INSTITUTE FOR DEFENSE ANALYSES

Toward a Zero Trust Metric

William R. Simpson, Project Leader

January 2022

IDA Non-Standard D-32912

INSTITUTE FOR DEFENSE ANALYSES
730 East Glebe Road
Alexandria, Virginia 22305

The Institute for Defense Analyses is a nonprofit corporation that operates three Federally Funded Research and Development Centers. Its mission is to answer the most challenging U.S. security and science policy questions with objective analysis, leveraging extraordinary scientific, technical, and analytic expertise.

About This Publication

This work was conducted by the IDA Systems and Analyses Center under contract HQ0034-19-D-0001, Project ITSDPB, "ITSD Publications," for IDA. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

For More Information

William R. Simpson, Project Leader
rsimpson@ida.org, 703-845-6637

Margaret E. Myers, Director, Information Technology and Systems Division
mmyers@ida.org, 703-578-2782

Rigorous Analysis | Trusted Expertise | Service to the Nation

Toward a Zero Trust Metric

Dr. William R. Simpson

Abstract — **Zero trust assumes that all points of trust will be questioned and mitigated, that the individual resources are protected, and that there is no reliance on the network for protection. This helps to limit threat mobility and contain damage. Rules for multifactor authentication and micro-segmentation are often cited as a Zero Trust Architecture (ZTA), but these so-called architectures lack guidelines for the major points of trust in the system. True zero trust is not achievable—only minimal trust can be achieved. Certain trust points are inevitable, such as certificate authorities, policy evaluation, and decision points. There are no metrics measuring whether or not zero trust objectives have been met. It is the goal of this paper to move toward a general metric of trust.**

Index Terms — **Zero Trust, Trust Metrics, Minimal Trust, Network Defense, Networking, Security Architectures**

I. INTRODUCTION

Implementation of Zero Trust Architecture (ZTA) is only the beginning of zero trust (ZT). The items not included in ZTA form the greatest risk to information security. This paper discusses a few of the IT mechanisms that are usually taken for granted and applied alongside a ZT approach.

II. WHY ZT, WHY NOW?

ZT is a new way to structure security defenses to better defend our digital resources against attackers. It is not a product or a security tool, but a way to organize the resources and the tools used to protect those resources. Instead of a network-based defense, which places protections at the network boundary, ZT is a resource-based defense that places protections at each valuable resource. This provides a better match to current threats by directly protecting what is being attacked, and it provides a more resilient defense against lateral movement within an organization. For the Department of Defense (DoD) at this time, the current network defense builds upon a clear concept of the fortress approach. Many of the requirements are based on inspection and reporting prior to delivery of the communication to the intended target. The inspection and reporting require a number of software tools to preclude malicious entities from conducting activities such as exfiltration of data, theft of credentials, blocking of services, and other nefarious activities.

These inspections require decryption of packets, which implies that the defensive suite either impersonates the requestor or has access to the private cryptographic keys of the servers that are the target of communication. This approach has been repeatedly bypassed and defeated by advanced persistent threats. The network-based approach has been repeatedly broken, which shows that it has not been working for some time now. ZT offers a new approach to defend our networks and digital resources.

III. ZT

To fix the problems associated with network defense at the border, a new approach is needed. ZT is better suited to combating the current attack methods while preserving existing end-to-end security measures. ZT changes the one-size-fits-all security approach of a boundary defense to a custom-tailored approach for each resource within that boundary. The defenses are implemented at the resource, so there is no gap between the security and the resource it protects. ZT is an endpoint-based solution. It does not break the end-to-end secure communication channel between requester and resource. It scans at the endpoints and reports findings to a central monitoring facility. This allows requester and provider to authenticate each other directly and perform encryption and integrity from end to end. By focusing on the endpoints, ZT eliminates the man-in-the-middle (MITM) that boundary security introduces.

Many of the new security techniques have moved to a distributed security approach. The ZT framework is a distributed security system that eliminates or mitigates many of the primary vulnerability points inherent with the fortress system, as shown in Figure 1. Each entity needs assurance that the entity and device they are engaged with are known entities and, specifically, the ones to whom the communication should be allowed. However, it is this distributed approach and the requirement for content inspection and reporting that causes the conflict with traditional fortress representation. All active entities and devices in ZT systems have public key infrastructure (PKI) certificates. Identity may be bolstered by using multi-factor techniques, and temporary credentials may be issued when necessary. Communication between active entities requires bilateral, PKI, end-to-end authentication of both the participants and their hardware.

ZT represents a change from current security practice. Instead of protecting resources by blocking outsiders, the protections are placed at the resources themselves. This approach is a better match to the current threats, which are consistently breaking through firewalls and other boundary protections. ZT provides defense against outsiders and malicious insiders, and it blocks attacker lateral movement within an enterprise.

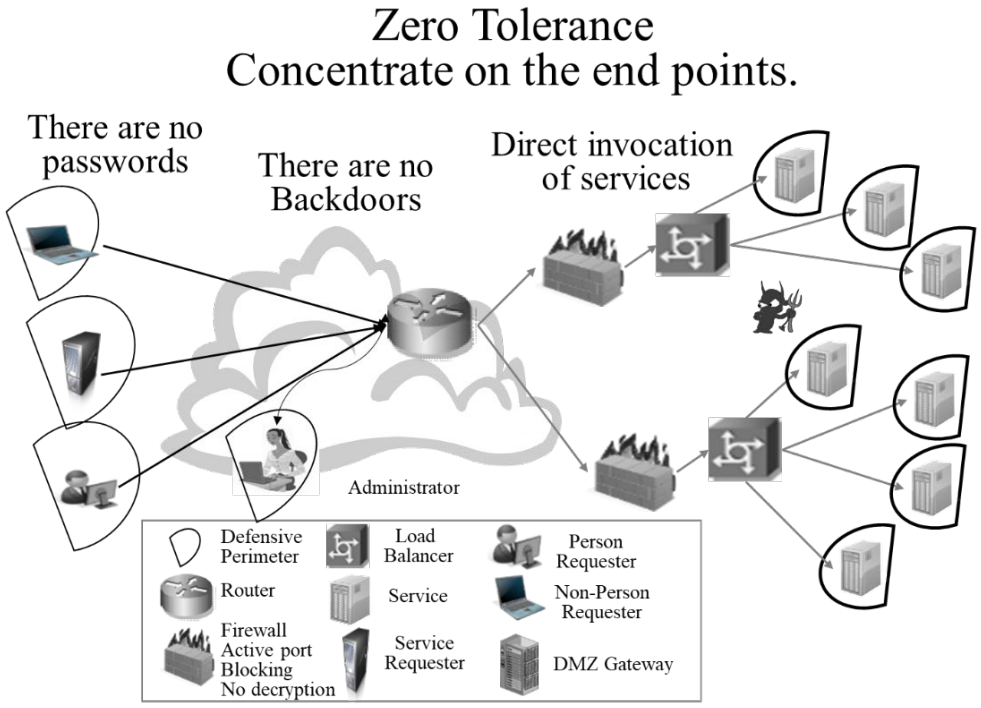

Figure 1. ZT Enterprise

IV. ZT Architecture

To achieve this vision, most architectural representations provide five foundational concepts for a ZT approach:

1. Two-way strongly authenticated communication, often with multi-factor authentication processes.
2. Endpoint device management.
3. End-to-end encryption and integrity. The encryption is not specified as "unbroken," but, for true ZT processes, it should be unbroken between two communicating endpoints.
4. Policy-based authorization. This may include role-based and claims-based access control.
5. Accountability for actions.

In the DoD, these techniques have been fully developed, tested, and verified on the National Cyber Range and are described in the Air Force Consolidated Enterprise IT Baseline [1-3].

ZTA was designed to address lateral threat movement within the network. ZTA embraces the principle of "never trust, always verify." ZTA is a paradigm that moves defenses from network-based perimeters to focus on users, assets, and resources. More information on ZTA is provided by NIST SP 800-207 [7]. However, these simplified architectural elements only partially address the ZT approach. What is clearly missing is an identification of trust points within the information technology (IT) enterprise

V. ZT AND POINTS OF TRUST

A metric is constructed by enumerating the many trust points in an IT enterprise. An arbitrary point value is accumulated when the violation of that trust occurs. The point values are arbitrary but should represent a rough correlation to the egregiousness of the trust violation. The list has been generalized, and other examples may be included, but it is the beginning of a metric basis for ZT. The list will be arbitrarily broken into several categories:

1. Issues of identity verification.
2. Incentives for multi-factor authentication
3. Issues of basic IT architectures as they have evolved.
4. Issues of trust in software tools.
5. Other issues of trust.

VI. ISSUES OF IDENTITY VERIFICATION

A. Use of Passwords for Software/Hardware/User with or without Multifactor

Compromised passwords are the single largest class of factors responsible for enterprise system compromise.

> **"…passwords are the single biggest threat to your online security – they're easy to steal, they're hard to remember, and managing them is tedious. Many people believe that a password should be as long and complicated as possible – but in many cases, this can actually increase the security risk. Complicated passwords tempt users into using them for more than one account; in fact, 66% of Americans admit to using the same password across multiple sites, which makes all those accounts vulnerable if any one falls." [4]**

The use of PKI certificates by a trusted Certificate Authority (CA) is much preferred to passwords. Because of the serious consequences of trusting passwords, using passwords is assessed a value of 20 points.

B. Trust in CA

Entity identities in large enterprises are often managed by a PKI. Standard PKI components include the following:

- Public key certificates
- Certificate repository
- Certificate revocation
- Key backup and recovery
- Non-repudiation of digital signatures
- Automatic update of key pairs and certificates
- Management of key histories
- Support for cross-certification
- Software implementation to use items listed above

Together, these form the basis for an automatic, transparent, and usable PKI [5, 6]. The use of PKI is widespread on the public web as well as within enterprises. Web servers use certificates from trusted CAs to authenticate to users connected from remote locations through potentially untrusted or hostile networks. Enterprises use PKI to provide employees, servers, services, and other entities with a convenient way to encrypt and decrypt data, sign and verify content, and perform third-party authentication, where neither party has an established relationship prior to the authentication.

The use of a trusted CA is a violation of ZT, but considerably less egregious than the use of passwords, and it is assessed a value of 10 points.

C. Use of Default Timeouts for Validation and Verification (V&V) of Certificates

Although PKI is the preferred solution, the CA should be robust enough to validate and verify each presentation of a certificate. Weakly provisioned CAs may not have the hardware and software available to perform these V&V activities at scale. The work-around that many system administrators use is to accept the certificate if the V&V does not respond within a certain, short time-frame.

> **"Insufficient Session Expiration occurs when a Web application permits an attacker to reuse old session credentials or session IDs for authorization. Insufficient Session Expiration increases a Web site's exposure to attacks that steal or reuse user's session identifiers." [7]**

The moral is that one should not give away trust gained by being weak in other aspects of implementation. This takes away much of the benefit of a CA and is assessed a value of 20 points.

VII. INCENTIVES FOR MULTI-FACTOR AUTHENTICATION

Incentives are applied to encourage the use of some techniques that are not widespread at this time. If they become commonplace, these incentives may be dropped from the metrics, just as other factors may be added from time-to-time. Some actual positive factors in authentication include the following:

A. Multi-factor Authentication of Hardware and Software Entities

The advantages of multi-factor authentication are touted throughout the industry (e.g., [8]). This is especially true when combined with a PKI approach. However, the techniques are seldom applied to the software side of the problem. As an extra incentive, the use of multi-factor authentication on software entities is given a bonus value. These benefits provide so much additional security, they are assessed a value of –5 points.

B. Multi-factor Authentication of Servers

The advantages of multi-factor authentication also translate to authentication servers where serial numbers and physical locations may be verified. However, the techniques are seldom applied to the hardware and software side of the problem. As an extra incentive, the use of multifactor authentication on hardware and software entities is given a bonus value. These benefits provide so much additional security, they are assessed a value of –10 points

VIII. ISSUES OF BASIC IT ARCHITECTURES AS THEY HAVE EVOLVED

A. Use of Single Sign-on (SSO)

Single sign-on (SSO) allows users to avoid multiple authentication instances in computer-based sessions. It is a way to centralize authentication for a collection of related resources. It simplifies the process of authentication by providing users a single place to establish their identity and a single method for resources to authenticate requesters. ZTA is a security approach that moves protections away from network borders and to the resources themselves. It removes the ability and need to trust networks, and it requires each requester to prove access based on their credentials at the time of a request. The question is whether these two can work together. The short answer is "no," but the full answer is more nuanced because the term SSO is used somewhat loosely. The concepts of SSO and ZTA show how the most common use of SSO does not work with ZTA.

SSO transfers authentication information between endpoints. The SSO server creates an SSO token after a requester authenticates to the SSO server [9]. This authentication may be tailored to the resource the user is requesting using multi-factor or other methods to provide different strengths of authentication. In addition, the SSO server may provide many different options to accommodate users with different credentials, locations, and devices. The primary motivation to adopt SSO is often ease of use. This applies to both the users and the enterprise. The users have a single portal for authentication that accommodates all users, and the enterprise implements one authentication server and simply implements token processors at the resources. It is centralized, efficient, and easy to use.

However, SSO is typically not secure. Any authentication token that can be reused or transferred between users allows impersonation, which is a fundamental violation of basic security. SSO tokens are often implemented as "bearer

tokens," meaning that the bearer (whether a proper user or attacker) can use the token to authenticate as the associated requester. SSO tokens are protected by Hypertext Transfer Protocol Secure (HTTPS) from SSO server to requester and again from requester to resource, but this piecemeal security leaves a gaping hole at the requester. Tokens that are implemented as a URL parameter or a cookie in the HTTP header can be easily copied and shared among users. The SSO approach is better than no security, but it falls short of the DoD's needs, and the complexity of proper implementation means a one-size-fits-all approach will cater to the lowest security level of the systems it supports.

SSO authenticates on one connection and provides resources on another connection. This violates the ZT assumptions. Although SSO authentication to the SSO server is dynamic and may be strictly enforced, the access is being granted at the resource, and the resource only receives a static SSO token, not a dynamic, interactive authentication. This also violates ZT assumptions.

The problem is that the SSO token provides no guarantee that the holder of the token is the entity named in the token. It is a bearer token. Thus, security relies on externally trusted entities, policies, and practices. This is not the ZT approach.

SSO is a broad term that can mean many things, and some implementations are better than others. However, the key problem for ZTA is the reliance on trust of external elements. One is the user. A user can easily extract, copy, and share the SSO token received from the SSO server. If a user can do it, an attacker can do it too. Often, the attackers are better at this than most users, and stopping these attacks can be difficult due to the contrasting requirements for security and maximum functionality in browsers and web protocols. Usage of SSO in any form is assessed 20 points.

B. Each Software Module that Breaks End-to-End Encryption

Entities in the enterprise may be active or passive. Passive entities include storage elements, routers, wireless access points, some firewalls, and other entities that do not themselves initiate or respond to web service or web application requests. Active entities are those entities that request or provide services. Active entities include users, applications, and services.

Although each of these is unique in its security approach, they all share seamless end-to-end encrypted communications in their architectures as shown in Figure 2. This is a basic conflict with current network defense models, which break this connection at one or more internal components, in effect making them active entities.

Figure 2 illustrates how end-to-end security requires that the front door to the enterprise be passive; however, within the fortress approach, a front door or single point of entry is established. The front door has evolved into a very active set of entities. This is a violation of the end-to-end security and confidentiality of ZT systems and is assigned a value of 20 points for each occurrence.

C. Each Identity Proxy

Identity proxies are provided at various points within the network and are often, but not exclusively, associated with load balancers [10]. These proxies assume the identity of the requester and are a classic MITM in all transactions. They act on the behalf of the user by consolidating web service activities and other features. They may claim to provide security services and are often provided access to hardware storage modules and/or private keys of users and servers. Considerable trust is given to these proxies, though they are not free of vulnerabilities and offer attack vector opportunities for adversaries. They violate several aspects of ZT and should be avoided if at all possible. Each identity proxy in the network is assessed 20 points.

D. Any Unencrypted Traffic Flow

All traffic flows should be encrypted, even those between appliances in the IT infrastructure. Unencrypted transmissions are an egregious violation of ZT concepts and are assessed a value of 20 points.

E. Any Modification of Traffic Content

This prevents the receiver of a message from verifying that the message received was the same as the message sent and is assessed a value of 20 points.

IX. ISSUES OF TRUST IN SOFTWARE TOOLS

A. Each Software Module Allowed Access to Infrastructure Files

Access to infrastructure files is unavoidable for a robust access control system. Each occurrence provides trust to the software model. However, the number and distribution of these software modules should be limited to the extent possible and a penalty of 5 points is assessed for each occurrence.

B. Excessive White Listing of Software Products

White listing is a way to exclude software from the analysis and constraints of zero trust processes. Although some whitelisting is justified for efficiency and trust, excessive white listing causes a violation of trust. Each of the white-listed products has vulnerabilities, both known and unknown (zero-day). Some, but not all, developers are vigilant about remediating known vulnerabilities. None can remediate unknown vulnerabilities. Such a violation led to the Solar Winds [11] incursion in 2019. For computation of the metric, three such white lists are allowed, but a penalty is assessed above that. This violation of ZT is assessed a value of 5 points per occurrence in excess of three.

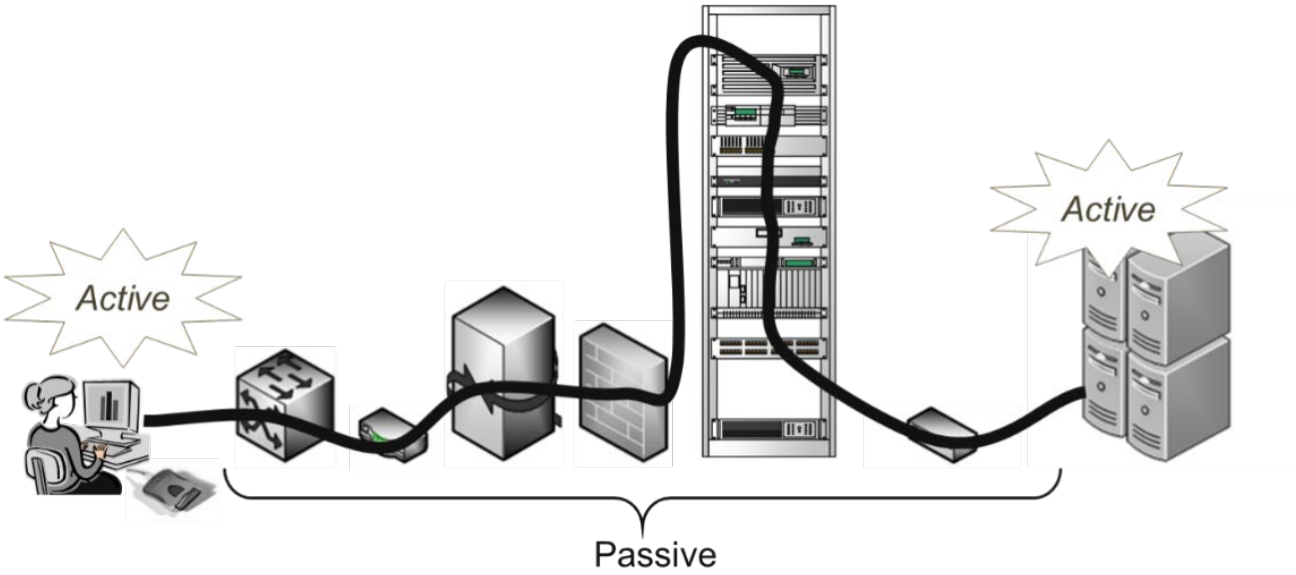

Figure 2. End-to-End Seamless Encrypted Communication

C. Each Software Module Allowed Access to Private Key of Server or HSM of Server

The private key is very close to the identity of an entity, Possession of the private key allows masquerading and reduces overall security by investing a great deal of trust in the software module given that privilege. These software modules are often white listed and not counted in ZT rules. This violation of ZT is assessed a value of 20 points.

X. OTHER ISSUES OF TRUST

A. Any Segmentation Above Micro-segmentation

Network segments containing more than one resource are equivalent to providing SSO and are assessed 20 points.

B. Every Other Instance of Explicit Trust

The diversity of network instantiations makes it impossible to foresee all contingencies; however, explicit trust includes unchallenged or automatic access, failure to verify and validate entities, and other security steps. Such occurrences are assessed 20 points

C. Server-side Authentication Only

This factor was placed in the mix because all communication is two-way. Failure to authenticate the server places implicit trust in that server. Servers may be co-opted and under the control of nefarious agents. Failure to explicitly authenticate these servers is assessed 20 points.

XI. SUMMARY

The proposed metric affords a process for evaluating current practices and measuring progress in achievement of a ZT network. As a yardstick, the relative values between iterations are probably more important than the actual values. It is expected to evolve with usage and architecture development. No doubt additional factors will evolve and these factors will be modified or eliminated. Many of the values in the initial formulation may be changed over time. The factors are summarized in Table 1, and a graphical representation is provided in Figure 3.

Table 1. ZT Factors

Factor	Value
Use of passwords for software/hardware/user with or without multifactor	+20
Trust in CA	+10
Use of default timeouts for V&V of certificates	+20
Each software module allowed access to infrastructure files	+5
Excessive white listing, per occurrence, in excess of 3	+5
Each software module allowed access to private key of server or HSM of server	+20
Use of SSO	+20
Each breakage of end-to-end encryption	+20
Each identity proxy	+20
Any unencrypted traffic flow	+20
Any modification of traffic content	+20
Any segmentation above micro-segmentation	+20
Every other instance of explicit trust	+20
Server-side authentication only	+20
Multi-factor authentication of software	-5
Multi-factor authentication of servers	-10

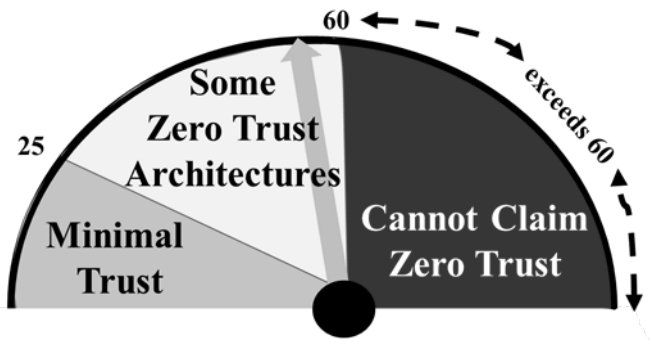

Figure 3. Graphical Scale of ZT

XII. CONCLUSION

There is a significant difference between ZTA and successful implementation of ZT concepts. Each architecture can provide security elements that minimize trust at a given point; however, adherence to ZTA principles does not provide a way to prevent that trust from being given away at other points within the network system. This paper highlights these trust factors. This work is part of a broader-based examination of network architectures, a portion of which are covered in references [12] – [18].

REFERENCES

[1] *Technical Profiles for the Consolidated Enterprise IT Baseline*, release 6.0. https://intelshare.intelink.gov/sites/afceit/ (CAC required).

[2] Simpson, William R., *Enterprise Level Security – Securing Information Systems in an Uncertain World*. Boca Raton, FL: Auerbach Publications, 2016.

[3] Simpson, William R., and Kevin E. Foltz. *Enterprise Level Security 2: Advanced Techniques for Information Technology in an Uncertain World* Abindgon, United Kingdom: Taylor & Francis Group, 2020.

[4] Risher, Mark, "Identity and User Security: A Simpler and Safer Future — Without Passwords," May 06, 2021. Google online safety-security Blog, https://blog.google/technology/safety-security/a-simpler-and-safer-future-without-passwords/, accessed October 7, 2021.

[5] Entrust Datacard, "What Is PKI?" https://www.entrustdatacard.com/pages/what-is-pki, accessed November 27, 2019.

[6] Cooper, D., et al., "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," May 2018. Available at https://tools.ietf.org/html/rfc5280, accessed December 9, 2019

[7] Auger, Robert, WASC Threat Classification, *Insufficient Session Expiration, Threat Type: Weakness*, Reference ID: WASC-47, December 2009. http://projects.webappsec.org/w/page/13246944/Insufficient%20Session%20Expiration, accessed October 7, 2021.

[8] Jones, Isa, SecureLink, *Benefits of multi-factor authentication,* October 01, 2021. https://www.securelink.com/blog/benefits-of-multi-factor-authentication/, accessed October 7, 2021.

[9] Teravainen, Taina. "Single Sign-on (SSO)." https://searchsecurity.techtarget.com/definition/single-sign-on, accessed April 26, 2021.

[10] Afzal, S., and G. Kavitha, 2019, *"*Load Balancing in Cloud computing – A hierarchical taxonomical classification.*" Journal of Cloud Computing* 8, 22. https://journalofcloudcomputing.springeropen.com/articles/10.1186/s13677-019-0146-7

[11] Datta, Pratim, 2021, "Hannibal at the Gates: Cyberwarfare and the Solarwinds Sunburst Hack," *Journal of Information Technology Teaching Cases*. https://doi.org/10.1177/2043886921993126.

[12] Simpson, William R., and Kevin E. Foltz, "Network Defense in an End-to-End Paradigm," in *Proceedings of the 9th International Conference on Software Engineering and Applications (JSE 2020)*, edited by David C. Wyld and Natarajan Meghanathan, pp. 177–187, Zurich, Switzerland, November 21–22, 2020.

[13] Simpson, William R., and Kevin E. Foltz, "Secure Server Key Management Designs for the Public Cloud," The 10th International Conference on Electronics, Communications, and Networks (CECNet 2020), October 25–27, 2020.

[14] Simpson, William R., and Kevin E. Foltz, "Network Defense in an End-to- End Paradigm," in *Proceedings of the 9th International Conference on Software Engineering and Applications (JSE 2020)*, edited by David C. Wyld and Natarajan Meghanathan, pp 177–187, Zurich, Switzerland, November 21–22, 2020, DOI: 10.5121/csit.2020.101414.

[15] Simpson, William R., and Kevin E. Foltz, 2021, "Resolving Network Defense Conflicts with Zero Trust Architectures and Other End-To-End Paradigms," *International Journal of Network Security & Its Applications* 13, no. 1: 1–20. DOI: 10.5121/ijnsa.2021.13101.

[16] Simpson, William R., and Kevin E. Foltz, "Zero Trust Using Delegation of Access and Privilege," Third International Conference on Internet of things, Data and Cloud Computing (ICC 2021), Cambridge, UK, June 2021, in process.

[17] Simpson, William R., and Kevin E. Foltz, 2021, "Maintaining Zero Trust with Federation," *International Journal of Emerging Technology and Advanced Engineering* 11, no. 3: in process.

[18] Simpson, William R., and Kevin E. Foltz, "Network Segmentation and Zero Trust Architectures," Lecture Notes in Engineering and Computer Science, Proceedings of the World Congress on Engineering (WCE) 2021, pp. 201–206, Imperial College, London, July 7–9, 2021.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE (DD-MM-YY)	2. REPORT TYPE	3. DATES COVERED (From – To)
00-01-22	Non-Standard	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Toward a Zero Trust Metric	HQ0034-19-D-0001
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBERS

6. AUTHOR(S)	5d. PROJECT NUMBER
William R. Simpson	ITSDPB
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES	8. PERFORMING ORGANIZATION REPORT NUMBER
Institute for Defense Analyses 730 East Glebe Road Alexandria, VA 22305	NS D-32912

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR'S / MONITOR'S ACRONYM
Institute for Defense Analyses 730 East Glebe Road, Alexandria, VA 22305	IDA
	11. SPONSOR'S / MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

Project Leader: William R. Simpson

14. ABSTRACT

Zero trust assumes that all points of trust will be questioned and mitigated, that the individual resources are protected, and that there is no reliance on the network for protection. This helps to limit threat mobility and contain damage. Rules for multifactor authentication and micro-segmentation are often cited as a Zero Trust Architecture (ZTA), but these so-called architectures lack guidelines for the major points of trust in the system. True zero trust is not achievable—only minimal trust can be achieved. Certain trust points are inevitable, such as certificate authorities, policy evaluation, and decision points. There are no metrics measuring whether or not zero trust objectives have been met. It is the goal of this paper to move toward a general metric of trust.

15. SUBJECT TERMS

Zero Trust, Trust Metrics, Minimal Trust, Network Defense, Networking, Security Architectures

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Institute for Defense Analyses
Unclassified	Unclassified	Unclassified	Unlimited	6	19b. TELEPHONE NUMBER (Include Area Code)