Software Assurance Tips

A product of the Software Assurance Tips Team[2]

Jon Hood

Monday 10th June, 2024

1 The Zero Trust Paradox: Second Guessing the Good Guys

Updated Thursday 6th June, 2024

In February, the DoD CIO issued RMF security control guidance intending to be a starting point for programs "required to implement zero trust within the DoD."[5, p. 2] These security controls, when properly implemented, can help monitor for threats, conduct continuous assessments, automate the security posture evaluations of components, and support defense-in-depth practices within an organization's system boundary. In particular, the overlays expound on continuous ATO requirements for ongoing authorizations under the Application & Workload Pillar. These controls not only form a solid foundation for which ones should be continuously assessed, but form a baseline set of rules for any application development to follow.

But what happens when the assessment data itself is bad? Though these are not tied to individual systems, the following issues have been observed:

- One organization scanned their software with a custom Fortify rulepack that suppressed or omitted most rules.
- Another organization used SonarQube to scan Ada code.
- A command created a process to do a scan with Coverity, then promptly deleted the results without ever looking at them.
- Enterprise software received an Assess Only assessment approval with the assessment, "The software was not available for review, so no issues are identified."

This begs the question that is referred to here as the Zero Trust Paradox. If you trust your implementation of Zero Trust controls, you have failed to implement the key tenet of Zero Trust: its namesake, *Zero Trust*.

Zero Trust is not a product you can buy off the shelf nor a contract requirement you can give to a contractor to implement; it is a foundation principle for conducting security assessments at the right level of granularity to foster a modular, secure set of information technology.[3]

There is no control in the Risk Management Framework for making sure your program leaders are thinking about their assessments from a Zero Trust perspective, and a Zero Trust overlay poses the danger of treating what should be a mindset for assessments as if it were a checklist of requirements to implement. This is demonstrated by the aforementioned examples. Consider each of these examples with a *minimum compliance* mindset versus a *Zero Trust* mindset to demonstrate why it's important that security control assessments employ a Zero Trust model for their initial evaluations.

In the first example, a program used Fortify to fulfill some of the requirements of RMF control SA-11(1), one of the required controls in the CIO overlay. While the program implemented a good tool for conducting the assessment, there was no check on whether the tool was configured to properly "employ static code analysis…to identify common flaws." The program put trust that the right tool was selected for the right job to build the right assessment data, but no one documented the trust metrics for if the tools were configured correctly to build such evidence. A compliance mindset checks the box that SA-11(1) is implemented by statically scanning the software. A Zero Trust mindset asks, "Why should I trust that data?" and implements steps to make sure that a rigorous, comprehensive evaluation of the controls is correctly implemented.[4]

A "minimal compliance" mindset also plagues the remaining examples. If the mindset is to get an ATO with as little trouble as possible, then bringing transparency into the security findings of a product will slow down or even deny authorizations to operate. The Zero Trust architecture requires transparency, and employing efforts to hide data violates the first core capability of CISA's Zero Trust Maturity Model: *Visibility and Analytics*.[1]

As ISSMs and Authorizing Officials continue to mature in zero trust training guidelines, the "minimal compliance" attitudes will continue to be weeded out. Evaluating your security controls from a Zero Trust perspective now can save your system from a disastrous security control assessment in the future. You won't regret it—trust me!

References

[1] Cybersecurity and Infrastructure Security Agency. Zero Trust Maturity Model. Tech. rep. Version 2.0. 2023. URL: https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf.

[2] Jon Hood, ed. SwATips. https://www.SwATips.com/.

[3] Eric Jackson. "When Zero Trust Makes Zero Sense". In: (2024). URL: https://blog.aquia.us/blog/2024-05-31-zero_trust_zero_sense/.

[4] National Institute of Standards and Technology. Zero Trust Architecture. Tech. rep. Special Publication (SP) 800-207. Washington, D.C.: U.S. Department of Commerce, 2020. DOI: 10.6028/NIST.SP.800-207. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

[5] Office of the Chief Information Officer. "Department of Defense Zero Trust Overlays". In: (2024). URL: https://dodcio.defense.gov/Portals/0/Documents/Library/ZeroTrustOverlays-2024Feb.pdf.