

The Physical Blind Spot of Enterprise Cybersecurity: Zero-Trust Policy Failures, Peripheral Injection, and Hardware-Rooted Defenses in Byod Ecosystems

Aman

Security Analyst, V4 IT Services, Parramatta, Sydney, Australia.

Email: amank5793@gmail.com

How to cite : Aman , The Physical Blind Spot of Enterprise Cybersecurity: Zero-Trust Policy Failures, Peripheral Injection, and Hardware-Rooted Defenses in Byod Ecosystems, *Revista Bioetica* Oct,05,2026.

DOI: <https://doi.org/10.5281/zenodo.23182993>

Received: 10-09-2026

Accepted: 25-09-2026

Published: 05-10-2026

ABSTRACT

Bring Your Own Device (BYOD) enterprise models are increasingly based on logical abstraction layers, including containerization and mobile device management, and assume that the physical host is 100% provenance-checked. This study examines the enterprise's exposure and vulnerability when unmanaged consumer hardware faces physical tampering, peripheral exploits, and environmental attacks. Structurally, we build a five-vector taxonomy for physical attack surfaces, create a structural comparative control matrix with enterprise-hardened baselines, and establish a four-level mathematical progression model of physical-to-logical lateral movement. The empirical evaluations show that exposure to an unhardened personal endpoint increases the likelihood of corporate network penetration by a factor of 53.6%, or an acute 900x increase over the enterprise-managed baseline (0.06%). Additionally, OS hypervisors and host endpoint telemetry do not handle hardware implants and DMA attacks, allowing them to evade security audit logs. This paper suggests a multi-layered defense architecture that combines cryptographic remote attestation, kernel-level bus gating, micro-virtualization with transparent memory encryption, and hardware-bound FIDO2 authentication tokens, backed by pragmatic and blame-free incident reporting. Incorporating zero-trust principles into a hardware anchor helps enterprises maintain the mobility dividends without exposing corporate networks to physical threats.

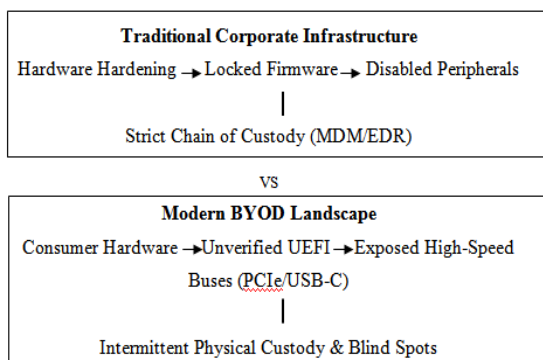
Keywords: Bring Your Own Device (BYOD), Direct Memory Access (DMA) Attacks, Hardware Root of Trust (RoT), Physical Endpoint Security, Zero Trust Architecture (ZTA)

I. INTRODUCTION

Bring Your Own Device (BYOD) is an innovative productivity trend that was once a niche option and has become an integral part of enterprise architectures (EAs) worldwide (Sokolov & Skladannyi, 2025, pp. 136–156). The trend of enterprise information technology becoming consumerized (Harris et al., 2012) has accelerated in the era of remote and hybrid working practices. Better operational outcomes have been achieved, from reduced capital outlay on hardware purchases to faster hardware turnaround to employee satisfaction with comfortable, more familiar computing environments (Disterer & Kleiner, 2013, pp. 43–53).

However, the traditional enterprise security model relied on perimeter security and hardware ownership. In classic enterprise asset management, the corporation bought, hardened, maintained, and physically managed the entire life cycle of the physical host (Majeed, 2026, pp. 1– 8). Cryptographic modules (including discrete Trusted Platform Modules and Hardware Security Modules), unused external interfaces (including

Thunderbolt, PCIe, USB, and FireWire), and chassis intrusion detection sensors were provisioned under corporate root Certificate Authorities (CAs), with the chassis interfaces cryptographically locked with administrative passwords, and the chassis intrusion detection sensors alerting systems engineers when an external interface was connected or accessed without their permission (Webb et al., 2025, pp. 1–7). In contrast, a BYOD model's decentralized nature makes these endpoints subject to peripheral manipulation and firmware exploits that could allow unauthorized access to secure network areas (Vengara, 2026, pp. 875–877).



BYOD policies disrupt this fundamental physical perimeter. Today, enterprise mobility management (EMM) assumes almost complete use of logical abstraction layers:

- Mobile Device Management (MDM) profiles,
- Mobile Application Management (MAM) sandboxes,
- Secure Enclave-based containerization,
- Conditional Access Virtual Private Networks (VPNs), and
- Endpoint Detection and Response (EDR) agents.

These controls add host operating system (OS) isolation. However, this is a new, simple security challenge: software cannot be trusted if its host machine is compromised. Underlying hardware can collapse if an adversary gains physical access to a personal endpoint (or if the endpoint connects to a compromised hardware peripheral in an unmonitored area). Mobile devices are carried daily and exposed to a wide variety of physical environments, making them especially susceptible to advanced side-channel attacks that can evade these software-based security mechanisms (Spreitzer et al., 2017, pp. 465–488).

They can neutralize hypervisor-protected memory and exploit microarchitectural flaws without generating the typical EDR audit log entries, as is the case with physical attacks. A staff member may work on a public computer, laptop, tablet, or smartphone while commuting via public transit, in a cafe, in a shared house, or in an unsecured conference room. If not in company, there is the possibility of physical tampering, unauthorized accessory connection, or shoulder surfing. Additionally, the use of personal devices that may not have the same level of security as the devices being controlled can be detrimental, as these devices are not equipped with the same context-aware security mechanisms that enable access requests to be authenticated, even in potentially insecure environments (Hwaitat et al., 2024, pp. 125–157).

This paper addresses the physical security blind spot of BYOD policies in the following ways:

1. Methodical analysis of the vulnerabilities in personal endpoints that could be exploited in business tasks—especially in hardware, peripheral, and spatial contexts.
2. Building a Taxonomy of the enterprise's granular attack surface for vector transitions from physical to logical enterprise intranets.
3. Comparative study of physical controls in place in the enterprise vs. BYOD hardware profiles.
4. Crafting a defense-in-depth architectural blueprint with hardware-based cryptographic verification along with physical access gating using zero-trust policies that can be enforced to prevent unmanaged hardware exposure, and human governance policies.

II. THEORETICAL FOUNDATIONS AND THREAT LANDSCAPE

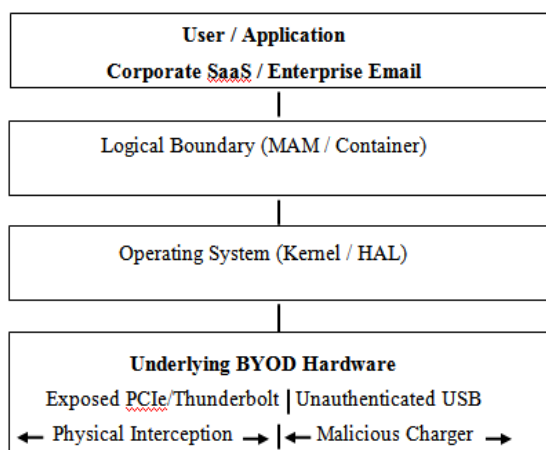
The Convergence of Consumer Electronics and Enterprise Trust

Modern personal computing systems use I/O bus standards for high-speed communication between peripherals, which are not physically separated. New protocols like Thunderbolt 3/4, USB4, and PCIe externalization allow direct connections to the memory controller and the physical system bus, enabling faster data transfers, high-resolution display output, and external GPUs. This unintended connectivity can enable a direct memory access attack, which a malicious physical device can carry out to access the operating system's security abstraction layer and sensitive information in system memory.

With a traditional enterprise deployment, Direct Memory Access (DMA) protection features, such as kernel-level Input-Output Memory Management Unit (IOMMU) configuration, DMA protection registries, and hardware peripheral allow-lists, are enforced globally. Personal consumer devices, by contrast, ship with different hardware revisions, BIOS implementations, and operating system builds. It is common for personal users to fiddle with the UEFI configuration to enable peripheral drivers that are not normally supported or to install dual-boot configurations or to boost performance, all of which essentially bypass the protections that vendors install. Such misconfigurations, combined with the widespread availability of high-speed ports, enable easy connectivity and, thus, a powerful avenue for firmware exploitation and unauthorized memory manipulation (Markettos et al., 2019, pp. 1–15; Vengara, 2026, pp. 875–877).

If this kind of device is software containerized and plugged into corporate enterprise applications, the logical layer assumes that the kernel host ring 0 and

hardware abstraction layer (HAL) are safe from compromise. This does not align with basic security engineering principles. The system-level interconnect fabric provides no physical separation between untrusted components and memory, allowing a malicious peripheral to impersonate a trusted peripheral (Nabeel et al., 2020, pp. 1611–1625).



As shown above, an attacker attacking the underlying BYOD hardware can break through to memory structures under the operating system and thus nullify logical security mechanisms.

Socio-Technical Drivers of Physical End-User Vulnerability

Bring Your Own Device models are supported by user needs for mobility in the workspace, often before strict physical security measures such as limiting ports or locking the BIOS. As a result, end-users focus on getting things working and often sacrifice security for convenience by connecting peripherals that masquerade as trusted

devices to exploit system memory through DMA-based memory exploitation (Markettos et al., 2019, pp. 1–15).

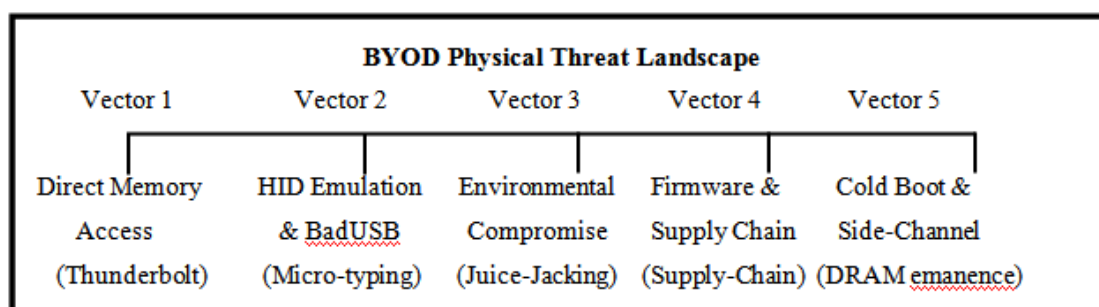
The dynamics of end-user behavior add to physical endpoint vulnerabilities. Organizational assets under the corporate umbrella have ongoing tracking, stringent loss-reporting requirements, and asset-reclamation procedures. In contrast, the BYOD endpoints are part of an ad hoc, informal operating environment:

- **"Borrowing":** Many times, staff allow third parties, family members, and friends to access their personal device.
- **Accessory Contamination:** Users purchase third-party (low-cost) power adapters, hubs, cables, and external docks from non-trustworthy user supply chains.
- **Delayed Incident Telemetry:** Users are not reporting lost or physically damaged personal devices for fear that their personal data will be deleted, the device will be looked at by administration, or that they will get into trouble.

These socio-technical factors hinder incident response teams by revoking session tokens or by requiring immediate remote wipes of affected devices.

Taxonomy of Physical Threat Vectors

This paper presents a framework for analyzing physical attacks on BYOD endpoints, categorizing them into five attack vectors: Hardware/Direct Memory Access (DMA), Malicious Peripherals and HID Emulation, Physical Interception and Environmental Compromise, Supply Chain and Firmware Injection, and Cold Boot/Side-Channel Extractions.



Vector 1: Direct Memory Access (DMA) Exploits

High-throughput interconnects are exposed to the outside and reveal the internal system memory architecture. The Thunderbolt, USB4, and external PCIe ports communicate directly with the system memory bus via direct memory access channels.

These high-speed interfaces are the targets of adversaries who can install malicious peripheral hardware that accesses the physical memory of the machine or injects arbitrary code into the kernel, thus avoiding OS-level security abstractions (Heartfield & Loukas, 2015, pp. 1–39; Stajnirod et al., 2021, pp. 259–269).

- **Mechanism of Exploitation:** An adversary that has a fleeting physical presence (such as a PCIe screamer, an FPGA board using PCILeech, or a rogue peripheral). If the target platform does not implement strict IOMMU protection or if the IOMMU translation tables have dynamic hypervisor-level bypass vulnerabilities, then the device completely ignores CPU privilege checks. In addition, many contemporary systems prioritize fast data transfer over fine-grained bandwidth tracking, which is necessary to identify the origin of each DMA operation. Moreover, current systems emphasize high throughput data transfers over fine-grained monitoring of the bandwidth of individual DMA operations (Tian et al., 2018).
- **BYOD Impact:** The attacker executes memory injection into ring 0 kernel space, overwrites authentication flags (e.g., `msv1_0.dll` authentication routines on Windows or PAM verification arrays on UNIX-like platforms), and turns off endpoint EDR processes. Sensitive corporate keys, TLS session tokens, VPN private certificates, and MAM sandbox decryption keys are extracted in cleartext directly from DRAM. Advanced threats can also exploit this DMA functionality to enable bit flipping during Rowhammer timing attacks, a direct way to cause corruption, gain higher-level privileges, or break kernel-level protections using carefully crafted PCIe request patterns (Dumitru et al., 2025; Rothwell, 2017).
- **Defense Evasion:** No telemetry is generated during the activation phase of this exploit by the host-based EDR tool or by the software-based DLP mechanism. Since they run under the kernel's radar, or below it, they can effectively defeat software-defined security controls (Or-Meir et al., 2019, pp. 1–48).

Vector 2: Human Interface Device (HID) Emulation & BadUSB

The Universal Serial Bus (USB) architecture is based on default trust paradigms. If there is an endpoint peripheral claiming a Human Interface Device (HID) (keyboard or pointing device), then the operating system accepts the input commands without demanding any additional cryptographic authentication. This forms the basis of a hidden trust exploited by badUSB implants, which can issue keyboard/mouse commands to the computer using scripts to perform shell commands in automatic mode, changing the lock state of the interactive session (Rothwell, 2017).

This is known as a hardware attack tool (e.g., USB Rubber Ducky, Bash Bunny). Malicious

microcontrollers (MG cables) are hidden in regular flash drives, adapters, or charging cables. When the unit is connected, it transmits keystrokes at machine rates (more than 1,000 characters per minute). This enables the implant to quickly run PowerShell or terminal scripts, enabling unauthorized payload installation or privilege escalation without manual involvement (Wang & Hsu, 2024).

BYOD Impact: The script runs a modified version of the command line and then modifies the DNS settings, loads memory-resident reverse shells in memory, and exports cached corporate OAuth authorization tokens to an external command-and-control (C2) server within 5-7 seconds. An example of such a physical-to-logical bridge is hardware-based keystroke injection attacks that can manipulate cryptographic protocols, as "Mallory" bypasses software-defined security (Harrison et al., 2024, pp. 1-24).

The Personal Device Multiplier: Group Policies are often configured on corporate laptops to block new HID enumerations and USB mass storage and/or to limit the use of USB class identifiers. Organizations rarely enforce them on BYOD devices, as users routinely connect mice, game controllers, audio interfaces, and digital cameras, meaning organizations cannot block USB endpoints globally on the devices they use. Moreover, operating systems assume the HID will act as a legitimate user, allowing peripherals to carry out actions that bypass normal security measures (Nicho & Sabry, 2022).

Vector 3: Physical Interception and Environmental Exploits

BYOD devices roam uncontrolled public environments and therefore present capture vectors for endpoints.

- **Juice-Jacking and Rogue Power Delivery:** Public charging stations (such as in transit hubs or hotels) include power delivery along with working USB data pins. Rogue charging hubs use the physical connection to trigger an automatic MTP (Media Transfer Protocol) or ADB (Android Debug Bridge) handshake, and try to exploit files silently or deliver payloads via a vulnerability. Moreover, in such environments, if the cable or adapters contain malicious circuits, man-in-the-middle attacks can steal information and/or record keystrokes (Soubhagyalakshmi & Reddy, 2022, pp. 696-703).
- **Malicious Docking Stations:** Hot-desking and shared workspaces can pose a threat of malicious docking stations. An untrusted hub with internal memory-capture logic or a hardware man-in-the-middle (MitM) controller

can tap video signals and capture unencrypted corporate presentations, customer records, and credentials shown on the monitor. Furthermore, these stations may provide continuous access and set up an alternative communications path that can circumvent enterprise perimeter security defenses to exfiltrate sensitive data in real time.

- **Visual Eavesdropping and Shoulder Surfing:** High-resolution directional optical capture devices readily collect credentials, two-factor authentication SMS prompts, and proprietary documents from personal devices, whether they are operated with or without physical polarization filters, in transit or third-party facilities. Furthermore, the human nature of these environments often makes social engineering easier, given that employees trust seemingly legitimate public infrastructure – and attackers can use this trust to deliver advanced persistent threats (APTs) (Javaheri et al., 2023).

Vector 4: Supply Chain, Component Swap, and Firmware Injections

Enterprises cannot control the supply chain for personal devices, and unauthorized third parties can easily tamper with or repair them.

- **Unauthorized Repair Services Exploits:** If a staff member breaks a laptop screen, battery, or motherboard on their own laptop or handset, they usually go to non-certified third-party repair vendors instead of enterprise warranty pipelines. Malicious repair actors can implant hardware, edit the UEFI SPI flash chips, or flash modified microcontroller code in the battery management system (BMS). These changes enable ongoing, low-level data leakage that is not detected even after reinstalling an operating system or updating firmware (Howell et al., 2023).
- **Firmware Flashing via Insecure Boot Configurations:** Personal endpoints may also have Secure Boot disabled or use custom keys to support alternative OS installations, known as firmware flashing via insecure boot configurations. Malicious code can be loaded

via the Unified Extensible Firmware Interface (UEFI) or by flashing vulnerable firmware and even loading persistence bootkits—like CosmicStrand or MoonBounce—that remain active after operating system reinstallations, even before the kernel has loaded. Many consumer-grade mobile devices lack a concept of a "root of trust" that makes it hard for traditional endpoint security software to protect against baseline-level firmware manipulation.

Vector 5: Cold Boot Attacks and Microarchitectural Side-Channels

If the device is suspended or recently powered off, an attacker can obtain volatile data from its memory modules by physically touching the device.

- **DRAM Remanence Exploits:** Dynamic RAM will keep its bit states for seconds to minutes after power is removed, and this time can be extended to hours with sprays of cryogenic coolants. An attacker can remove SODIMM modules from an employee's own laptop and insert them into a diagnostic acquisition rig, and obtain the enterprise full disk encryption key (FDEK), such as BitLocker or FileVault Master Key, without resorting to disk-level security measures (Jiang et al., 2023, pp. 1–2).
- **Physical Probe & Power Analysis Side-Channels:** Advanced adversaries can use physical probe and power-analysis side channels: record power-consumption traces (Differential Power Analysis) or observe electromagnetic radiation (EM side channels) during cryptographic operations on the motherboard. This enables recovery of the private RSA/ECC keys that are generated in non-tamper-resistant platform chips (Guillaume et al., 2026, pp. 1-11).

Analytical Comparison: Corporate Managed Endpoints vs. BYOD

The following is a comparison of corporate hardware controls to consumer endpoints when used in modern BYOD paradigms.

Security Control Vector	Corporate-Managed Device	Modern BYOD Endpoint	Risk Differential & Impact
I/O Bus & DMA Defense	Kernel-enforced IOMMU; Thunderbolt peripheral authorization white-	Variable IOMMU activation; peripheral authorization set to auto-connect;	Critical: Uncontrolled external DMA leads to immediate memory manipulation and key theft.

Security Control Vector	Corporate-Managed Device	Modern BYOD Endpoint	Risk Differential & Impact
	lists; OS-level port disabling via enterprise GPO.	unrestricted PCIe externalization.	
Firmware & Secure Boot	Cryptographically locked BIOS/UEFI; hardware-enforced measured boot attestation via fleet TPM; custom keys blocked.	Consumer-managed BIOS; frequent legacy support or disabled Secure Boot; vulnerable to bootkit implants.	High: Root-of-trust subversion compromises the OS and EDR agents prior to kernel execution.
USB/HID Execution Policy	Endpoint agent restricts new HID enumerations; USB Mass Storage blocked; keyboard micro-typing rate detection active.	Unrestricted USB plug-and-play; unmonitored human-interface drivers; no keystroke velocity anomaly checks.	High: Rapid HID script injection facilitates remote shell persistence in under 10 seconds.
Physical Enclosure & Telemetry	Kensington chassis slots; tamper-evident chassis seals; real-time internal chassis-open sensors report to SIEM.	Consumer-grade plastic/metal bodies; zero tamper evidence; unmonitored hardware service interventions.	Medium: Undetected physical case openings permit internal hardware taps and rogue microcontroller implants.
Chain of Custody & Offboarding	Standardized corporate chain of custody; geofenced remote wipe; mandatory immediate physical return policies.	Fragmented personal usage; family sharing; untrusted third-party repair; delayed loss notifications.	High: Prolonged attacker physical exposure windows maximize offline cryptographic extraction feasibility.

Quantitative Risk Modeling: Physical-to-Logical Lateral Movement

To estimate the enterprise risk brought by physical endpoint access on a BYOD device, we model the likelihood of the adversary being able to pivot from physical access to the full compromise of the corporate infrastructure.

Mathematical Probability Formulation of Compromise

Suppose $P(C)$ denotes the total probability of compromising an enterprise network through a single BYOD device that is physically compromised. The four dependent transitions are used in the progression:

1. $P(A)$: Probability that the adversary can physically access the device when the attack is feasible (unattended desk, theft, interception during transit, malicious repair facility).
2. $P(E \mid A)$: Probability that hardware is exploited successfully when physical access is given (DMA memory extraction / BadUSB injection / cold boot acquisition).
3. $P(K \mid E)$: Probability of getting working corporate credentials, session tokens, or private keys from the exploited physical memory space or container environment.
4. $P(L \mid K)$: Probability that, with those credentials, access to the Enterprise network can be accomplished logically and Lateral

movement can be performed without using physical hardware attestation challenges.

The joint probability is written as follows:

$$P(C) = P(A) \times P(E \mid A) \times P(K \mid E) \times P(L \mid K)$$

In the context of locked ports, enforced IOMMU, TPM measured boot, and continuous zero-trust context evaluation, it is very close to zero ($P(E \mid A) \approx 0.02$). On the other hand, when used in an unhardened consumer laptop:

- This is because of exposed Thunderbolt/USB interfaces and lack of HID throttling, which gives $P(E \mid A) \approx 0.85$.
- $P(K \mid E) \approx 0.90$ because of non-volatile cached credentials, browser-stored OAuth refresh tokens, and cleartext keys in DRAM.
- If businesses focus on static credentials or software-based MFA without hardware-based tokens, then the probability of a successful attack is $P(L \mid K) \approx 0.70$

This model assumes that with physical access $P(A)$, the probability of compromise for enterprises on BYOD endpoints increases greatly from that of hardened assets:

- $P(C \mid A)_{\text{BYOD}} = 0.85 \times 0.90 \times 0.70 = 0.5355 \text{ quad } (53.6\%)$
- $P(C \mid A)_{\text{Corporate}} = 0.02 \times 0.20 \times 0.15 = 0.0006 \text{ quad } (0.06\%)$

This shows a 900-fold greater chance of endpoint penetration after physical access when the endpoint is not hardened, compared with a hardened endpoint in an enterprise environment. These risks can mount quickly, and comprehensive security solutions such as containerization and mobile device management are crucial to address vulnerabilities across various personal device environments (Mamogale & Mpekoa, 2025, pp. 310–318).

The Lateral Movement Kill Chain

From acquisition to penetration of the infrastructure, the process is systematic:

Stage 1: Physical Acquisition

5- 60 seconds physical access time



Stage 2: Hardware Injection / DMA

* FPGA PCILeech (or Rubber Ducky) activates payload

* Bypasses Ring 0 protection of the operating system



Stage 3: Credential Harvest

* Enterprise refresh tokens are isolated in the memory dump.

- Private VPN keys and session cookies extracted



Stage 4: Network Impersonation

* Attacker opens a tunnel to the corporate intranet, which is legitimate

A device's MAC/hardware ID is spoofed.



Stage 5: Enterprise Lateral Movement

* Active Directory queries, micro-segmentation traversal, and access to proprietary cloud repos.

Stage 1 Physical Acquisition: Obtain the endpoint in a public location, while crossing a border, or at a maintenance location where they did not know.

Stage 2 Hardware Injection/DMA: Attacker connects to an FPGA-based PCILeech or plugs in a BadUSB device via the Thunderbolt port. It takes only seconds to break through with the exploit, which can run through the active lock screen and gain kernel execution privileges.

Stage 3 Credential Harvesting: The adversary now directly accesses the Kerberos tickets, SAML assertions, and decrypts corporate OAuth tokens from memory. The enterprise MAM sandbox is decrypted by the adversary using keys obtained from DRAM.

Stage 4 – Network Impersonation: The attacker's command rig is filled with the stolen corporate VPN configuration, certificate profile, and session tokens. The attacker instead has the victim use the attacker's hardware ID (MAC address and attacker's TLS certificate) instead of the employee's machine's hardware ID.

Stage 5 (Enterprise Lateral Movement): The hacker moves across enterprise micro-segmentation boundaries, accesses enterprise shared storage, and can compromise it by introducing ransomware payloads, stealing customer databases, or even gaining access to enterprise source code repositories.

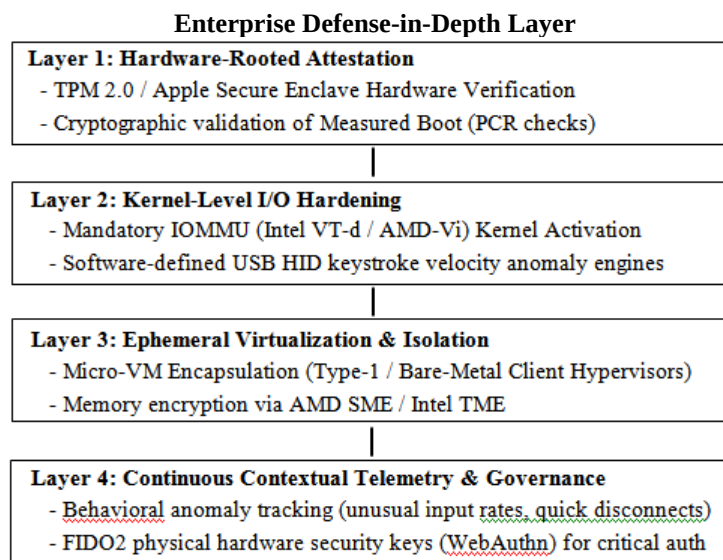
Defensive Architecture: Engineering a Resilient BYOD Physical Security Framework

This presentation will cover how to create a physical security plan for BYOD that resists interference.

The only way to deal with physical endpoint attacks in BYOD environments is to build architectures based on the assumption that the physical port and underlying host operating system

are potentially hostile. The answer is to create a zero-trust foundation based on the most concrete hardware-rooted trust points. Because each session must be bound to the hardware, the organization

can detect tampering at the kernel level before allowing access to its resources (Alevizos et al., 2021, pp. 1-27).



Layer 1: Hardware-Rooted Remote Attestation

Businesses need to stop allowing software container installations to prove device integrity. BYOD access policies should require Cryptographic Remote Health Attestation (CRHA):

- The device must have a vendor-certified hardware secure processor (TPM 2.0 or Apple Secure Enclave) that is activated.
- The device has to produce a cryptographic quote of its Platform Configuration Registers (PCRs) before accessing corporate access brokers.
- The enterprise verification server checks the PCR signature to ensure the UEFI firmware, bootloaders, and kernel parts are authentic, unaltered, and firmly set to Secure Boot. Devices with altered firmware states and/or core protections disabled are not granted any connection tokens.

Layer 2: Kernel-Level I/O Hardening and Strict DMA Controls

For laptops enrolled in BYOD programs, conditional access frameworks must enforce strict operating-system baselines, including kernel-level direct memory protection.

Enforced IOMMU Activation: The operating system needs to enforce Intel VT-d or AMD-Vi at the hypervisor/kernel level to limit access to external peripherals to only pre-allocated safe DMA buffers. Legacy devices (those that do not

support IOMMU) should not be assigned to higher privileged roles within the enterprise.

Peripheral Access Control Agents: Enterprise agents installed on the endpoint can help enforce the protection profile for DMA (e.g., Kernel DMA Protection for Windows, or USB Authorization for macOS), and automatically lock out external PCIe tunneling protocols when the workstation goes into screen lock mode.

HID Rate Limping: Add software-defined drivers to track the rate at which keystrokes are input. The interface freezes the input if they come in at superhuman speed, such as 500 characters per second (typical of DuckyScript injection), and notifies the security team of the occurrence.

Layer 3: Ephemeral Virtualization and Zero-Trust Execution Enclaves

Organizations should implement micro-virtualization with hypervisor technology to separate corporate workflows from peripheral user interactions.

- Corporate resources are needed to run independently of the main personal host operating system in an isolated micro-virtual machine (micro-VM) or client hypervisor.
- **Transparent Memory Encryption:** Use CPU architectural features, such as Intel Total Memory Encryption (TME) or AMD Secure Memory Encryption (SME), to encrypt memory lines that are stored in DRAM chips, with hardware-generated encryption keys. This

will eliminate cold boot memory extractions and hardware bus probe attacks.

- The micro-VM does not allow any pass-through of external peripherals, meaning that personal USB/PCIe ports are not able to communicate directly with enterprise data environments.

Layer 4: Modern Authentication and Physical Telemetry Integration

- **Decoupling Credential Trust with FIDO2 Hardware Keys:** Eliminating Stored, Reusable Passwords and Software-Only Tokens with Decoupling Credential Trust & FIDO2 Hardware Keys. Decoupling Credential Trust & FIDO2 Hardware Keys: Eliminating Stored, Reusable Passwords and Software-Only Tokens. Corporate authentication shall be based on a physical, user-presence-verified FIDO2/WebAuthn security token (such as a YubiKey) that must be touched or challenged by the user on the external security token. Even if an attacker obtains a cleartext session token, operations that require a step-up challenge cannot be completed without possession of the external token (Barbosa et al., 2025, pp. 304–332).
- **Context-Driven Geofencing and Physical Anomaly Telemetry:** Security systems should compare device telemetry (Wi-Fi triangulation, ambient BLE signals, and sudden hardware disconnection logs) to determine whether the environment is safe or not. The system can automatically revoke conditional access tokens if a device connects from an anomalous spatial context with newly introduced, unverified peripherals (Vilaskar et al., 2025, pp. 1–6).

Policy, Human Governance and Operational Realities

Technological solutions cannot address physical-device vulnerabilities in BYOD. A new governance model is needed to suit the "couch potatoes" in the home environment:

A Holistic BYOD Governance Framework
Clear Demarcation Policies Set clear guidelines on acceptable hardware repairs Boundaries of device lending, secure disposal of devices.
Secure Hardware Accessories at a Reduction Distribute certified USB data blockers and privacy screen filters for hardware devices and tamper-evident transport sleeves for employees.
Blameless Physical Loss Reporting Create a policy for timely reporting of lost or stolen endpoints by No-penalty policies, faster network revocation times.

Explicit BYOD Device Maintenance Policies:

Establish clear, easy-to-understand device maintenance policies. Policies should include a rule prohibiting uncertified third-party repair shops from repairing devices with enterprise data access profiles without first clearing the enterprise containers.

Secure Hardware Accessories (SHAs): Hardware accessories the enterprise subsidizes and certifies, rather than employees purchasing them individually. This helps prevent juice jacking, visual eavesdropping, and other threats by distributing verified USB data-blockers, USB data-blocking hardware privacy screen filters, and tamper-evident travel sleeves.

Blameless Physical Incident Reporting: Immediate Disciplinary Action or Complete Erasure of Personal Pictures on an Aggressive Remote Device Wipe: If a staff member fears they will be disciplined or have all of their personal pictures erased by an aggressive remote device wipe, they may not report the lost or stolen device immediately. Instead of reporting structures that are responsive and blameless, organizations should wipe selective data partitions rather than personal ones.

III. CONCLUSION

In the modern era, the integrity of the logical software abstraction can be guaranteed within the enterprise security paradigm only if the host's provenance is assured. The researchers' findings indicate that BYOD initiatives are not offering any protection against DAM, microarchitectural key extraction, or human interface device injection, and therefore "automatically break the physical perimeter, exposing corporate infrastructures to all sorts of attacks. This quantitative risk formulation demonstrates that an unhardened consumer endpoint's risk to the network is 900 times greater than that of an enterprise-managed endpoint. If you

need to address this architectural weakness, do so, but be aware that you are in an untrusted environment. The key transformation the organization faces is moving from passive to multi-layered zero-trust hardware. Technologies used for defense in-depth are cryptographic remote health attestation, kernel-level direct memory access bus gating, client-level micro-virtualization and transparent memory encryption, and – not least of all – hardware-bound FIDO2 authentication tokens. It should also augment technical security with socio-technical governance mechanisms, like blameless incident reporting and subsidized physical data-blockers. Businesses that progress gradually through these phases can enjoy the productivity benefits of BYOD, without setting themselves up to guard important resources.

REFERENCES

- [1]. Alevizos, L., Ta, V. T., & Eiza, M. H. (2021). Augmenting zero trust architecture to endpoints using blockchain: A state-of-the-art review. *Security and Privacy*, 5(1), Article e191. <https://doi.org/10.1002/spy2.191>
- [2]. Barbosa, M., Boldyreva, A., Chen, S., Cheng, K., & Esquivel, L. (2025). Privacy and security of FIDO2 revisited. *Proceedings on Privacy Enhancing Technologies*, 2025(3), 304–332. <https://doi.org/10.56553/popets-2025-0100>
- [3]. Baseri, Y., Chouhan, V., & Ghorbani, A. A. (2026). Cybersecurity in the quantum era: Assessing the impact of quantum computing on infrastructure. *Computers & Security*, 167, Article 104917. <https://doi.org/10.1016/j.cose.2026.104917>
- [4]. Disterer, G., & Kleiner, C. (2013). BYOD: Bring your own device. *Procedia Technology*, 9, 43–53. <https://doi.org/10.1016/j.protcy.2013.12.005>
- [5]. Dumitru, R., Wan, J., Genkin, D., Kennell, R., Dave, T., & Yarom, Y. (2025). Thunderhammer: Rowhammer bitflips via PCIe and Thunderbolt (USB-C). *arXiv*. <https://doi.org/10.48550/arXiv.2509.11440>
- [6]. Guillaume, J., Pelcat, M., Nafkha, A., & Salvador, R. (2026). Multi-screaming-channel attacks: Frequency diversity for enhanced attacks. *IEEE Transactions on Information Forensics and Security*, 21, 1–11. <https://doi.org/10.1109/tifs.2026.3683278>
- [7]. Harris, J. G., Ives, B., & Junglas, I. (2012). IT consumerization: When gadgets turn into enterprise IT tools. *MIS Quarterly Executive*, 11(3), Article 4. <https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1245&context=misqe>
- [8]. Harrison, J., Jessurun, N., & Tehranipoor, M. (2024). SoK: A security architect's view of printed circuit board attacks. *arXiv*. <https://doi.org/10.48550/arXiv.2410.09993>
- [9]. Heartfield, R., & Loukas, G. (2015). A taxonomy of attacks and a survey of defense mechanisms for semantic social engineering attacks. *ACM Computing Surveys*, 48(3), 1–39. <https://doi.org/10.1145/2835375>
- [10]. Howell, G., Franklin, J., Sritapan, V., Souppaya, M., & Scarfone, K. (2023). Guidelines for managing the security of mobile devices in the enterprise (NIST Special Publication 800-124 Rev. 2). National Institute of Standards and Technology. <https://doi.org/10.6028/nist.sp.800-124r2>
- [11]. Hwaitat, A. K. A., Fakhouri, H. N., Alawida, M., Atoum, M. S., Abu-Salih, B., Salah, I., Al-Sharaeh, S., & Allassaf, N. (2024). Overview of mobile attack detection and prevention techniques using machine learning. *International Journal of Interactive Mobile Technologies*, 18(10), 125–157. <https://doi.org/10.3991/ijim.v18i10.46485>
- [12]. Javaheri, D., Fahmideh, M., Chizari, H., Lalbakhsh, P., & Hur, J. (2023). Cybersecurity threats in FinTech: A systematic review. *Expert Systems with Applications*, 241, Article 122697. <https://doi.org/10.1016/j.eswa.2023.122697>
- [13]. Jiang, Y., Wang, S., Figueiredo, R., & Jin, Y. (2023). Warm-boot attack on modern DRAMs. In *2023 Design, Automation & Test in Europe Conference & Exhibition (DATE)* (pp. 1–2). IEEE. <https://doi.org/10.23919/date56975.2023.10136888>
- [14]. Majeed, R. (2026). The paradigm shift: A comprehensive analysis of zero trust architecture in cybersecurity. *International Journal of Scientific Research & Engineering Trends*, 12(1), 1–8. <https://doi.org/10.5281/zenodo.18711740>
- [15]. Mamogale, C., & Mpekoa, P. N. (2025). ShieldDroid enterprise: A comprehensive security framework to protect corporate

- data on personal devices. In 2025 8th International Conference on Information and Computer Technologies (ICICT) (pp. 310–318). IEEE.
<https://doi.org/10.1109/iciict64582.2025.00055>
- [16]. Markettos, A. T., Rothwell, C., Gutstein, B. F., Pearce, A., Neumann, P. G., Moore, S. W., & Watson, R. N. M. (2019). Thunderclap: Exploring vulnerabilities in operating system IOMMU protection via DMA from untrustworthy peripherals [Conference paper]. Apollo - University of Cambridge Repository.
<https://doi.org/10.17863/cam.35771>
- [17]. Nabeel, M., Ashraf, M., Patnaik, S., Soteriou, V., Sinanoglu, O., & Knechtel, J. (2020). 2.5D root of trust: Secure system-level integration of untrusted chiplets. *IEEE Transactions on Computers*, 69(11), 1611–1625.
<https://doi.org/10.1109/tc.2020.3020777>
- [18]. Nicho, M., & Sabry, I. (2022). Threat and vulnerability modeling of malicious human interface devices. *The Eurasia Proceedings of Science, Technology, Engineering and Mathematics*, 21, 241–247.
<https://doi.org/10.55549/epstem.1225679>
- [19]. Or-Meir, O., Nissim, N., Elovici, Y., & Rokach, L. (2019). Dynamic malware analysis in the modern era—A state-of-the-art survey. *ACM Computing Surveys*, 52(5), 1–48.
<https://doi.org/10.1145/3329786>
- [20]. Rothwell, C. (2017). Exploitation from malicious PCI Express peripherals [Doctoral dissertation, University of Cambridge]. Apollo - University of Cambridge Repository.
<https://doi.org/10.17863/cam.21474>
- [21]. Sokolov, V., & Skladannyi, P. (2025). Developing a balanced security policy for Bring Your Own Device in corporate networks. In *Information Security and Communication Technologies* (pp. 136–156). <https://doi.org/10.36690/itsc-136-156>
- [22]. Soubhagyalakshmi, P., & Reddy, K. S. (2022). An efficient security analysis of bring your own device. *IAES International Journal of Artificial Intelligence*, 12(2), 696–703.
<https://doi.org/10.11591/ijai.v12.i2.pp696-703>
- [23]. Spreitzer, R., Moonsamy, V., Korak, T., & Mangard, S. (2017). Systematic classification of side-channel attacks: A case study for mobile devices. *IEEE Communications Surveys & Tutorials*, 20(1), 465–488.
<https://doi.org/10.1109/comst.2017.2779824>
- [24]. Stajner, R., Yehuda, R. B., & Zaidenberg, N. (2021). Attacking TrustZone on devices lacking memory protection. *Journal of Computer Virology and Hacking Techniques*, 18(3), 259–269.
<https://doi.org/10.1007/s11416-021-00413-y>
- [25]. Tian, J., Scaife, N., Kumar, D., Bailey, M., Bates, A., & Butler, K. (2018). SoK: "Plug & pray" today – Understanding USB insecurity in versions 1 through C. In 2018 IEEE Symposium on Security and Privacy (SP) (pp. 1032–1047). IEEE.
<https://doi.org/10.1109/sp.2018.00037>
- [26]. Vengara, N. S. P., & Bhoir, Y. S. N. (2026). USB security threats and physical access vulnerabilities: A comprehensive review. *International Journal of Advanced Multidisciplinary Research and Educational Development*, 1(4), 875–877.
<https://doi.org/10.5281/zenodo.18154704>
- [27]. Vilaskar, T. D., More, S. G., Salunke, A. A., Mirajkar, R. R., Kaakandikar, R. M., & Dhole, P. B. (2025). AccessGuard++: AI-enhanced risk intelligence for zero trust systems. In 2025 IEEE Pune Section International Conference (PuneCon) (pp. 1–6). IEEE.
<https://doi.org/10.1109/punecon67554.2025.11378025>
- [28]. Wang, C., & Hsu, F. (2025). USBIPS framework: Protecting hosts from malicious USB peripherals. *Computer Standards & Interfaces*, 95, Article 104040.
<https://doi.org/10.1016/j.csi.2025.104040>
- [29]. Webb, N. L., Johnson, M., & Saenz, P. (2025). Enhancing satellite cybersecurity through FPGA-based secure boot. In 2025 IEEE Aerospace Conference (pp. 1–7). IEEE.
<https://doi.org/10.1109/aero63441.2025.11068623>