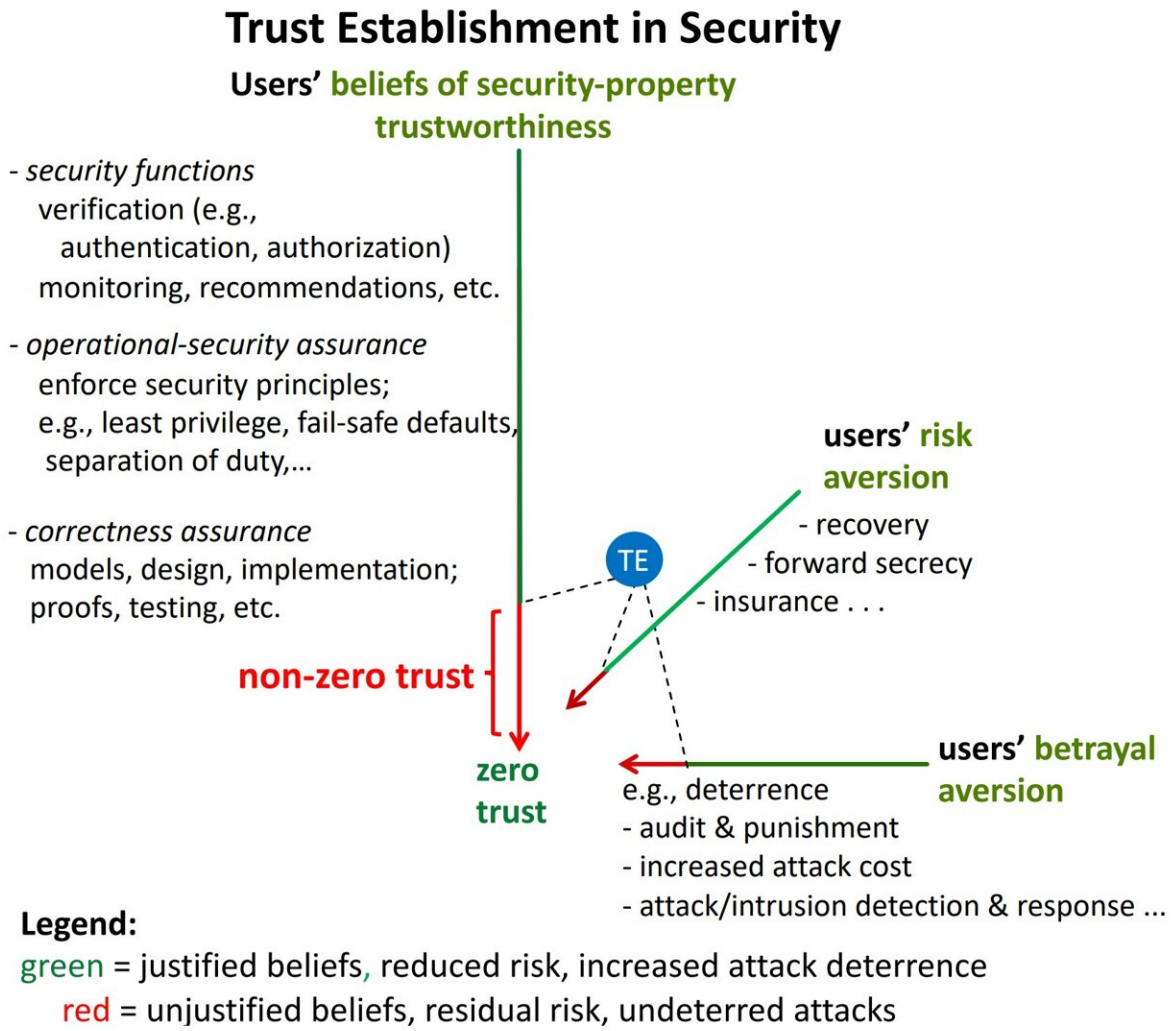
Zero trust in 'zero trust'

March 6 2023, by Ryan Noone



Trust, Zero Trust, and Trust Establishment (TE). Credit: *Zero Trust in Zero Trust?* (2023).

In May 2021, the President of the United States issued an executive order, initiating a government-wide effort to sure up its cybersecurity practices. The mandate tasked agencies with implementing zero-trust architectures and a cloud-based infrastructure by 2024, aiming to increase security and mitigate potential risks.

But Carnegie Mellon University Electrical and Computer Engineering Professor Virgil Gligor says the plan leaves much to be desired and explains achieving zero trust isn't possible.

"Before I tell you what zero trust is, maybe I should start by defining trust," said Gligor. "Trust is the acceptance of the truth of a statement without evidence or investigation; it is blind faith or wishful thinking if you will."

"There are some areas where unjustified beliefs are ok, but in cybersecurity, believing that a security property holds without any evidence or investigation is a liability. So, cybersecurity professionals look to eliminate blind beliefs."

To achieve zero trust, the highest level of trust establishment, Gligor says several tenets would have to be realized. Most importantly, all security properties of an enterprise network would have to be proven unconditionally and with certainty (i.e., with probability one in finite time).

"If you're able to do this, there is no liability left; you've reached zero trust," explains Gligor. "Unfortunately, this is theoretically impossible for some properties and practically unachievable for others."

In his technical report, "Zero Trust in Zero Trust?", Gligor says that "black box" devices, which are used in all servers and endpoints of enterprise networks, make zero trust unachievable, as there is at least one

security property that cannot be justified unconditionally with certainty.

So, what does the government mean when it says zero trust architectures? And what does it hope they will achieve?

Zero-trust architectures are not penetration resistant. Therefore, they do not eliminate breaches. Gligor says, by implementing these architectures, the government's primary goal is to limit adversaries' 'lateral' movement by segmenting networks in an effort to reduce the amount of damage an adversary can cause.

To secure these network segments or implicit trust zones, the government outlines a plan that would grant access to resources based on continuous verification of users' attributes (e.g., roles, permissions, access levels) and enforce the least privilege principle (a security concept that states a user or entity should only have access to the specific data resources and applications needed to complete a required task). However, Gligor says this concept is technically unsound.

Limiting 'lateral' adversary movement can only be achieved if the continuous verification checks and application of least privilege principal prevent cross zone-attacks. Continuous monitoring of devices' behaviors must also detect them. But Gligor explains that zero-trust architectures often fail to detect and prevent against these types of attacks, citing several examples in his technical report.

"The goal of limiting adversaries' movement to a minimized trust zone cannot be accomplished because the criteria that zero trust architectures use fail to minimize many critical trust zones," says Gligor.

"Several other minimization principles exist, which zero trust architectures ignore for practical reasons. Their implementation would require security redesign, which the government seeks to avoid as it

could delay deployment."

While Gligor says zero trust architectures cannot serve as security models due to their inability to counter major security exposures, he stresses they are not useless.

"Although the architectures have a low defense value, they offer useful breach recovery value."

Using data from IBM, Gligor shows that segmenting networks into minimized trust zones can significantly reduce the amount of data lost in a breach, decreasing the overall cost of recovery efforts.

"When you recover data after a breach, you must determine how many information records were lost. With zero trust architectures, instead of losing 20 million records to an adversary, you might lose only 1,000 because you've limited the number of records the adversary has access to. Hence, there is a lot less to recover."

More information: Report: www.cylab.cmu.edu/_files/pdfs/ … ts/CMUCyLab22002.pdf

Provided by Carnegie Mellon University, Department of Chemical Engineering