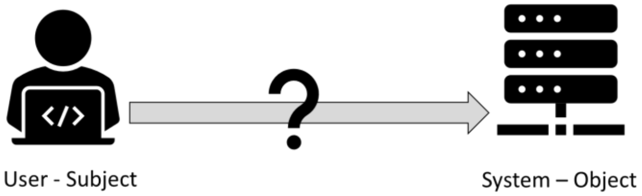
User-Centric Zero Trust – Shifting the Focus to Protect the User!

Dr. Sarbari Gupta, CISSP, CISA

Current zero trust security architectures focus on protecting IT resources (networks, systems, services and data) from users. NIST recently released Special Publication 800-207, entitled *Zero Trust Architecture*. This document states that zero trust "involves minimizing access to resources (such as data and compute resources and applications/services) to only those subjects and assets identified as needing access as well as continuously authenticating and authorizing the identity and security posture of each access request." The focus is on protecting enterprise resources from entities requesting access to those resources.

In the classic computer security Subject-Object model, the User is the subject trying to access a computer resource which is the Object as shown below. Before the user (subject) is allowed access to a protected system (object), the user is required to answer the question "Who are you?".

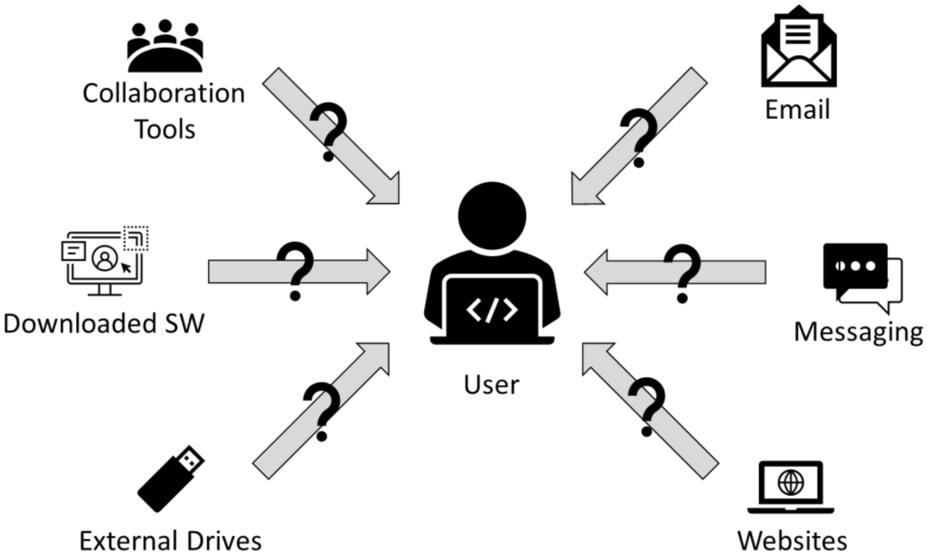


Various types of security controls are implemented to protect the target system from a potential bad actor. For example, the user is asked to undergo authentication to assert and then prove their digital identity. The system checks whether the authenticated user has the privileges needed to perform the action requested. Audit controls may be in place within the system to track user behavior to serve as a deterrent for bad actors and to enable future analysis. The communication channel between the user and the system may be protected with cryptography to prevent unauthorized users from viewing or tampering with the information in transit. And the list goes on.

Mature IT organizations know that the user is often the “weakest link” in the cybersecurity protection chain for the organization. The traditional fix for this problem is mandatory and frequent user training on computer security and privacy topics. However, such training often falls upon deaf years since the training is typically repetitive and tedious. Users just go through the motions to complete the training and get their completion certificate. For home users and children, the situation is even worse. They get little or no guidance on how to keep their computers, their online accounts, and their information secure against the increasing threat of malicious actors lurking in every online pathway that they traverse.

With the increasing complexity of connected information systems in the modern era, it is becoming more and more difficult for legitimate users to keep up their part of the burden of maintaining security. There are more and more collaboration applications and services (email, multiple messaging and social media applications, video and teleconferencing applications, soft phones, etc.) with different interfaces with which users must become familiar. While users are struggling to keep up with their day to day functional responsibilities, it is nearly impossible for them to also be aware of and protect against the avalanche of online attacks being launched continuously.

The average user does not know how to discern clever phishing attacks despite repeated phishing training sessions. The average user will not be able to tell whether the website they browsed to is the authentic website or one whose URL is one or two characters different from the legitimate one. The average user will probably click on a link sent through a messaging application telling them that there was a debit from their bank account for a significant amount of money.



As a veteran in the cybersecurity space and someone who has been watching and influencing the state of the art in this realm, I believe it is time to focus our security protection mechanisms towards protecting the user. We need to develop, refine and implement consistent security mechanisms that enable the user to protect himself or herself. As mentioned above, the average user on an end point device (workstation, laptop, tablet, smart phone, etc.) interacts with other entities in the vast online cyber universe through multiple pathways, including:

- Email
- Websites
- Messaging applications
- Videoconferencing/Teleconferencing applications
- Downloading and installing new applications
- External drives and fobs

How does the User know which interactions and entities to trust?

It is time that we start considering the user not only as the subject of an online transaction, but also as an object of a transaction that is initiated by another party. Consider what the user possesses that is of potential value to a malicious cyber entity:

- Passwords, PINs to various systems that house data and/or services
- Personal identifiable information (PII) that can be used to promote identity theft or otherwise harm the user
- Credit card and financial information that can be used to steal money
- Work related sensitive information that can be used to harm the user’s employer or other stakeholders
- Access to organizational systems which can be used as a launch point for an attack against the organization

Thus, it is no surprise that as systems and networks are getting hardened to protect against hackers, the user is viewed as the soft target for attacks.

I propose a “User-Centric Zero Trust” (UC-ZT) model that focuses on protecting the user from bad actors trying to fool them into taking actions that can expose their personal data or compromise the security posture of their organizational or home. In the UC-ZT model, the user distrusts (that is, has zero trust in) all online entities and systems until the latter establish their identity and reason to interact with the user.

There exists a variety of technologies that can help to enable UC-ZT environments, such as server authenticated SSL/TLS[1], email authentication using DKIM/DMARC/SPF[2], email server tools to scan attachments and bad URLs, digital signatures and thumbprints to check software integrity, scanning tools for attached drives, etc. However, the problem with many of these techniques is that they are neither robust nor easy to apply consistently. Even when implemented, these existing technologies leave a great deal of the responsibility on the user and their ability to discern and thwart attacks. Consider the following examples:

- The user establishes a TLS-protected secure session with www.cit1bank.com and provides their login credentials for their account on www.citibank.com
- The organizational user gets an email purporting to be from the organization’s IT helpdesk asking them to click on a link, and the DKIM/DMARC/SPF checks pass for the incoming email
- The user downloads a piece of software from the Internet which can be validated against a thumbprint; however, the user does not know how to perform the validation step

What is needed is a new mindset within the cybersecurity community that recognizes the user as a high-value asset that requires multi-layered protection. To promote such UC-ZT architectures, we need more focused research and development to strengthen existing technologies as well as identify new methods that can provide robust protection of the user from online attacks through the various channels discussed above.

The ideal user-centric zero trust architecture would have characteristics similar to the protections afforded to a head of state living in their private estate:

- Robust walls around the estate
- Tripwires and monitored cameras to catch anyone that happens to scale the walls
- Guards at every entry point
- Visitors asked to provide valid identification for entry
- Visitors asked to provide the reason for their visit which is validated before entry is granted
- Visitors undergo x-ray checking of their bags and physical being
- Any physical items being brought into the enclave are checked for quality and integrity

Architectures that implement user-centric zero trust will thus:

- Require every external entity that connects with the user on his/her end point devices to undergo multiple layers of security checks
- Require each external entity to prove their identity and their right to interact with the user

[1] Secure Sockets Layer (SSL) and Transport Layer Security (TLS)

[2] DKIM (DomainKeys Identified Mail), DMARC (Domain-based Message Authentication, Reporting and Conformance) and SPF (Sender Policy Framework)

- Block harmful interactions (based on policy) so that the user does not have to decide
- Deploy technologies that do the heavy lifting (such as digital signature validation, checking against whitelists, etc.) in a robust manner and present the user with easy ways to distinguish between trustworthy and untrustworthy interactions/connections

To summarize, cybersecurity technology professionals have been focusing on protecting systems and services from users for many years and this has resulted in significant advances in our ability to protect these entities from bad actors. Now, we need to put our talents and capabilities to strengthen existing technologies and devise new ones that can protect the user from external entities through blocking techniques and/or techniques that provide user-friendly indicators to assist the user to make decisions regarding which entities to trust. This is the concept behind User-Centric Zero Trust!