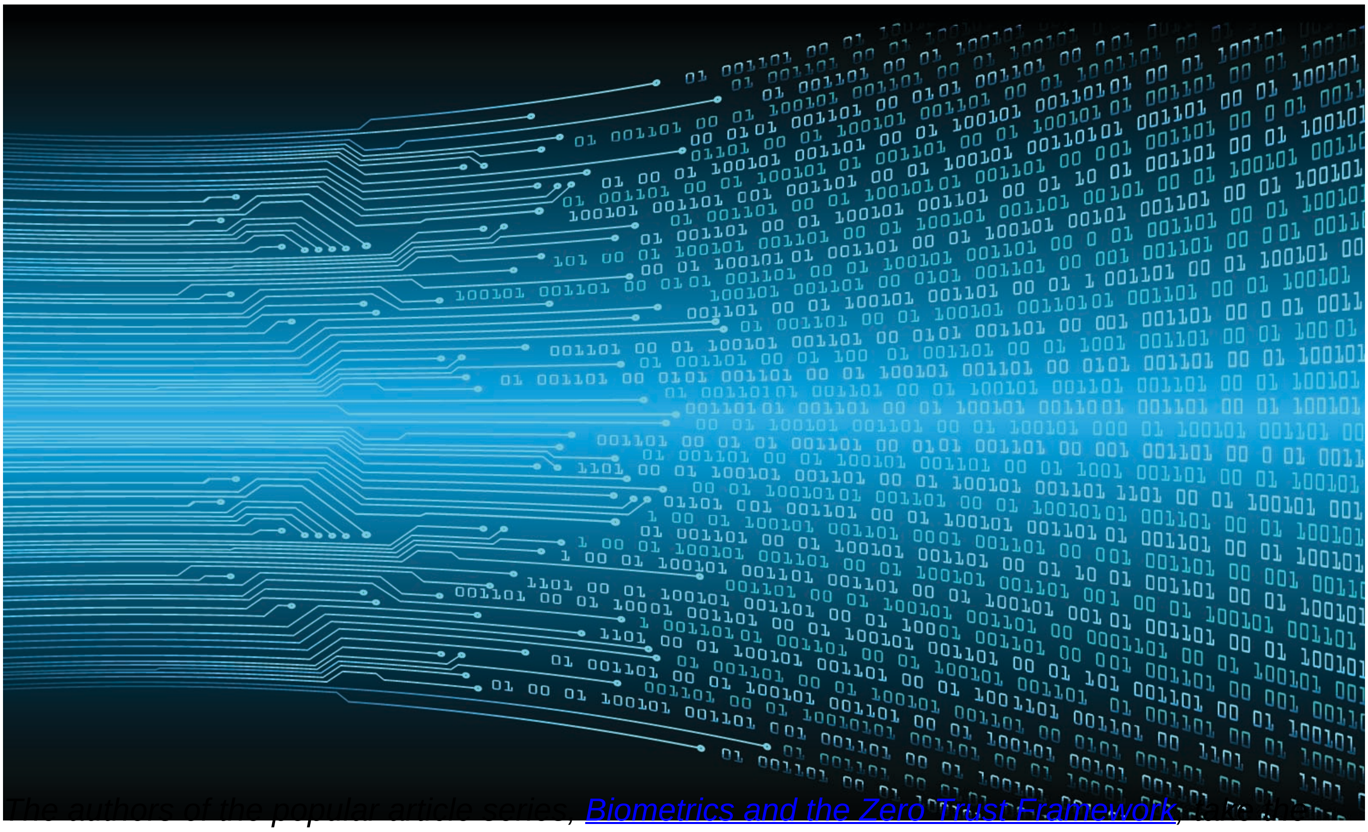
ZTF: The Secret to Seamless Authentication: Part 3

Author :



The authors of the popular article series, [Biometrics and the Zero Trust Framework](), take the topic to the next level in their new book, [ZTF: The Secret To A Seamless Authentication Experience]() (on Amazon). In a previous excerpt from the book, the authors examined [emerging trends and advances in cryptography]().

In this excerpt, the authors begin a discussion of Privileged Access Management (PAM), which gives human users as well as non-human users (such as applications and machine identities) special access or abilities above and beyond that of a standard user in an enterprise setting.

The Weaknesses of Repeated Authorization and Authentication

[One] major weakness of the traditional Zero Trust Framework is its repeated need to keep authenticating and authorizing an end user (or an employee) each and every time they need to get access to something. Although the philosophy of the ZTF is to "never trust" but keep verifying, it can really be a nuisance in the end. On top of that, having to go through this process over and over, especially for larger companies, can tax computing and processing.

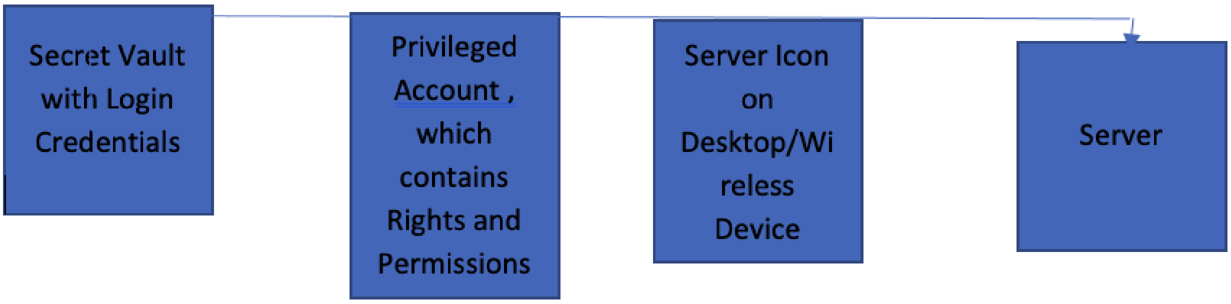
But not only that, the end users (or employees) can also get frustrated with having to go through this process every single time. Is there a solution for this? Yes, and the answer resides in what is known as "Privileged Access Management." In a very broad sense, this area deals with providing a higher level of security for those accounts that are deemed to a higher level than the regular employees. For example, this includes the likes of the CISO, network administrator, database administrator, or even the project manager on a software development team.

Essentially, anybody that has a managerial position at the IT level will have these kinds of accounts. A technical definition of Privileged Access Management (also known as “PAM”) is as follows:

“In an enterprise environment, “privileged access” is a term used to designate special access or abilities above and beyond that of a standard user. Privileged access allows organizations to secure their infrastructure and applications, run business efficiently and maintain the confidentiality of sensitive data and critical infrastructure. Privileged access can be associated with human users as well as non-human users such as applications and machine identities.”

As one can see from this definition, even AI and ML can be given Privileged Level Access. It is important to note at this point that all of the authorization and authentication information and data are kept in what is known as a “Secret Vault”. This is the where the automation process comes into play. For example, if a network administrator needs to gain access to a server, all he or she has to do is simply click on the application icon, and they will be automatically logged into the server.

The login credentials to this server are already stored in the Secret Vault. The network administrator will have their own Privileged Account, and the rights and privileges for the server will be stored here. So, when this individual clicks on the application icon on their desktop or wireless device, this will trigger a response to be sent from the Privileged Account to the Secret Vault, requesting that access be made to this particular server. From here, the Secret Vault will then transmit the login information to this server, and within seconds, the network administrator will be able to get into the server. This is illustrated in the diagram below:


Secret Vault with Login Credentials
Privileged Account , which contains Rights and Permissions
Server Icon on Desktop/Wireless Device
Server

Since PAM is such an integral component of our proposed Zero Trust Framework, it is necessary to [do] a deeper dive into it, in order to gain a much firmer understanding of it.

The Strains of On Prem PAM

Before the COVID-19 pandemic hit, mostly all businesses had an On Prem Infrastructure, or some parts of it were also located on a Cloud based platform, such as that of the AWS or Microsoft Azure. But using PAM in this manner is now showing it is not viable for the following reasons:

- The IT and Network Infrastructures of today are no longer deemed to be static in nature. Rather, they are dynamic, with many end users logging in at the same time to access shared resources, as well as the sheer influx of information that businesses have to

store today in data warehouses, and the various states that they have to go through. These include if they are archived, being transmitted to different points, or are being processed and analyzed.
- Access to the above often made use of GUIs in order to access a PAM server to get the privileged login information. This was done all manually, thus adding more administrative headaches to an already strained process.
- Logging into separate applications required multiple logins into the PAM server in order to access the proper credentials. Given today’s mantra for automation and APIs, and as a result, this is no longer feasible to use.

PAM based solutions are much better suited for Cloud based deployments, especially when it comes to the Hybrid Cloud. *This and other aspects of PAM will be discussed in the next excerpt from the book.*

Sources/References:

See: *ZTF: The Secret To A Seamless Authentication Experience* *(on Amazon)*

Join the conversation.

GO

Visit Keesing Technologies