WHY THE ROAD TO ZERO TRUST AUTHENTICATION GOES THROUGH ZKX

The Zero Trust security model requires a revolutionary shift from traditional authentication methods that have been in use for decades. Traditional networks are perimeter-based and by design automatically trust anyone and anything once inside the network. In a Zero Trust architecture, every user or device that tries to access a resource requires strict verification every single time. In other words, a zero-trust architecture trusts no one and nothing.

While the DoD has mandated migration to zero-trust networks, most organizations are still unclear on how to get started. This briefing outlines why the road to zero trust networks logically starts with ZKX authentication technology.

AUTHENTICATION IS AT THE CENTER OF THE ZERO TRUST ARCHITECTURE

Zero Trust Architecture requires three fundamental steps, applied at the level of applications and services within the network:

1. Verify the user (authentication, part 1)
2. Verify the device (authentication, part 2)
3. Verify access privileges (authorization)

Notice how two-thirds of the steps are authentication-based. Get this wrong and the whole Zero Trust architecture crumbles. Authentication is the linchpin for the operational success of Zero Trust.

“Zero-trust” means we are not awarding privileges based on purported identity alone. We need a lightweight, repeatable, and bulletproof method to prove identities claimed & previously verified as legitimate per perimeter-breaching transaction. Authentication must occur before any and every instance of perimeter traversal is allowed.

HOW ZKX USER AND DEVICE AUTHENTICATION WORKS

- **ZKX securely authenticates the user and device at the same time, simplifying the ZTA equation.**
- **This also lets organizations separate user privileges more granularly and in a more automatic fashion on the basis of device (DBAC).**

PROTECTING AUTHENTICATION CREDENTIALS

There are hundreds of thousands of attempted cybersecurity attacks against DOD networks every day. Data Loss Prevention (DLP) is the current method that is assumed to protect data by monitoring, detecting, and blocking sensitive data while in use, in motion, and at rest. However, since the number of attacks is so large even a very highly successful system will fail.

Case in point: assume 100,000 attacks per day (36,500,000 per year). Even in a system with a success rate of 99.99999% (7 nines!), there will still be 3.65 successful attacks per year. If these attacks were on user credentials, then you are requiring users to re-establish credentials every 3 or 4 months!

HOW ZKX SECURES USER AUTHENTICATION CREDENTIALS

- **ZKX does not store user credentials anywhere.**
- **Any data that is used can be made public and the system is still very secure.**
- **Quite simply, with ZKX there is no user data to steal!**

MITIGATING PHISHING AND SOCIAL ENGINEERING ATTACKS

Adversaries continue to find creative methods of getting around commonly used security methods via social engineering attacks that manipulate users into giving away their credentials.

Under the current security model, the solution is to keep increasing the number of firewalls, which is a never-ending game of “whack-a-mole”. Costs and user training keep going up, with no end in sight.

HOW ZKX COMBATS SOCIAL ENGINEERING ATTACKS

- **With ZKX, credentials are tied to devices, therefore stealing passwords is useless unless the device and all credentials are obtained.**
- **Leaking just one part may still not damage the whole. Even if an attacker gleans a PIN and has access to a device, a successful breach is still not guaranteed if they lack other factors such as a token or answers to a security question.**
- **ZKX is inherently multi-factored, further spreading security risk amongst several components**

CONSTANT INCREASE IN ATTACK SURFACE

DoD cybersecurity is at a critical juncture. Its networks are growing in both size and complexity, requiring massive amounts of rapid data transfer to maintain situational awareness on the digital and physical battlefield. This expansion is stretching existing cybersecurity apparatuses to their breaking point, as an ever-growing number of users and endpoints increases the attack surface of the network.

The fallacy that ZTAs will solve this is unfounded for the simple reason that the attack surface is not a permitter problem but rather an area problem. Breaking up a large perimeter security-based system into smaller zoned-based systems using ZTA just distributes the area of attack rather than reducing it.

With each perimeter comes another iteration of the necessary authentication & authorization checks needed to pass the perimeter. Operational & user friction expands geometrically as a function of the number of perimeters (how many times we are dividing the area) that are created to achieve “zero trust” security.

HOW ZKX REDUCES THE ATTACK SURFACE

- **With ZKX, the attack on user credentials is eliminated outright.**
- **ZKX extends beyond an organization to its federated partners. This is critical not just for existing network ops (where today PKI and its accessories must be perfectly synchronized) but also for the ZTA-to-ZTA interoperability, a topic which the industry at large has been suspiciously silent on.**

AUTHENTICATION OF NON-PERSON ENTITIES AND USER IDENTITIES

In current ZTA designs, Non-Person Entity (NPE) identity and user identity are tracked independently allowing for separate paths of validating confidence levels across enforcement points.

HOW ZKX KEEPS BOTH NON-PERSON ENTITIES AND USERS ON THE SAME PATH

- **Simplifies a complex network with the use of a single authentication protocol. The same logs can be used for all entities and the same analytics programs can be used across the entire ZTA environment.**
- **Moves management of NPEs and users up from the authentication protocol level to the policy level. Now a policy manager can just treat all entities the same and control access via policy, credential types, and confidence score.**
- **Brings the actualization of Zero Trust principles to IoT-focused environments (e.g., distributed sensor networks).**
- **Enforces active connections of autonomous nodes with simple, server-side key management.**