PACNET

ZERO TRUST ARCHITECTURE: TAIWAN'S NEXT STEP FOR BUILDING CYBER RESILIENCE

BY IRFAN UL HAQ

Maximilian DiGiovanni *(maxidigio@gmail.com) is a current student at the University of New Hampshire working towards a B.A. in both History and Political Science. His time as an intern at the Near East South Asia Center for Strategic Studies exposed him to numerous perspectives on current American strategic objectives, with particular emphasis on emerging technologies and the cyber domain.*

Taiwan has long endured a relentless barrage of cyberattacks, suffering as many as 30 million per month in 2022. While the Taiwan's Ministry of Digital Affairs has increasingly invested in government cybersecurity infrastructure, some vital sectors still require attention. Taiwan's semiconductor and telecommunications industries are central to its economy and have a large impact on global supply chains. Thus, these two sectors most urgently require cybersecurity improvements. To fulfill that need, zero-trust architecture (ZTA), designed to minimize the damage retained from cyberattacks, should be adopted and augmented by Taiwan as quickly as possible.

Volt Typhoon, a major Chinese hacking group, prefers to disguise its activity as regular system or network behavior as it infiltrates, a technique known as living-off-the-land (LOTL). This allows them to potentially surpass software trained to merely detect activity by end user devices like smartphones and laptops. Implementing ZTA will bridge the gap between what is needed to combat this technique and what is already being done with its security.

ZTA's basic functionality is to create a checkpoint between an enterprise's resources—whether that be data, services, and assets like devices and infrastructure components—and subjects such as end users, applications, or other non-human entities that may request access. Even autonomous systems must request access to resources in a zero-trust system, thus mitigating the possibility of an LOTL attack masking itself as an autonomous system and bypassing security.

In contrast to a system prioritizing a strong defensive perimeter and maintaining trust for activity within its network, ZTA examines all communication between subjects and the resources they wish to access regardless of the subjects' network location. For ZTA, connection to the enterprise's network does not translate to trust, and requests by enterprise-owned network infrastructure are met with the same level of scrutiny as unfamiliar networks. A hacker using LOTL techniques may be able to disguise their request as friendly network behavior, but this would not guarantee them any greater level of access than if they were communicating from a foreign network.

Within ZTA, access to individual resources is granted on a per-session basis, and with each request it evaluates large flows of data from the enterprise's policy rules, aggregated network and system activity logs, and other diagnostics before analyzing each subject's request and deciding whether to grant them permissions. ZTA also reduces each subject's privileges to access only the minimum resources necessary for the task it wishes to complete, heavily restricting lateral movement across an enterprise's network upon gaining access.

ZTA is designed to force subjects into a repeated cycle of obtaining access to resources on request, each time reevaluating its trust in subjects based on their adherence to the enterprise's behavioral norms and standards. This design would aim to subject a disguised LOTL hacker to frequent autonomous behavioral review as it attempts to access enterprise resources. It would also attempt to restrict an intruder's capabilities to access the enterprise's resources after compromising its system by forcing them to submit new, suspicious requests each time

they wish to perform new tasks, which could substantially neutralize LOTL attacks.

While not quite ZTA, Taiwanese industries are currently eager to adopt the US Department of Defense's cybersecurity framework, as it has mandated compliance for all its supply chain vendors by 2026. While harboring a strong potential to later build into ZTA, the framework still allows the precedence of strong perimeter firewalls and internet gateways. These are great at blocking attackers from accessing an enterprise's internet, but less useful at dealing with hackers from within the network—which is how LOTL attacks function—because they allow full access to those who can break the digital perimeter.

Taiwanese industries could pivot toward ZTA in various ways. They already aim to require organizations to employ controls over information flow, such as prohibiting direct information transfers between connected systems like computers. This is a tenant of ZTA because it requires information transfers to be facilitated by a centralized mechanism as opposed to directly between systems. That mechanism is also required to verify requested permissions before accepting information from another network or connected system, which could certainly be adapted into an all-encompassing permissions access system like ZTA.

While Taiwan would benefit immensely from ZTA as another line of defense from hacks, Taiwan's recent demands in its 2021-2024 National Cybersecurity Development Program only amassed in ZTA for its government network. To secure the island's future economic resilience, Taiwanese authorities should consider extending their investment in ZTA to Taiwan's semiconductor and telecommunications industries. Because their current cybersecurity posture already lays much of the groundwork for ZTA, its implementation should be a comfortable step forward. External support could expedite this process, so foreign stakeholders such as Japan and the US should consider providing subsidies.