Why Zero Trust is the future of Cybersecurity

Steven McNutt, CCIE #6495 (RS/Security)

stmcnutt@cisco.com

Daily, there are stories about organizations large and small being shut down and having their operations held hostage by anonymous cybercriminals or disgruntled ex-employees. Bad actors are having a tremendous amount of success at the expense of their victims and society as a whole. The security model employed by these organizations is not working. Organizations need a new model that properly accounts for the threat landscape in which they operate. Zero Trust is the network security paradigm of the future because it addresses the organizational challenges of securing cloud-native applications, remote workforces, and critical assets from both internal and external threats.

Zero Trust addresses the challenge of securing cloud-native applications. Securing applications that can potentially be running anywhere and accessed from anywhere may be broken down into two main areas: Securing access to the application and securing the application itself, from code to distribution to the running instance.

For securing access to applications, Google created an influential model called BeyondCorp. In this model, users and devices are securely identified and authenticated. Then this composite identity is authorized to access the application through an access proxy that sits in front of the application (Ward, R., & Beyer, B. 2014). The main thing to point out here is that the control point is the access proxy. In this design, one could also argue that the application proxy acts as a perimeter control, much like a firewall. The weakness of depending on the perimeter for security is once breached, the attacker has freedom of movement on the inside. Therefore in this design, the application environment needs to be secured as well.

Modern cloud-native applications typically use an automated deployment process called a pipeline that assembles the application components, tests them, then instantiates the application in the cloud provider environment. The construction and operation of this pipeline is referred to as DevOps, which is a portmanteau of Development and Operations. DevSecOps leverages the properties and processes of DevOps to embed security tooling into the deployment of the applications themselves (Gilman, E., Barth, D. 2017). One of the interesting security-related aspects of applications built from a DevOps pipeline is the running instance of the application is considered to be immutable. i.e., it is never altered. When a change needs to be made, the running instance is destroyed, and a new one is created to take its place. Short-lived immutable application instances provide a built-in measure of security. Even if a running instance of the application were to be compromised, it would be replaced in short order anyway. Immutable infrastructure deployed via pipeline stands in stark contrast to older application architectures. In older applications, a deployment instance is often a bespoke creation that may have a lifetime of a decade or more and nearly impossible to recreate should it be damaged beyond repair. The in-use mutability, long lifetime, and difficulty of replacement make older applications brittle and an attractive target for cybercriminals looking to extract a ransom payment. Implementing Zero Trust through DevSecOps techniques turns the conventional wisdom of the cloud being inherently less secure on its head. Somehow organizations also need to cope with users working remotely and accessing applications from networks outside of their physical control. How can Zero Trust principles help with this?

Zero Trust addresses the challenge of securing the remote workforce. The rise of public clouds and Software as a Service (SaaS) had led to a phenomenon known as shadow IT, where departments and business units within an organization bypass the Information Technology department and purchase services directly from vendors, often creating their own applications that run on public cloud providers. While this increase in speed and agility is highly desirable, it creates a set of visibility and accountability problems for the organization. Initially, the perimeter controls were adapted to identify SaaS traffic at the organization edge. Then, as users left the building, the strategy became less effective. Zero Trust empowers Corporate Security teams to regain control of information access and use in this new environment (Saran, C. 2020). By moving the authorization decision directly on the endpoint or application, visibility and control is re-established.

However, because human beings are involved, there are privacy concerns when agents are installed on computing devices that allow for fine-grained monitoring and control. When adopting a Zero Trust framework, technical controls need to be evaluated in the context of the countries' legal restrictions and cultural norms where the organization operates (McKay, P. 2020). For example, Western European countries have strong worker privacy protections with severe repercussions for organizations that violate them (McKay, P. 2020).

Zero Trust Secures the remote workforce by moving security tooling to the end-user device and close to the application instead of depending on the network or location-based controls. What about critical applications and data, the so-called crown jewels?

Zero trust addresses the challenge of securing critical assets. Although many organizations have embraced the public cloud, most keep critical information assets under direct control. Often these assets are long-lived and based on older architectures. A good starting option for protecting these resources is a technique often referred to as macrosegmentation. In this design, the perimeter firewall is moved to the middle of the network and inspects traffic between all network segments Kindervag, J. (2010a). This provides cost-effective protection without disturbing the legacy applications and potentially breaking them. A related and similar option is to provide security controls at the individual port or virtual port level. This technique is often referred to as microsegmentation

For protecting high-value assets, a new technique called Risk-Adaptable Access Control (RAdAC) holds promise. RAdAC was invented by Robert McGraw of the National Security Agency (NSA) in 2009. RAdAC is a policy framework based on several concepts that provide dynamic access control based on risk, operational need, and the importance of the asset relative to the organization's mission (Lee, B., Vanickis, R., Rogelio, F., & Jacob, P. 2017). To implement such an algorithm in a firewall a new policy language is required. Research is active and ongoing, and some of the concepts may start to make appearances in commercial products in the near future. How are these crown Jewels protected from malicious insiders?

Zero Trust addresses the challenge of protecting the organization from both internal and external threats. Internal and external threats are commonly considered as separate cases. However, cybercriminals and malicious insiders often team up. In his 2010 paper *No More Chewy Centers : Introducing The Zero Trust Model Of Information Security* John Kindervag cites a case he refers to as the "Phillip Cummings Problem." From 1999-2000, Phillip Cummings worked for a company that provided software to credit reporting bureaus such as Equifax and Experian. Mr. Cummings entered into a business arrangement with an organized crime syndicate in which he received $60.00 for every credit report (Kindervag, J. 2010b). Mr. Cummings left a laptop on the corporate network that continued to operate and supply information to his Niergian partners for two years after leaving the company. In fact, the software company never discovered the breach; it was discovered by a credit bureau customer (Kindervag, J. 2010b). The pattern of undetected threats persisting on organizational networks, stealing or altering information over long periods of time is not uncommon. The opportunity for this to occur is because of the inherent trust of the internal network in a perimeter-based model. To address this requires two conceptual adjustments. First, all data sources and computing services are considered resources. Secondly, no resource should be inherently trusted (National Institute of Standards and Technology. 2020). To successfully combat internal, external, and combination threats, the security model must not rely on inherent trust and static controls. Zero Trust assumes that the organization network and everything connected to it is no more trustworthy than the public Internet.

Conclusion: Zero Trust is the network security paradigm of the future because it addresses the organizational challenges of securing cloud-native applications, remote workforces, and critical assets from internal and external threats. Cloud-native applications may be secured through DevSecOps Practices and application proxies. Remote workers can be secured through authentication of the user and their devices and through continuous authorization to applications and other resources. The legal requirements and cultural norms of the country in which the workers reside needs to be considered when evaluating the use of agent software to monitor the posture of worker devices. Critical assets (the Crown Jewels) may be secured through resource-specific gateways or general firewalls that evaluate information from multiple sources and grant per-connection access based on need and situational awareness. By always assuming the network to be hostile, practices and architectures that can effectively defend organizations from modern cyberattacks by internal, external, and combination threats have emerged, and organizations should move to embrace them.

References

Gilman, E., Barth, D. (2017). Zero Trust Networks : building secure systems in untrusted networks. Sebastopol, CA: O'Reilly Media.

Kindervag, J. (2010a). Build Security Into Your Network's DNA: The Zero Trust Network Architecture. 1-27. Retrieved from http://www.virtualstarmedia.com/downloads/Forrester_zero_trust_DNA.pdf

Kindervag, J. (2010b). *No More Chewy Centers : Introducing The Zero Trust Model Of Information Security*. 1-15. Retrieved from https://media.paloaltonetworks.com/documents/Forrester-No-More-Chewy-Centers.pdf

Lee, B., Vanickis, R., Rogelio, F., & Jacob, P. (2017). Situational awareness based risk-Adaptable access control in enterprise networks. IoTBDS 2017 - Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security, IoTBDS, 400–405. Retrieved from https://doi.org/10.5220/0006363404000405

McKay, P. (2020). How to find the right zero-trust strategy: Large tech companies and the US Federal Government have adopted zero trust as their next-generation security model. Computer Weekly, 22"24. Retrieved from: https://www.computerweekly.com/feature/How-to-find-the-right-zero-trust-strategy

National Institute of Standards and Technology. (2020). Zero Trust Architecture. NIST Special Publication 800-207, 49. Retrieved from https://doi.org/10.6028/NIST.SP.800-207

Saran, C. (2020). Zero Trust: Taking Back Control of IT Security. Computer Weekly, 15"18. Retrieved from https://www.computerweekly.com/feature/Zero-trust-Taking-back-control-of-IT-security

Ward, R., & Beyer, B. (2014). Beyondcorp : a new approach to enterprise security. ;;Login:: The Magazine of USENIX & SAGE, 39(6), 6"11. Retrieved from https://www.usenix.org/system/files/login/articles/login_dec14_02_ward.pdf