Zero trust: Never trust, always verify

CyberSA
Allison Wylde
Marketing and Strategy
Cardiff University Business School
Cardiff University, Wales, UK
wyldea@cardiff.ac.uk

***Abstract*—This short paper argues that current conceptions in trust formation scholarship miss the context of zero trust, a practice growing in importance in cyber security. The contribution of this paper presents a novel approach to help conceptualize and operationalize zero trust and a call for a research agenda. Further work will expand this model and explore the implications of zero trust in future digital systems.**

***Keywords*— zero trust, no presumptive trust, zero knowledge, negative expectations, safe digital systems, control, risk, trust**

I. Introduction

Trusted digital systems allow the safe operations of societal and organizational activities. Yet healthcare and research sectors are current targets of nation state actors and cyber criminals actively stealing data [1], hence the importance of understanding how to secure these systems.

Central in the scholarly trust literature is a view that trustors hold positive expectations of trustworthy behaviour of the other party [2],[3]. Arguably, this is demonstrated by the doveryai, no proveryai, "trust but verify" words of former US President Ronald Reagan used in the 1980s nuclear arms talks with former Russian President Mikhail Gorbachev [4]. While this approach remains pervasive, as illustrated by a recent IEEE Standards paper on AI calling for businesses to build deep trust with their customers [5]; a call for zero trust has emerged in cyber security, notably [6].

Although much is published about trust, in particular the formation of trust, notably the Mayer, Davis and Schoorman Integrative Trust Model (ITM) [3], little is known about how this may be applied in contexts of zero trust and zero trust architectures. In addressing this gap in the scholarly trust and organization studies literature, previous research on zero trust is also extended. Zero trust thinking, therefore, may herald a reversal of "trust but verify"; a paradigm shift, to never trust and always verify, notably, [7],[13].

This extended abstract/ short paper proceeds by first reviewing prominent thinking in zero trust, briefly discussing zero knowledge proof systems and then revisiting the widely cited integrative trust formation model (ITM) [3], with special attention paid to the key assumptions and processes in trust formation [2],[3]. These key issues are then further examined and characterized in a zero trust context. Next, drawing on the findings from this exploration, important steps in the ITM are unravelled in contexts of zero trust and zero trust architectures. Finally a fresh conceptual framework is presented to help our understanding of zero trust and zero trust architectures.

II. Zero Trust

The term zero trust, coined in 2016 by John Kindervag [6], is proposed as a cyber security solution to security concerns that have arisen as a consequence of an overreliance on trust and trusted systems, notably, [7],[13]. Further, as organizational boundaries have became blurred, with links reaching into the cloud and the Internet of Things (IoT) [11] and with third-parties inside the network [7],[9], many now view trust as a vulnerability [6],[7]-[13].

In this paper, zero trust is viewed as based on no presumptive trust, and a risk-based approach to trust, along with verification of trust on a continuous basis[1] [7],[13]. Traditional perimeter-based security with a fixed-trust boundary is considered as no longer secure since individuals cannot be trusted simply on the basis of their location, whether inside or outside of the network [6],[7]-[13].

The UK's National Cyber Security Centre (NCSC) released guidance on zero trust architectures in 2019 [7], further developed through calls for open source input 2020 [7]. Zero trust architectures rely on the removal of inherent trust networks; NCSC suggest that attackers are able to move laterally because everything on the network is trusted. [7],[8]. In a zero trust architecture the network is treated as hostile; instead, confidence has to be gained through the authentication, verification and authorization of users, devices and services [7],[8].

Zero trust and zero trust architecture thinking views identity as the start of the verification process, with trust flowing from identity, device state and context, and not just location. Identity is central to this view, and identity is not simply an individual person, it can also be a thing (a device) or a process, or service [7], for example, the IoT [10]. Developing this approach, the NCSC proposes ten principles for zero trust: (1) knowledge of the architecture, users, devices and services; (2) the creation of a single strong identity; (3) a strong device identity; (4) authenticate everywhere; (5) knowledge of the health of devices and services; (6) monitoring devices and services; (7) policies based on the value of the devices and services; (8) control access to devices and services; (9) don't trust the network, including the local network; and (10) choose services designed for zero trust [7]. The NCSC's approach relies on both policy and authorization-based decision-making [7],[8]. Security thus involves the continuous prioritization of organizational-critical data, assets and services (DAAS); data identification, monitoring and protection [11]; and, for an extended review, see [12].

The National Institute of Standards and Technology (NIST) in the US' special publication on zero trust highlights that zero trust was in use prior to its naming [13], in early forms such as black core. This form of security focused on individual transactions and the de-perimeterization security [13]. The definition for operative zero trust (ZT) states that: "ZT provides a collection of concepts and ideas designed to

[1] Drawing on definition as suggested by C-MRiC anonymous reviewer3.

minimize uncertainty in enforcing accurate least privilege peer-request-access decisions in information systems in the face of a network viewed as compromised" [13]. Zero trust architecture (ZTA) is an "enterprise's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies". Therefore, a "ZT enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of ZTA plan" [13].

NIST also define the terms, user, subject and resource; with the former encompassing end users, and non-human entities that request information from resources (for example, assets, applications, workflows, network accounts, services and devices), with the latter substituting for data [13]. The term "subject is used as standard unless a human end user is involved when the term user is be specifically used" [13]. Zero trust "usually involves minimizing access to resources to only those subjects and assets identified as needing access as well as continually authenticating and authorizing their identity and security posture of each access request" [13]. ZT and ZTA are "about resource access (e.g., printers, computer resources, Internet of Things [IOT] actuators) not just about data access" [13]. Access can be granted through authentication and authorization, on the basis that a subject is authentic and that the request is valid [13]. This is achieved through policy decision/ enforcement point (PDP/PEP) judgements [13]. Trust algorithms may be applied to evaluate, enforce and to calculate levels of confidence in subjects based on contextual elements set as policy by the enterprise (time, geolocation, device health, behavior) [13].

In practice, operationalizing ZT/ZTA depends on ensuring that sensitive information is not discoverable. Yet many systems depend on sharing identity or passwords, so an eavesdropper could determine an identity or a password. Prominent approaches that overcome these limitations (when we do not trust anyone), include zero knowledge proofs [14] and garbled circuits [15], briefly discussed next.

The zero knowledge protocol allows two parties (a prover and a verifier) who each hold a secret and want to jointly compute some function, to prove that they know the secret, without releasing information other than the truth that they know [14]. This protocol prevents the unintended disclosure of information during the sharing, and potential problems of compromise where information and privacy may leak [14].

Zero knowledge proof approaches are founded on the principles of correctness, soundness and zero knowledge [14]. Correctness, so that a verifier will always accept the proof (if it is true), soundness, any fraudulent prover will always be rejected, and, zero knowledge, nothing further than that the statement is true, can be learned during any exchange [14]. An additional approach involves the addition of a trusted "witness" (an oracle, or angel or Merlin) whose presence helps to encourage a verifier to accept a proof [15].

A second way to solve the problem of two party secure computation is through garbled circuits [15]; two parties want to enter into an exchange but keep their inputs secret [17]. This process involves holding secret inputs which are inputed into a mathematical computation, for example, the factorization of prime numbers, or the Hamiltonian circuit of a publicized large graph; which allow each party to generate a random integer [17]. The input is hidden from each party but an answer can be computed as desired [17]. This procedure is founded on the properties of validity, privacy and fairness/correctness [17]. While it would be of interest to compare these approaches in more depth [16],[17], further discussion is not possible due to limitations of space.

Recent empirical studies have explored the practical implementation of ZT/ZTA in a range of settings. Dynamic optimization of authentication gateway trust levels was found to offer improved detection and blocking of DDoS attacks in a cloud data center network [18]. In a study of the dynamic evaluation of continuous authorization in consumer IoT, a smart home involving continuous multi-sensor authentication [19] identified collective situational awareness, which enhanced the zero trust architecture. The authors also called for studies to examine other scenarios and domains including smart vehicles. An investigation into the security of student records' systems, in the absence of a trusted central authority [20], recommended the application of a consensus algorithm to decide whether or not to deploy actions, to allow the system to be governed.

Summing up, zero trust and zero trust architecture offer promising and defined decision-making approaches, "based on the recognition that all subjects (users, applications and or services or devices) and resource access, must be authorized and approved" [13]. Advances in tools, including zero knowledge proofs and garbled circuits, offer tried-and-tested solutions for implementation [14]-[17]. Calls for the adoption of ZT and ZTA are now supported by governments [7],[13] and industry [21]-[23]; indeed the Microsoft Azure project suggests ZT and ZTA herald the arrival of an integrated philosophy to security [24].

Considered next is the well-established integrative trust model, which it is proposed here may help further our understanding of the integrated philosophy [24] of ZT/ZTA.

III. Trust Revisited

Trust is well-characterized and defined with the key assumptions and processes [2],[3] set out in Table 1., below. An extensive review [25] argues the importance of also considering the different levels of trust, and in particular who is being trusted in, and at what level.

Key assumptions in trust formation [2],[3] are based on: firstly, the presence of positive expectations of trustworthiness of the trustee [2],[3]; secondly, a willingness to accept vulnerability [2],[3]; thirdly, the suspension of uncertainty [26]. These elements lead to positive expectations of the intentions of the other's behavior [2],[3].

Taken together, these elements leads to a generally held definition that states that trust is based on the "willingness of a party to be vulnerable to the actions of another party, based on the expectation that the other will perform an action important to the trustor, irrespective of the ability to monitor or control other parties" [3].

The processes of trust formation are clarified [3] as based on; firstly, an assessment of the trustee's ability, benevolence and integrity (ABI), as moderated, secondly, by the trustor's propensity to trust. Thirdly, the ITM views a trustor's state as based on a willingness to be vulnerable and, fourthly, to take a risk in the process trusting [2],[3]. Also considered, is who is trusted to do what, and at what level; at the level of the individual, or the team or the organization [25] is trusted to do what, and at what level; at the level of the individual, or the team or the organization [25]. The assumptions and process steps in the ITM are next revisited in the context of ZT/ZTA to allow conceptual clarity of zero trust theory.

TABLE 1. COMPARISON OF THE KEY ASSUMPTIONS AND ELEMENTS DRAWN FROM THE INTEGRATIVE TRUST MODEL (ITM) [3] WITH THOSE HELD IN (ZT/ZTA) [7],[13].

Element	**Comparison of key assumptions**	
	Trust: Integrative trust model (ITM) [3]	***Zero trust and zero trust architectures (ZT/ZTA) [7],[13]***
Start-point (assumption)	Positive expectations of trust [2]	Expectations of threats, or malicious actors (inside or out)
Assessment	Ability, benevolelnce, integrity	Threat traffic: authentication and authorization
Propensity [27]	Multidimensional	No presumptive trust
Vulnerability	Willingness to be vulnerable [2]	Not willing to accept vulnerability
Uncertainty [26]	Suspension of uncertainty	Uncertainty is a given- aim to minimize [13]
Risk	Risk taking	Not willing to take/ aim to reduce risk
Outcomes	Trust	Authentication and authorization: trust
Control	Absence of control	Constant control
Monitoring	Absence of monitoring	Constant monitoring
Feedback loop	End point	Continuous multielement feedback
Level [25]	Individual, team, organization	Subject: user (human), non-human (service, device, application)

the team or the organization [25]. The assumptions and process steps in the ITM are next revisited in the context of ZT/ZTA to allow conceptual clarity of zero trust theory.

IV. ITM AND ZERO TRUST

As illustrated, in Table 1., the assumptions and steps in the ITM, from assessment to trust outcomes [3], are presented alongside elements from prominent thinking on processes in ZT/ZTA for comparison.

The ITM starts from a state based on positive expectations of trust and the ABI trust assessment as moderated by the trustor's propensity to trust [3]. Propensity is characterized as multidimensional and operating across several scales [27]. Reconsidering the ITM in ZT/ZTA, the proposition of holding positive expectations does not hold true. Zero trust starts from the reverse, a viewpoint based on no presumptive trust [7],[13]. One set of trust scholars suggests zero trust is simply a starting point in an inevitable progress to trust [27], rather than a stable state [2],[3]. This process view is reflected in ZT/ZTA; as confidence is gained, trust is gained [7]. The second assumption of the ITM involves an assessment of the trustor by the trustee, as moderated by their propensity to trust [27]. The perceived elements under consideration in the ITM are based on ability, benevolence and integrity (ABI) [3]. In ZT/ZTA, perception and propensity are based on assumptions of threat traffic and potential malevolent acts [7],[13]. Though, if the assessment of identity is verified, as confidence is gained, trust is gained [7],[13]. Next, the ITM conceives the trustor's state as involving a willingness to be vulnerable. In ZT/ZTA, there is no willingness to be vulnerable. This is followed by the ITM view of trusting as involving taking a risk [3], based on a suspension of uncertainty [26]. In ZT/ZTA, uncertainty is a given, the aim is to minimize; the aim is to reduce risk. Finally, in the ITM, trust formation occurs regardless of any control and/ or monitoring [3]. Conversely, control and monitoring are integral to the decision-making processes involved in ZT/ZTA. In considering trust referents, the ITM is concerned with trust at the level of individuals, or teams or organizations (seen as collections of individuals), in other words, in humans [13]. In ZT/ZTA, authentication and authorization extend beyond humans (users), to include nonhuman subjects, such as devices, services and/ or applications [7],[13].

To sum up, although the starting assumptions of trust in the ITM and ZT/ZTA may appear as binary opposites [24], both approaches result in trust formation through performing an initial assessment [3], or in the case of ZT/ZTA, authentication and authorization [7],[13]. Indeed, both involve considerations of vulnerability and risk; ITM is based on acceptance, while in ZT/ZTA, concerns are with avoidance and reduction. In the end, a positive assessment/ authentication and authorization results in trust. The ITM approach may provide the basis for a scheme to support policy and decision-making to evaluate and integrate the separate elements and steps in implementing ZT/ZTA.

V. CONCLUSION AND IMPLICATIONS

The contribution, call for further research, implications and limitations are discussed next.

The contribution of this paper expands the scope of the ITM [3] and incorporates the operational dynamics of contexts of ZT/ZTA [7]-[13]. This is achieved through leveraging key thinking in ITM and ZT/ZTA. From the ITM evaluation of ABI, vulnerability [2],[3] propensity [25] and temporality [26]; and from ZT/ZTA practical steps [7]-[13] supported through zero knowledge and garbled circuits [14][18]. Together this further clarification may aid practical implementation of ZT/ZTA policy decision-making and policy enforcement [7]-[13].

Yet, as stated, an unanswered puzzle remains; although ZT/ZTA are encouraged by governments, industry and academics, who call for their adoption, many organizations are still tied to presumptive based trust networks.

This work on ZT/ZTA is presented as a short paper and as such is limited in its scope and exploration. Work in progress will address these limitations and deepen understanding through further conceptual development and by inviting other researchers' interest. Future studies may examine organizational and practitioners' decision-making as they accept/ or not, calls to implement ZT/ZTA.

Finally, with the increasing levels of safety and security threats faced by organizations, society and individuals, and the critical national infrastructure that we all depend on [1]; this evaluation advances thinking on ZT/ZTA. By providing a first conceptual model and an agenda for ZT/ZTA research, this paper helps to raise awareness and encouragement among policy-makers, practitioners and academics.

ACKNOWLEDGMENT

The author thanks Leanne Salisbury, Senior Manager at EY, for helpful discussions, and colleagues in Marketing and Strategy at Cardiff University Business School, for supportive comments as the first draft was presented (05/Feb/21). Thank you also to the C-MRIC 21 anonymous reviewers for insightful suggestions for improvements and, in particular, Reviewer 3, for clarification on the definition of ZT, which has helped develop this manuscript. Any mistakes remain the sole responsibility of the author.

REFERENCES

[1] T. Burt, "New nation-state cyberattacks," Microsoft, Redmond, WA, US, 02/Mar/2021. [online]. Available: https://blogs.microsoft.com/on-the-issues/2021/03/02/new-nationstate-cyberattacks/

[2] D. M. Rousseau, S. B. Sitkin, D. S. Burt and C. Camerer, "Not so different after all: A cross discipline view of trust," Academy of Management Journal, 23(3), pp.393-404, 1998.

[3] R. Mayer, J. Davis and F. Schoorman, "An integrative model of organizational trust". Academy of Management Review, 20(3), pp. 709-734, 1995.

[4] Reagan Library, "Remarks on signing the intermediate range nuclear forces treaty," 08/Dec/1987. [online]. Available: https://www.reaganlibrary.gov/archives/speech/remarks-signingintermediate-range-nuclear-forces-treaty

[5] IEEE Standards Association, "A call to action for businesses using AI," Jan/2021. [online]. Available: https://standards.ieee.org/content/dam/ieeestandards/standards/web/documents/other/ead/ead-for-business.pdf

[6] J. Kindervag, "No more chewy centres: The zero trust model of information security," Forrester Research, 23/Mar/2016. [online]. Available: http://crystaltechnologies.com/wp-content/uploads/2017/12/forrester-zero-trust-model-informationsecurity.pdf

[7] S. H, "Zero trust architecture design principles," National Cyber Security Centre (NCSC), 20/Nov/20219. [online]. Available: https://www.ncsc.gov.uk/blog-post/zero-trust-architecture-designprinciples

[8] UKNCSC, "Zero trust architecture design principles," 01/Dec/2020. [online]. Available: https://github.com/ukncsc/zero-trustarchitecture/blob/master/README.md

[9] J. Kindervag, "No more chewy centres: The zero trust model of information security," Forrester Research, 23/Mar/2016. [online]. Available: http://crystaltechnologies.com/wp-content/uploads/2017/12/forrester-zero-trust-model-informationsecurity.pdf

[10] J. Voas, R. Khun, P. Laplante and S. Applebaum, "Internet of things, trust concerns," White paper (draft). Computer Security Resource Centre (CSRC), National Institute for Standards and Technology (NIST). 17/Oct/2018. [online]. Available: https://csrc.nist.gov/publications/detail/white-paper/2018/10/17/iottrust-concerns/draft

[11] C. Onwubiko, "CyberOps: Situational Awareness in Cybersecurity Operations." International Journal on Cyber Situational Awareness, 5(1), pp.82-107, 2020.

[12] GitHub, "A curated collection of awesome resources for zero trust." 19/Oct/2020. [online]. Available: https://github.com/pomerium/awesome-zero-trustGitHub - pomerium/awesome-zero-trust

[13] S. Rose, O. Borchert, A. Mitchell and S. Connelly, "Zero trust architecture, NIST special publication 888-207," NIST, Aug/2020. [online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800207.pdf

[14] S. Goldwasser, S. Micali and C. Rackoff, "The knowledge complexity of interactive proof systems", Siam Journal of Computing, 18(1), pp.186-208, 1989.

[15] A. C-C. Yao, "How to generate and exchange secrets," 1986 IEEE 27th Annual Symposium on Foundations of Computer Science (SFCS 1986), 1986, pp.162-167.

[16] J. Kuriakose, P.S. Sisodia, Armuth, V, D. K. Shah and S. More, "Comparative study of diverse zero-knowledge argument systems," 2016 International Conference on Data Mining and Advance Computing (SAPIENCE), 2016, pp.284-293, doi:10/1109/SPAIENCE. 2016.7684134.

[17] M. Jawurek, F. Kerschbaum and C. Orlandi, "Zero knowledge using garbled circuits or how to prove non algebraic statements efficiently," CCS 13, Proceedings of the 2013 Conference on Computer and Communications Security, (ACM SIGSAC), 2013, pp.955-966, doi:10.1145/2508859.2516662.

[18] D. Eidle, S. Y. Ni, C. DeCaustis and A. Sager, "Autonomic security for zero trust networks," 2017 IEEE 8th Annual Ubiquitous Computing Electronics and Mobile Communication Conference (UEMCON), 2017, pp.288-293, doi: 10.1109/UECON.2017.8249053.

[19] T. Dimitrakos et al., "Trust aware continuous authorization for zero trust in consumer internet of things," IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2020, pp.1081-1812, doi:10.1109/TrustCom50675.2020.000247.

[20] A. P. Patil, G. Karkal, J. Wadhwa, M. Sawood and K. Dhanush Reddy, "Design and implememtation of a consensus algorithm to build zero trust model," 2020, IEEE 17th India council International Conference (INDICON), 2020, pp.1-5, doi:10.1109/INDICON49873.2020.9342207.

[21] L. Orans, N. MacDonald and S. Riley, "Market guide for zero trust network access". 08/Jun/2020. [online]. Available : https://www.gartner.com/doc/reprints?id=1-245YJ33O&ct=200916&st=sb

[22] Crowdstrike, "What is zero trust security?" 30/Apr/2020. [online]. Available: https://www.crowdstrike.com/cybersecurity-101/zerotrust-security/

[23] L. Sailsbury and A. Wylde, "Grey areas, what if asking your cyber security team "are we good" is just not good enough?" LinkedIn, 2020. [online]. Available: https://www.linkedin.com/pulse/greyareas-what-asking-your-cyber-security-team-we-good-salisbury?/

[24] Microsoft, "Security: a guide to building resilience," Solution guide series, Microsoft. Jul//2020. [online]. Available: https://clouddamcdnprodep.azureedge.net/gdc/gdcPJ9yCm/original

[25] A. Fulmer and M. Gelfand, "At what level (and in whom) we trust: Trust across multiple organizational levels," Journal of Management, 38(4), pp.1167-1230, 2012.

[26] G. Möllering, "Trust: Reason, Routine, Reflexivity," Bingley, UK: Emerald Group, 2006.

[27] V. Patent and R. Searle, "Qualitative meta-analysis of propensity to trust measurement," Journal of Trust Research, 9(2), pp.136-163, 2019.

[28] R. J. Lewicki, E. C. Tomlinson and N. Gillespie, "Models of interpersonal trust development: Theoretical approaches, empirical evidence and future directions," Journal of Management, 32(6), pp. 991-1002, 2006.

[29] R. J. Lewicki, D. McAllister and R. Bies, "Trust and distrust: New relationships and realities," Academy of Management Review, 23(3), pp. 438-458, 1998.