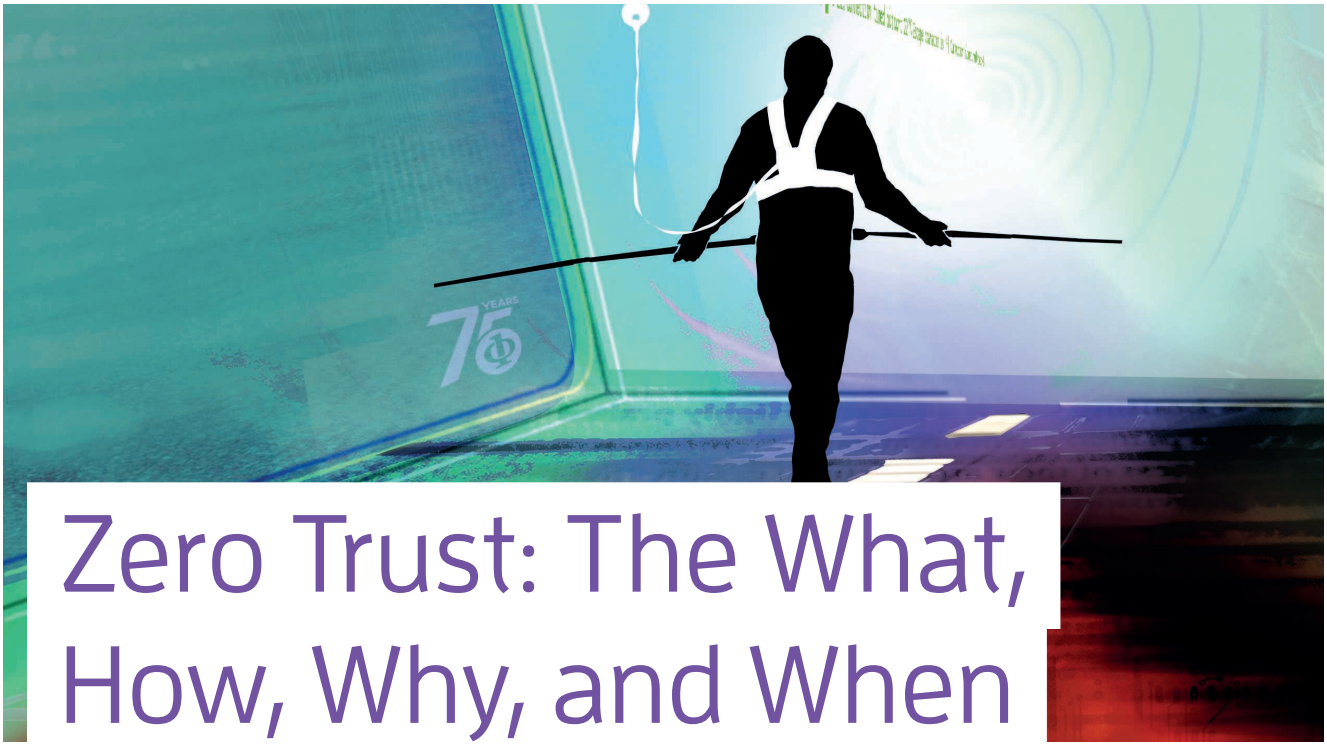

Zero Trust: The What, How, Why, and When

Malcolm Shore, Deakin University
Sherali Zeadally, University of Kentucky
Astha Keshariya, IBM

Trust is a critical characteristic of computer systems, but the traditional approach of evaluating systems has failed to deliver the required levels of confidence. We review the emerging zero trust paradigm and propose a new set of zero trust tenets and an enhanced zero trust model.

With digital transformation, our reliance on IT products, systems, and networks grows and increasingly demands well-implemented and comprehensive security mechanisms. In a dynamic computing environment, we need to have assurance that we can trust the fundamental security mechanisms such as authentication and authorization, data privacy and protection, user privileges, and network security. From an early stage, trust has been a core issue for governments when deploying IT systems, and over the years there have been substantial investments in schemes for promoting trust in technology. The emergence of Internet-borne cyberthreats has brought trust into focus as a vital component of cybersecurity strategies.

The February 2003 National Strategy to Secure Cyberspace[34] focuses on the need for a trusted environment for IT and particularly supervisory control and data acquisition systems (which are an integral part of various types of critical infrastructures) to deliver consumer trust. Strangely, the subsequent Comprehensive National Cybersecurity Initiative,[10] Executive Order Improving Critical Infrastructure Cybersecurity,[35] and National Cyber Strategy of the United States[36] have little or no mention of trust. Despite appearing to have declined as a national strategic priority, the concept of trust remains important and is once again receiving

Digital Object Identifier 10.1109/MC.2021.3090018
Date of current version: 22 October 2021

significant attention from a seemingly different direction: zero trust.

TRUSTWORTHY TECHNOLOGY

Security has always been a consideration for computer systems, with the U.S. Department of Defense's Trusted Computer System Evaluation Criteria (TCSEC)[11] driving an approach based on an evaluation process. In May 1990, the U.K. government first introduced an alternative evaluation scheme, called the *IT Security Evaluation Criteria* (*ITSEC*), subsequently updated in 1991,[12] which is based on assessments against product-specific security functionality while maintaining scheme-defined assurance levels. Eventually, in the late 1990s, the TCSEC and ITSEC approaches were both replaced by a single harmonized set of criteria, referred to as the *Common Criteria*,[7] which was adopted for national use by the United States, the United Kingdom, Canada, Australia, and New Zealand and is now recognized by 28 countries as the means of approving equipment for use by governments and national infrastructure. The Common Criteria approach to trustworthiness has not been successful, however, in delivering an adequate level of confidence in the security of commercial products, and, with the United Kingdom withdrawing from evaluations,[22] the future of the scheme is uncertain.

In the United States, the concept of a tailored trustworthy space as a design for providing trusted enclaves was introduced as a research topic by the federal Networking and Information Technology Research and Development (NITRD) Agency.[25] Tailored trustworthy spaces are individual electronic zones having well-defined security policies that enable potential users of those domains to establish trust within those spaces. NITRD subsequently ran a workshop on tailored trustworthy spaces as a solution for applying security in the smart grid.[26]

Technology trust is also of international interest. The release in 2018 of *China's E-Science Blue Book*[8] included a national priority requirement to develop trusted networks. In the United Kingdom, the National Cyber Security Strategy[6] includes the requirement for industry to deliver trusted systems, and the British Standards Institute published Publicly Available Specification 754, which later evolved to become BS 10754-1: *Information Technology—Systems Trustworthiness*.[5] The BS 10754-1 standard defines five facets of trustworthiness: safety, reliability, availability, resilience, and security. It enhances the engineering for trustworthy systems in several ways, including the definition of, and the approach to the assessment of, trustworthiness levels. Conferences such as the International Conference on Trusted Systems and the Chinese Conference on Trusted Computing and Information Security contribute significantly to the literature.

Software trust is directly related to the existence of defects that could potentially be exploited. In this context, a defect is a software flaw that is not detected by testing prior to release of the software, and the number of defects per thousand lines of source code is a typical quality metric for software development. Several strategies for minimizing defects have been described by Jayaswal and Patton.[16] However, the most effective approach to creating low-defect software is by using high-integrity languages such as Ada/SPARK, which are used extensively in the military, aerospace, and nuclear industries. Such languages not only provide functional code, but also incorporate assertions, also known as *aspects* or *promises*, which enable automated proving tools to verify the integrity of the code. In Croxford and Chapman,[9] the authors showed that processes that are designed to reduce or remove defects in software combined with Ada/SPARK can achieve very low defect rates while at the same time improving the total software life cost by reducing the cost of software maintenance. The wider industry has not embraced Ada partly because of the constraints it applies to make the code more secure, such as strong data typing, and partly because of its reputation for being a difficult language in which to code. New high-integrity languages such as Haskell and Rust are emerging and gaining some attention.[3]

WHAT IS ZERO TRUST?

The concept of *zero trust* has been around since 2011 when it was introduced by Forrester in collaboration with the National Institute of Standards and Technology (NIST).[18] However, it took some years for enabling technology to support its implementation. The zero trust paradigm makes two assumptions.

- First, external and internal threats are present on the network at all times. The network must therefore be prepared to defend against them at all times.
- Second, just because a network is local/internal does not make it trusted. Network intrusion with lateral movement (using access on one system to gain access to another one, deeper in the network) is a proven attacker strategy. Network trust comes from ensuring that access to network resources is effectively controlled.

Zero trust is a paradigm that recognizes that a business's secrets are no longer kept secure behind the corporate perimeter and protected by firewalls. It takes a data-centric approach to security and assumes a hostile environment so that systems should "never trust, always verify." There is no single agreed-on definition of zero trust; however, the following three concepts are commonly associated with zero trust:

- Just-in-time access (JITA) involves authentication and access decisions based on a policy decision made at the time of the access request, and just enough access (JEA) ensures that only those privileges needed to carry out the request are provided for the duration of the request. This requires support from an access control subsystem that can provide automated, real-time response, with a commensurate increase in effectiveness.
- The tokenization or encryption of data is used to avoid exposing sensitive data. By making sensitive data nonsensitive (for instance, by replacing a name with an arbitrary identifier) the data-attack surface is reduced because there are no sensitive data to access. This means that much of the risk, particularly of a data breach, is avoided.
- Access control policies must be dynamic and computed from as many sources of data as possible, and these are sometimes referred to as *adaptive policies*.

Zero trust is not an approach that reduces the need for assurance to be applied to security mechanisms. Take, for example, the security mechanisms used to achieve privacy in a system holding personal information. These mechanisms may include pseudonymity, role-based access control, encryption, and so on. For a user to trust that the system will maintain privacy for his/her information, there must be some form of assurance that the security mechanisms will do their job correctly. Zero trust is an access control approach that removes the assumption of trust based on past decisions and ensures that trust is established every time at the point of decision making. In this way it increases assurance that the access control decision is correct. The zero trust mechanisms themselves will then require the same level of assurance as any other mechanism to enable user trust.

WHY IS ZERO TRUST IMPLEMENTED?

A nation state-sponsored cyberattack on Akamai in 2010[32] resulted in the company creating an access model that separates application access from network access, using concepts that subsequently emerged as the zero trust paradigm. Akamai introduced a web interface for network access to applications and services, with both the users and the devices they use for access authorized on a case-by-case basis. The approach is designed to limit the damage that attackers can cause if they do manage to gain access to a user account, as they would be limited to 1) access to the specific tools and services available to that particular user and 2) access to the particular service authorized in the request. The opportunity for lateral movement is reduced, which substantially restricts the damage an intruder can do.

There is no single reason for implementing zero trust. In general, implementing a zero trust architecture is justified as a means to improve security. Microsoft[21] suggests that a new security model—zero trust—more effectively adapts to the complexity of the modern environment; embraces the mobile workforce; and protects people, devices, apps, and data wherever they are located. Steve Hunter, a senior director at Forescout, recommends adopting a zero trust approach to improve visibility, reduce infrastructure expenditure, reduce compliance effort, support a more cohesive approach to resolving IT issues, and enable digital transformation.[15] Li promotes the idea that zero trust shows promise for securing unmanaged devices that might be unable to run computationally expensive cryptographic suits.[19] It is likely that a deeper understanding of the benefits of taking a zero trust approach will emerge as the technology becomes more widely adopted.

HOW IS ZERO TRUST ARCHITECTED?

NIST zero trust architecture

In 2020, NIST published the second draft of its Special Publication on Zero Trust Architecture (SP 800-207),[24] which presents seven tenets of zero trust.

- All data sources and computing services are considered as resources.
- All communication is secured regardless of network location.
- Access to individual enterprise resources is granted on a per-session basis.
- Access to resources is determined by dynamic

policy using trigger conditions and rules set by a policy administrator.
- The enterprise ensures that all connected devices are secure.
- Resource authentication and authorization are dynamic.
- Information is collected about the network environment.

SP 800-207 describes an architecture for zero trust that comprises an untrusted zone, a policy domain that mediates access, and (behind that) what is known as an *implicit trusted zone*, as shown in Figure 1. The policy domain has three related parts: the policy engine and the policy administrator, which together form the policy decision point, which is used to determine whether access will be permitted or not; and the policy enforcement point, which enables or denies access based on the decision made. These are often colocated capabilities.

When an identity (such as a user) in the untrusted zone wishes to access a resource such as data or an application, the first check is on the authentication of the identity. The level to which authentication is carried out may change depending upon the environment. The next check would be to determine whether the security posture of the user satisfies the level of security needed to be allowed access. The authenticator makes the policy decision using risk-based policies, which can change at any time to reflect the latest situation; it is designed to support both human and device identities; and it uses a trust algorithm to make access decisions.

While the key security mechanisms are the policy decision and enforcement points supported by data access policy and identity subsystems, there are many other items that support a fully featured zero trust architecture. These include a public-key infrastructure, threat intelligence, a logging and monitoring subsystem, a continuous diagnostics and mitigation subsystem, and security information and event management.

Forrester has evolved the initial concept of zero trust into a more advanced zero trust extended (ZTX) ecosystem framework,[14] as Figure 2 depicts. ZTX supports an extended set of dataflows across local networks and cloud infrastructure and also through external applications, websites, and a wide range of endpoint devices, including items such as Internet of Things (IoT) sensors.

Another approach to zero trust is through Gartner's continuous adaptive risk and trust assessment.[28] This approach is based on continuous monitoring and risk management, and it has seven elements. First, it requires full device visibility and automated control and then the adoption of

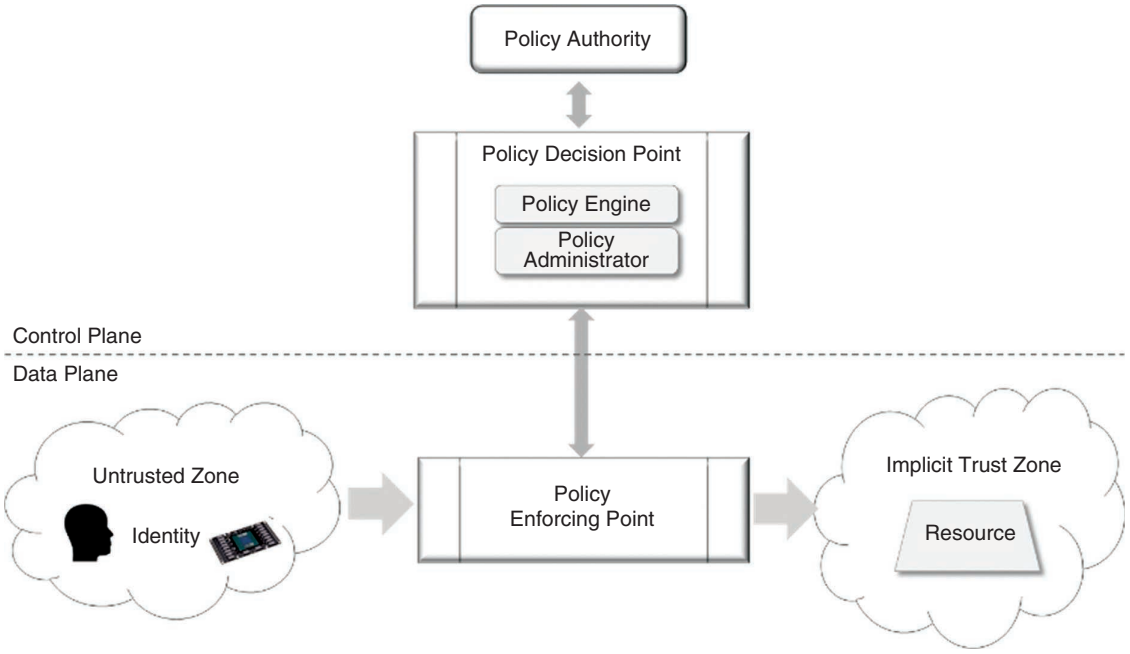

FIGURE 1. A zero trust architecture.

microsegmentation to contain breaches and limit lateral movement/damage as well as the use of technologies and products from multiple vendors to provide defense in depth. It requires multivendor orchestration and process/response automation; it requires the ability to manage an extended set of endpoint devices, including agentless IoT devices and cyberphysical operational technology systems; it provides for continuous monitoring, assessment, and remediation of cyber and operational risk; and, finally, it includes discovery, posture assessment, and remediation/control of physical and virtual devices as well as cloud infrastructure and workloads.

Zero trust risk considerations

SP 800-207[24] notes that the overall process of risk management will not change in a zero trust architecture, and that enterprises will need to develop risk-based policies. In line with this, Vanikis extends earlier work on a fuzzy risk framework to enable risk-based access control decisions to be made in zero trust networks.[31] The research proposes the PAROLE language, which incorporates the Firewall Access Control List generic language for firewall rules. This research provides a useful example of how policy decisions can be described and mapped to real-world devices. While this addresses the issue of making risk-based decisions, it does not address the new or enhanced risks that will be introduced when a zero trust architecture is adopted.

While zero trust assumes that there is no inherent trust in authentication and authorization, it relies upon a dynamic assertion of trust to justify the access decision. This is a more complex decision than it is with traditional access control. It requires a policy authority to set comprehensive trigger conditions and rules through which policy decisions can be made, and, arguably, it needs to be supported with more trustworthy security mechanisms. Certainly, the success of a zero trust technology depends upon it being able to provide a high level of confidence that its dynamic user authentication and access control mechanisms are effective.

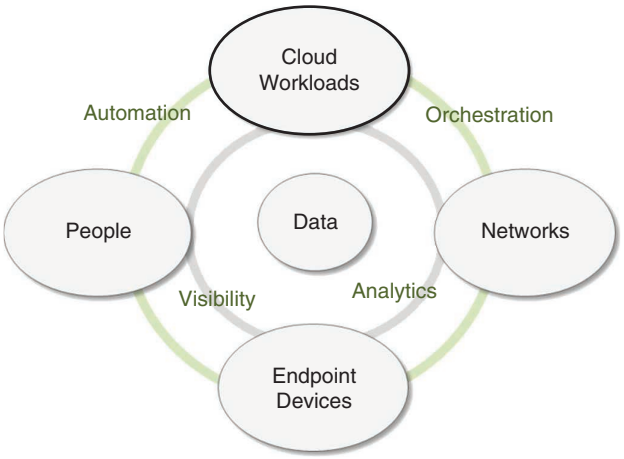

FIGURE 2. The ZTX framework.[14]

Traditional access control is typically managed using a business authority access approval process. Zero trust introduces the role of a policy authority to establish a policy- and rule-based access approval with dynamic decision making. Any errors made in the rules will undermine the effectiveness of the zero trust architecture.

Traditional access control was developed in a primarily human-access context, but digital transformation will increasingly see the use of autonomous systems and intelligent agents. The concept in the automotive context of an autonomous system being the user is discussed in Behere and Liljevquist.[4] More generally, Zero Networks has released its Zero Networks Access Orchestrator, which automatically defines, enforces, and adapts user- and machine-level network access policies.[30] This level of automation goes beyond dynamic access decision making and introduces new risks associated with automatic policy creation.

Architecting zero trust e-commerce

Using analytics for situational information, including location, time of day, device type, and so on provides an operational context to enable a zero trust policy-based access decision to be made effectively. However, the architectural context is also important in determining whether zero trust mechanisms must be invoked. A backend database system may need to be microsegmented and take a zero trust access approach, but the e-commerce website that reaches back to it will continue to be open to the Internet and likely offer anonymous browsing with no requirement to apply a zero trust mechanism. Cloud solutions such as

Amazon Web Services routinely apply security groups to achieve microsegmentation among load balancers, webservers, and databases with zero trust mechanisms becoming more critical the deeper into the network the access reaches. While informal designs are useful, further research is needed to develop robust zero trust patterns for e-commerce.

While the vendor can use the zero trust model to improve protection of its IT infrastructure, the question of how the customer can gain improved trust in the web service is an open one. The same website used for browsing may also act as a proxy for customers to log in and place orders, and customers need to have trust that their credentials, credit card details, and privacy will be protected. The conventional approach of using certificates to validate the authenticity of the website has not been successful.[20] Further research is required into developing reverse zero trust mechanisms that enable improved customer trust.

OUR PROPOSED EXTENDED APPROACH TO ZERO TRUST

The extended set of zero trust tenets

We propose an extended set of zero trust tenets, as shown in Table 1, that is founded on and extends the NIST zero trust tenets.[24] Note that collecting extensive information about user activity has the potential to introduce significant risk to the privacy of system users. The adoption of this tenet must be balanced with the requirements of privacy, particularly in jurisdictions that are covered by the European General Data Protection Regulation requirement, where failure to meet the requirement exacts a heavy toll.

An enhanced model of zero trust

In addition to the revised set of zero trust tenets, we propose a model of zero trust that extends the model defined by NIST in SP 800-207[24] by taking into account a more extensive situational awareness and the practicalities of operational deployment. In this model, shown in Figure 3, the subject and the endpoint are both taken into account when making the access decision, as seen in Forrester's ZTX ecosystem in Figure 2. In addition, the security postures of both the subject and the endpoint, as recorded in an environment monitor that maintains

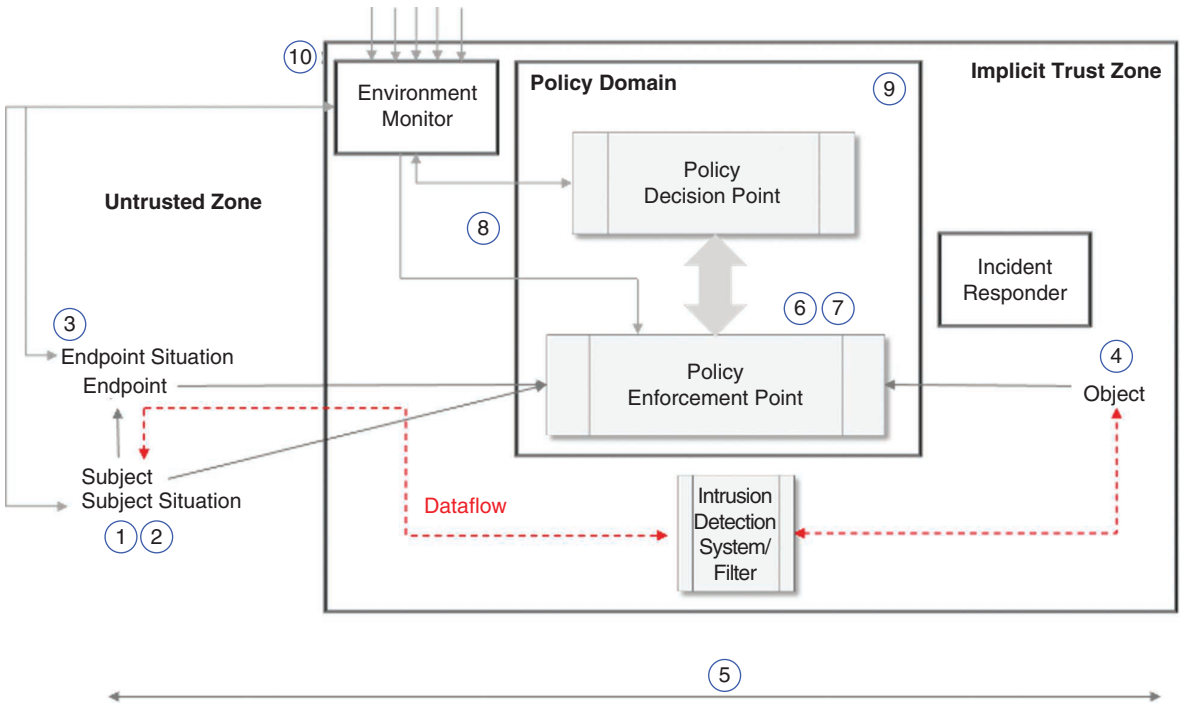

FIGURE 3. A proposed zero trust architecture model based on NIST's zero trust model (adapted from NIST[24]).

TABLE 1. The extended set of zero trust tenets.

	Revised zero trust tenet	Description	NIST SP 800-207
1	All subjects will be considered untrusted and subject to access control.	All users, including local and remote employees, service providers, and contractors, will be considered to be on an untrusted network and subject to access control via a common portal.	This is consistent with NIST Tenet 1.
2	Nonperson entities shall be considered access-mediated subjects.	The entity requesting access may not be a real person but an application on the same or another server, a serverless code function, an IoT sensor, some form of software-based artifical intelligence, or other such autonomous entity. They will be managed no differently than a human subject.	The use of nonperson entities is mentioned as an open item in NIST rather than a recognized entity.
3	All endpoint devices shall be access mediated.	For a zero trust solution, the trust in the technology being used by the subject to access the data is a significant consideration in the access policy decision. Hence, the endpoint and its security posture are a recognized element in the access request. We note that the endpoint may be a hardware-based sensor, workstation, or server or it may be a cloud application, serverless function, or similar.	This is covered in part by NIST Tenet 5, noting that the definition is not just device or application but can also include serverless functions or similar.
4	All objects will be microsegmented and accessed via a policy enforcement point.	A subject will make an access request for data or a service. This request may involve a number of discrete objects (also known as *resources*) such as load balancers, servers or applications, and data stores. Each object will be individually protected with its own perimeter and require a policy-based access control decision. This is fully consistent with attribute-based-access control (ABAC),[23] in which decisions are based on attributes that may change rapidly. ABAC and zero trust may thus be synergistic when applied in practice, as zero trust incorporates the notion of the continuous checking of policy and environment attributes of subjects and their access devices.	This is consistent with the discussion of resources across the NIST tenets. This tenet takes a microsegmentation approach, which may be as small as the resource itself.
5	All communications should be secured end to end from endpoint to object to ensure data source authentication, confidentiality, and integrity.	Ensuring data are protected is one of the two key aspects of zero trust, and this tenet supports that. It also ensures that source information which is not yet within the scope of the zero trust architecture is protected during ingress. However, not all endpoints (for example, IoT sensors) may have the capability to apply protection. When an endpoint does not provide data protection, and sensitive data are exposed to and from the endpoint, this will be taken into account in the access decision.	This aligns with NIST Tenet 2, noting that some endpoints may be unable to provide transmission security and this can be a risk-based consideration.
6	Access to objects is granted on a per-object/per-session basis.	Trust in both the entity and the endpoint is evaluated at the time of access, taking into account the requested object's access rules, to decide whether to grant access. Authentication and authorization take place in real time and are limited to the purpose and period of the session. Multifactor or other forms of advanced authentication may be required for access to some or all objects. Continuous monitoring with possible reauthentication and reauthorization may occur throughout the session, as defined and enforced by policy. Within a session, access to one object (resource) does not imply approval to access another object.	This aligns with NIST Tenets 3 and 6 and also covers some aspects of NIST Tenet 4 for asset status.
7	Privileges necessary for taking action on an object are granted on a per-object/per-session basis.	Least privilege principles are applied at each session to restrict subject visibility and accessibility to that required and no more. Privileges authorized for one object do not carry over to other objects.	This is covered in NIST Tenet 3, but not as a per-session issue.
8	Adaptive policies are used to make access decisions.	The policy that determines levels of trust and access decisions is dynamic and can change based on the observed state of the network. Policies may be rule based or may be more sophisticated, such as in the case of an artificial intelligence -based learning scheme. In all cases, the rights of an entity or an endpoint to access a resource may change over time. For example, the perceived threat level in the network or threat intelligence that identifies that the endpoint software may be vulnerable to a new exploit will change as new exploits emerge, and this will affect whether access is granted.	This aligns with NIST Tenet 4.

(*Continued*)

TABLE 1. The extended set of zero trust tenets. (*Continued*)

	Revised zero trust tenet	Description	NIST SP 800-207
9	The security mechanisms associated with the zero trust architecture will be sufficiently trustworthy to ensure confidence in the zero trust deployment.	Security products used in the zero trust deployment should have evidence of being developed and released using a formal trustworthiness engineering process, with evidence that they satisfy the requirements of recognized trustworthiness standards (such as British Standard 10754-1[5]) or are otherwise able to be assured as having a high level of integrity.	The issue of security mechanisms trustworthiness is not discussed in SP 800-207.
10	Situational information is collected and used to improve decision making, taking into account the requirement for privacy.	Operational data including the current update and patch state of network infrastructure, threat intelligence, traffic patterns, access requests, and so on are collected and used to improve policy creation and enforcement by having better situational awareness. These data can also be used to provide context for access requests from entities but need to take account of user privacy rights. Threat intelligence will be a key source of collected data. There will be a constant cycle of monitoring access, scanning and assessing threats, adapting, and continually re-evaluating trust in ongoing communications.	This aligns with NIST Tenet 7.

situational awareness, will be used when making the access decision. Once a positive decision is made, access is granted and the data are allowed to flow through an intrusion detection and filtering gateway. The points at which each of the proposed tenets comes into play are shown on the diagram.

Several networking vendors (such as Cisco and Illumio) have begun marketing zero trust products, using the terminology *zero trust network access*. These products have a core of JITA/JEA capability with individual products having their own set of extended capabilities, including sandboxing to ensure access does not extend beyond the application to the underlying network, enforcement of endpoint device hygiene requirements, encryption of network traffic, traffic monitoring and packet inspection to detect malware and sensitive data exposure, microperimeters around applications, and creation of an application-specific zoning architecture. The selection of specific products will influence how zero trust is architected.

Moving to a zero trust architecture is not without its challenges, and, as with any other change, planning ahead is essential. Francis provides guidance on how to implement zero trust.[13] The first step is to define the scope of the zero trust deployment. Then, before starting implementation, identify the data assets, the users, and the physical IT assets that will be within scope. The dataflows between clients and servers, and also internally between servers, must be well understood. Once it is clear who is accessing what, the access control permissions can be defined and the data assets and applications segmented appropriately. This can be done by moving the data and applications into an appropriate microsegmented network. Each network microsegment will then need to have a defined appropriate access policy.

WHEN TO SWITCH TO ZERO TRUST?

While research into zero trust models continues, such as the use of access control proxies,[1] vendors are now delivering zero trust products and services to enable businesses to adopt zero trust. Zero trust thought leaders such as Akamai[2] not only promote their services but have implemented zero trust in their own internal networks, and others are in the process of doing so. Several other large organizations have adopted zero trust already. In 2014, Google initiated the BeyondCorp program to implement zero trust in their network infrastructure.[33] Palo Alto has deployed zero trust,[27] and GitLab has also adopted a zero trust architecture.[29]

For some businesses, a trigger event such as an intrusion will instigate a move to a robust zero trust architecture. For others, zero trust may be introduced as network equipment is replaced, taking advantage of the zero trust capabilities of replacement equipment. For most businesses, however, it is likely that alignment with business changes, such as introducing more extensive work-from-home opportunities for staff, will provide the most compelling reason for adopting a zero trust strategy.

Zero trust, initially proposed in 2011, is quickly becoming a more accepted approach with zero trust security products emerging to support deployments. The standards community is increasingly providing clear guidance on the paradigm, concepts, and techniques used to deliver trusted technology, and research and commercialization of zero trust concepts have helped to evolve the paradigm. We have explained the current notions of zero trust and proposed a contemporary zero trust architecture and an extended set of zero trust tenets.

ACKNOWLEDGMENTS

We thank the editor and the anonymous reviewers for their valuable comments, which helped us improve the content and presentation of this article.

ABOUT THE AUTHORS

MALCOLM SHORE is an adjunct professor at Deakin University Cyber Security Research Institute in Melbourne, Victoria, 3125, Australia. His research interests include cryptography, cybersecurity architecture, and cyberwarfare. Shore received a Ph.D. in information systems security from Otago University, New Zealand. Contact him at malcolm@autumnriver.co.nz.

SHERALI ZEADALLY is a professor at the College of Communication and Information, University of Kentucky, Lexington, Kentucky, 40506, USA. His research interests include cybersecurity, privacy, Internet of Things, computer networks, and energy-efficient networking. Zeadally received a doctoral degree in computer science from the University of Buckingham, England. Contact him at szeadally@uky.edu.

ASTHA KESHARIYA is with IBM, Changi Business Park, 486048, Singapore. Her research interests are in projects for the financial and payment industry and business models for security and cognitive solutions in accordance with regulatory requirements. Keshariya received a Ph.D. from the Department of Information Science, Otago University, New Zealand. Contact her at keshariya.astha@gmail.com.

REFERENCES

1. I. Ahmed, T. Nahar, S. Urmi, and A. Taher, "Protection of sensitive data in zero trust model," in *Proc. Int. Conf. Comput. Adv.*, Jan. 2020, pp. 1–6, Art. no. 63.
2. "Zero trust security," Akamai, Cambridge, MA. Accessed: Jan. 15, 2021. [Online]. Available: https://www.akamai.com/us/en/solutions/security/zero-trust-securit-model.jsp
3. C. Allen, "Haskell and Rust," FPCOMPLETE.com. Accessed: June 30, 2020. [Online]. Available: https://www.fpcomplete.com/blog/2018/11/haskell-and-rust
4. S. Behere and B. Liljevquist, "Towards autonomous architectures. An automotive perspective," Dept. of Marine Design, Royal Inst. of Technol., Stockholm, Sweden, Tech. Rep. TRITA-MMK-2012:0 ISSN 1400 1179.
5. *Information Technology – Systems Trustworthiness Part 1: Governance and Management Specification*, BS 10754-1: 2018, 2018.
6. "National Cyber Security Strategy 2016–2021 progress report," Cabinet Office, U.K. Government. Accessed: June 30, 2020. [Online]. Available: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021-progress-so-far
7. Common Criteria for Information Technology Security Evaluation. Accessed: June 30, 2020. [Online]. Available: https://www.commoncriteriaportal.org/cc/
8. Chinese Academy of Sciences, Cyberspace Administration of China, Ministry of Education of the People's Republic of China, Ministry of Science and Technology of the People's Republic of China, Chinese Academy of Social Sciences, National Natural Science Foundation of China and Chinese Academy of Agricultural Sciences, *China's eScience Blue Book 2018*. Singapore: Springer-Verlag, Jan. 9, 2021.
9. M. Croxford and R. Chapman, "Correctness by construction: A manifesto for high-integrity software," *J. Defense Softw. Eng.*, vol. 18, no. 12, pp. 5–8, Dec. 2005.
10. "National Security Presidential Directive 54/Homeland Security Presidential Directive 23," DHS, Comprehensive National Cybersecurity Initiative (CNCI), NSPD-54/HSPD-23, Washington D.C., Jan. 2008.
11. "Trusted computer system evaluation criteria," U. S. Dept. of Defense (US DoD), CSC-STD-001-83, Aug. 15, 1983. Accessed: June 30, 2020. [Online]. Available: https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/dod85.pdf
12. "Information technology security evaluation criteria," U.K. Dept. of Trade and Industry (UKDTI), June 1991. Accessed: June 30, 2020. [Online]. Available: http://www.iwar.org.uk/comsec/resources/standards/itsec.htm
13. P. Francis, "Security think tank: Zero trust strategies must start small, then grow," ComputerWeekly.com, Feb. 18, 2020. Accessed: July 1, 2020. [Online]. Available: https://www.computerweekly.com/opinion/Security-Think-Tank-Zero-trust-strategies-must-star-small-then-grow
14. "The Forrester Wave: zero trust eXtended (ZTX) ecosystem providers," Forrester, Q4 2018. Forrester

Research, Cambridge, MA, Rep. E-RES137210, Nov. 2018.
15. S. Hunter, "The five business benefits of a zero trust approach to security," securitybrief.com, Aug. 19, 2020. Accessed: Jan. 15, 2021. [Online]. Available: https://securitybrief.com.au/story/the-five-business-benefits-of-a-zero-trust-approach-to-security
16. B. Jayaswal and P. Patton, *Design for Trustworthy Software: Tools, Techniques, and Methodology of Developing Robust Software*, 1st ed. Englewood Cliffs, NJ; Prentice-Hall, 2006.
17. S. Keeriyattil, "Microsegmentation and zero trust: Introduction," in *Zero Trust Networks with VMware NSX*. New York: Apress, 2019.
18. J. Kindervag, "Applying zero trust to the extended enterprise," Forrester Research, Cambridge, MA, Rep. E-RES60253, Aug. 2011.
19. S. Li, "Zero trust based Internet of Things," *EAI Endorsed Trans. Internet Things*, vol. 5, no. 20, June 2020. doi: 10.4108/eai.5-6-2020.165168.
20. S. Marwaha and P. S. Seshadri, "Convenience vs security in online shopping," Entrepreneur India, Aug. 26, 2020. Accessed: Jan. 23, 2021. [Online]. Available: https://www.entrepreneur.com/article/355333
21. "Enable a remote workforce by embracing zero trust security," Microsoft Corp., Redmond, WA. Accessed: Jan. 15, 2021. [Online]. Available: https://www.microsoft.com/en-nz/security/business/zero-trust
22. "The NCSC and the common criteria scheme," NCSC. Accessed: June 30, 2021. [Online]. Available: https://www.ncsc.gov.uk/information/common-criteria-0
23. *Special Publication 800-162 - Guide to Attribute Based Access Control (ABAC) Definition and Considerations*. National Institute of Standards and Technology, Gaithersburg, MD.
24. "Zero trust architecture," NIST Gaithersburg, MD. Accessed: Jan. 15, 2021. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf
25. "NITRD tailored trustworthy spaces program suggests avenues for research," NITRD. Accessed: June 30, 2021. [Online]. Available: https://www.securityarchitecture.com/nitrd-tailored-trustworthy-spaces-program-suggests-avenues-for-research/
26. NITRD, "Tailored trustworthy spaces: Solutions for the smart grid," in *Proc. NITRD Workshop*, Arlington, TX, July 2011. Accessed: June 30, 2021. [Online]. Available: https://www.nitrd.gov/pubs/NITRD_TTS-SmartGrid_Workshop_2011.pdf
27. "Zero trust deployment at Palo Alto Networks." Palo Alto, Santa Clara, CA. Accessed: Jan. 15, 2021. [Online]. Available: https://www.paloaltonetworks.com/resources/use-case/zero-trust-deployment-at-palo-alto-networks
28. K. Panetta, "The Gartner IT security approach for the digital age smarter with Gartner," Gartner, Stamford, CT, June 2017. Accessed: June 30, 2021. [Online]. Available: https://www.gartner.com/smarterwithgartner/the-gartner-it-security-approach-for-the-digital-age/
29. M. K. Pratt, "Zero-trust model case study: One CISO's experience," TechTarget. Accessed: Jan. 15, 2021. [Online]. Available: https://searchsecurity.techtarget.com/feature/Even-with-a-roadmap-zero-trust-model-an-ongoing-process
30. D. Schalm, "Zero Networks launches industry's first autonomous network access orchestrator," securityboulevard.com, Feb. 20, 2020. Accessed: Jan. 15, 2021. [Online]. Available: https://securityboulevard.com/2020/02/zero-networks-launches-industrys-first-autonomous-network-access-orchestrator-announces-4-65-million-in-funding/
31. R. Vanickis, P. Jacob, S. Dehghanzadeh, and B. Lee, "Access control policy enforcement for zero-trust-networking," in *Proc. 29th Irish Signals Syst. Conf.*, June 2018, pp. 1–6.
32. J. Vijayan, "How Akamai implemented a zero trust model," CSOOnline.com, May 2019. Accessed: June 30, 2021. [Online]. Available: https://www.csoonline.com/article/3392820/how-akamai-implemented-a-zero-trust-model.html
33. R. Ward and B. Beyer, *BeyondCorp: A New Approach Enterprise Security*, vol. 39, no. 6, 2014. Accessed: Jan. 15, 2021. [Online]. Available: https://research.google/pubs/pub43231/
34. "The National Strategy to secure cyberspace," U.S. Government, Feb. 2003. Accessed: Sept. 12, 2021. [Online]. Available: https://us-cert.cisa.gov/sites/default/files/publications/cyberspace_strategy.pdf
35. "Executive order improving critical infrastructure cybersecurity," U.S. Government, Feb. 2013. [Online]. Available: https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
36. "National cyber strategy of the United States of America," U.S. Government, Sept. 2018. Accessed: Jan. 15, 2021. [Online]. Available: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf