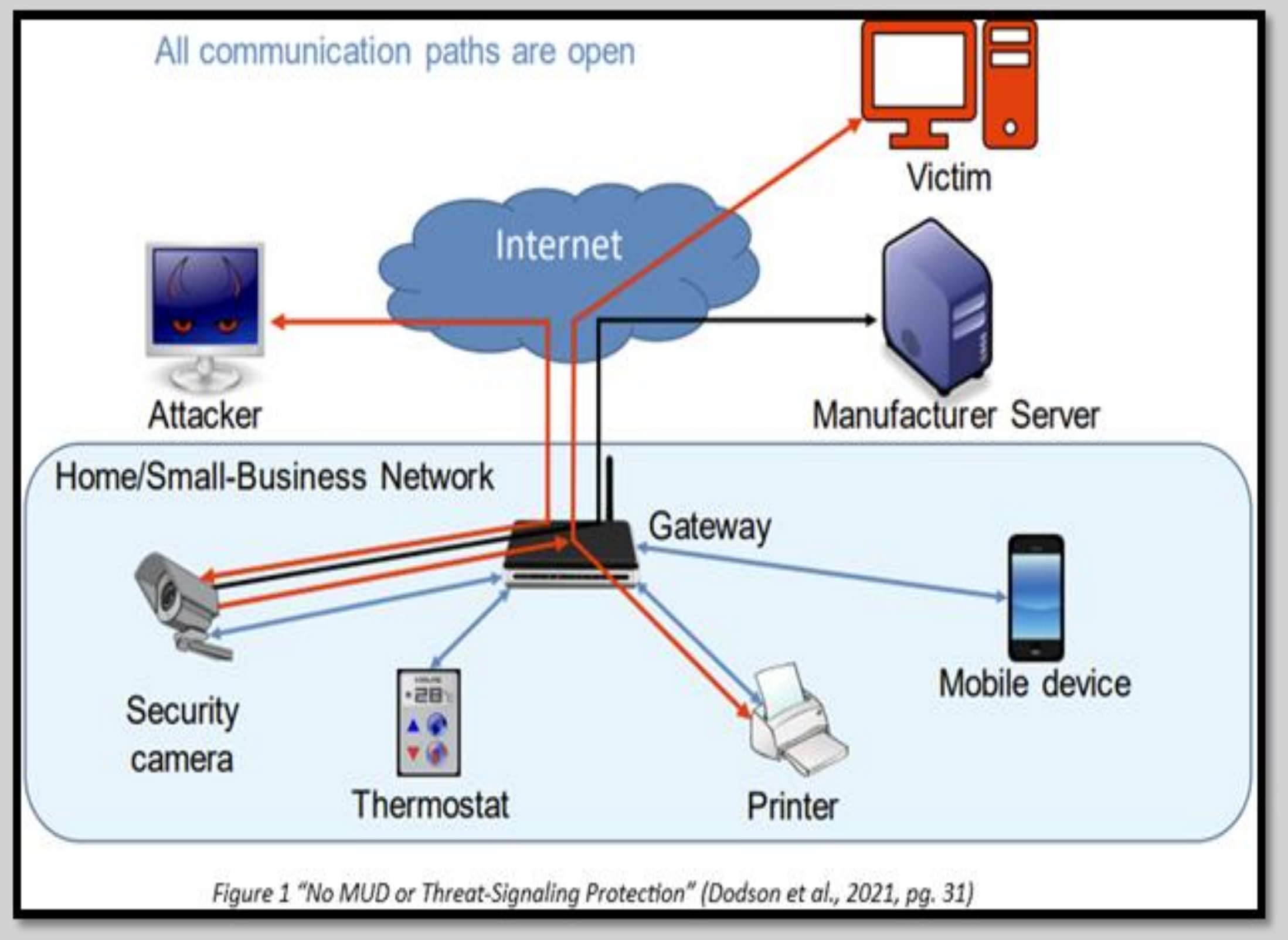


Figure 1 "No MUD or Threat-Signaling Protection" (Dodson et al., 2021, pg. 31)

Approach:

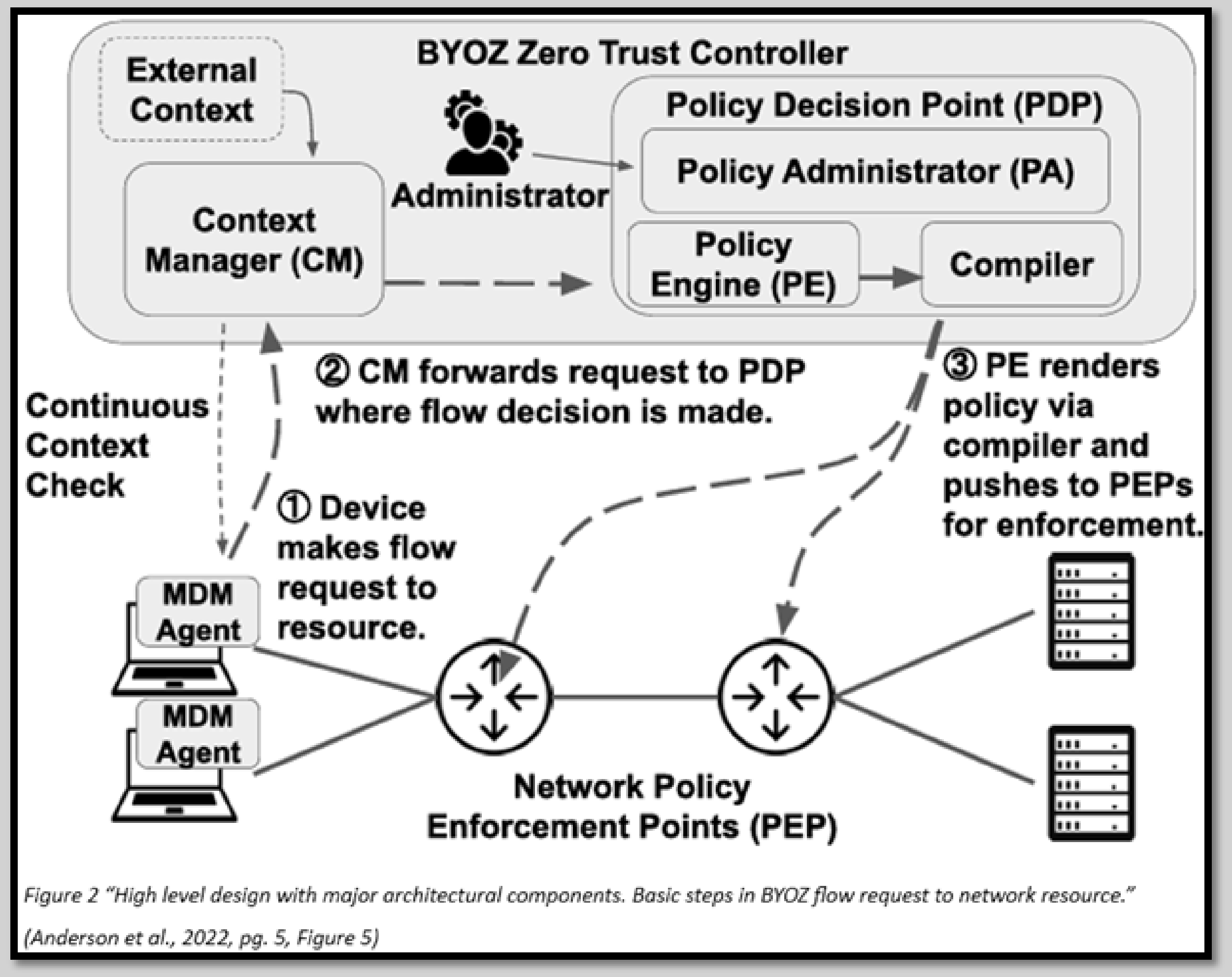
BYOD adoption has been observed as early as 2009 with Intel's strategy to embrace employee-owned devices and the following year manifested ZTA through research by Kindervag (2010) on building security into the network. As stated previously, the rapid adoption of both practices has been further accelerated by external factors influencing their intersection.

This mixed-method, nonexperimental research was conducted entirely through accessing online academic libraries. Beginning with Google Scholar, the searches lead to IEEE Xplore, ScienceDirect, and various tech websites. Obtained were NIST Special Publications, official reports, and a range of peer-reviewed research papers.

INFORMATION & COMPUTER SCIENCES
UNIVERSITY *of* HAWAIʻI *at* MĀNOA

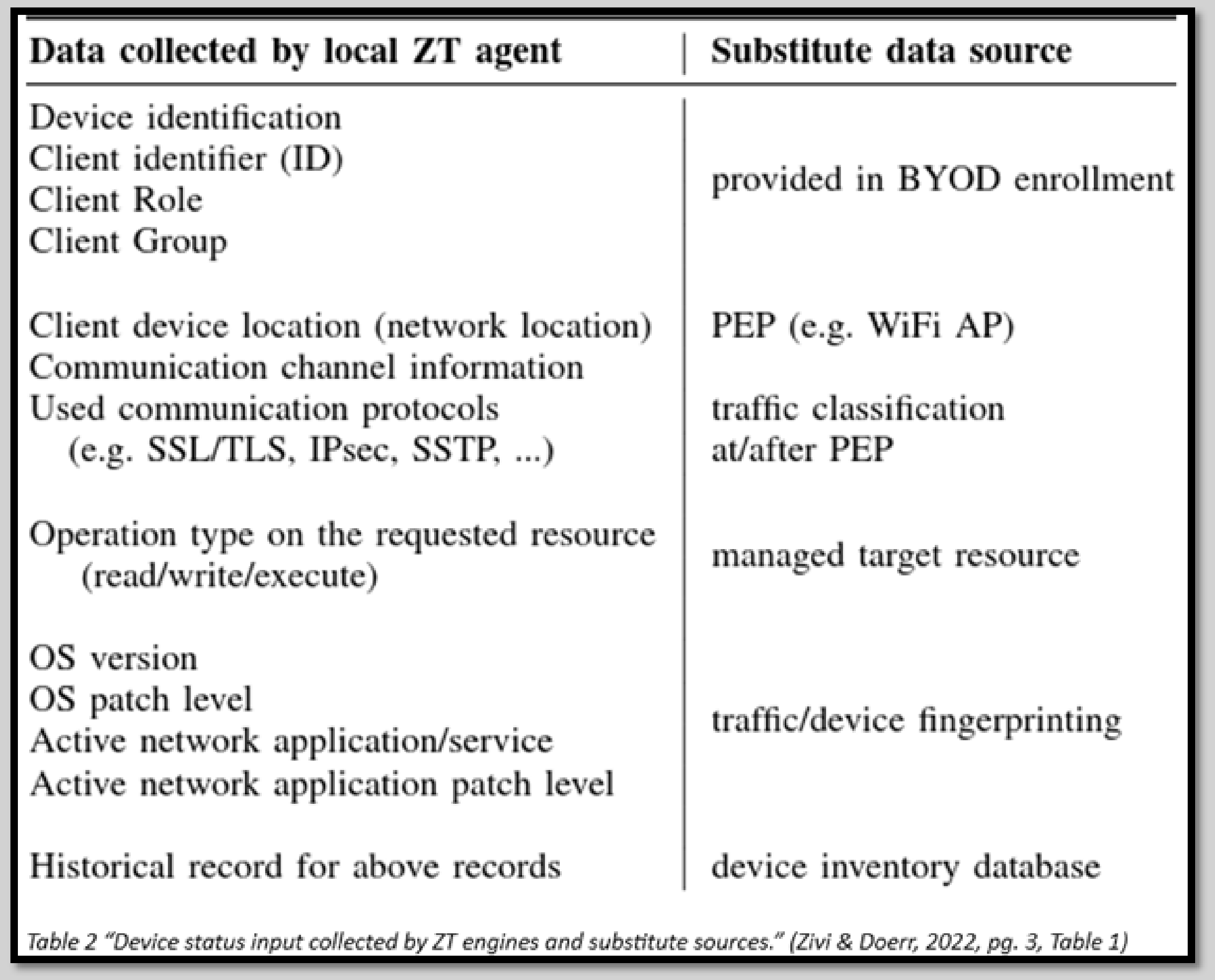
Discussion & Conclusion:

No single device/technology will produce a ZT Framework; ZT is a holistic approach, leveraging several different technologies. This assumption demonstrates that there are multiple approaches. Below are two such options: (Left) BYOZ architecture and policy language, and (Right) Agent-less, network inspection for BYOD.



BYOZ Zero Trust Controller
External Context
Administrator
Policy Decision Point (PDP)
Policy Administrator (PA)
Context Manager (CM)
Policy Engine (PE)
Compiler
Continuous Context Check
② CM forwards request to PDP where flow decision is made.
③ PE renders policy via compiler and pushes to PEPs for enforcement.
① Device makes flow request to resource.
MDM Agent
MDM Agent
Network Policy Enforcement Points (PEP)

Figure 2 "High level design with major architectural components. Basic steps in BYOZ flow request to network resource." (Anderson et al., 2022, pg. 5, Figure 5)



Data collected by local ZT agent	Substitute data source
Device identification Client identifier (ID) Client Role Client Group	provided in BYOD enrollment
Client device location (network location)	PEP (e.g. WiFi AP)
Communication channel information Used communication protocols (e.g. SSL/TLS, IPsec, SSTP, ...)	traffic classification at/after PEP
Operation type on the requested resource (read/write/execute)	managed target resource
OS version OS patch level Active network application/service Active network application patch level	traffic/device fingerprinting
Historical record for above records	device inventory database

Table 2 "Device status input collected by ZT engines and substitute sources." (Zivi & Doerr, 2022, pg. 3, Table 1)

- ➢BYOD can be deployed with (BYOZ build) or without an agent (Network inspection).
  - ✓ Privacy concerns are mitigated through an agent-less deployment.
  - ✓ SDN represents interoperability and micro-segmentation potential with BYOZ.
  - ✓ IoT interaction with compromised devices can be mitigated with MUD.
- ➢Android devices represent a broadened, botnet-capable attack surface.
  - ✓Addressed with static code analysis, mobile firewalls, and security updates.
  - ✓Regular training may reduce overall risk, produce transparency and accountability
- ➢CSFs identified in 2023 are available to align ZT endeavors.
  - ✓Zero trust cybersecurity maturity reports are available based on CSF assessment.

Path Forward:

Future works on this topic can include building upon policy enforcement languages and producing an open standard, testing existing underdeveloped fingerprinting techniques in various ZTA models to mature those aspects, and conducting a comprehensive technology survey to alleviate vendor lock-in and align organizations with the technology required for a successful ZTA deployment.

References:

Anderson, J., Huang, Q., Cheng, L., & Hu, H. (2022). BYOZ: Protecting BYOD Through Zero Trust Network Security.

Zivi, A., & Doerr, C. (2022) Adding Zero Trust in BYOD Environments through Network Inspection

UNCLASSIFIED/APPROVED FOR PUBLIC RELEASE