The Zero-trust Paradigm: Concepts, Architectures and Applications

Other titles in Foundations and Trends® in Privacy and Security

Security Analysis and Formal Verification on Blockchain and its Applications
Kang Li, Ronghui Gu, Jun Xu, Zhaofeng Chen, Siwei Wu, Yajin Zhou, Mu Zhang, Xiapu Luo, Yuzhe Tang, Yi Li, Xiaokuan Zhang and Yibo Wang
ISBN: 978-1-63828-568-7

Recommender Systems Meet Large Language Model Agents: A Survey
Xi Zhu, Yu Wang, Hang Gao, Wujiang Xu, Chen Wang, Zhiwei Liu, Kun Wang, Mingyu Jin, Linsey Pang, Qingsong Weng, Philip S. Yu and Yongfeng Zhang
ISBN: 978-1-63828-564-9

Trustworthy Machine Learning: From Data to Models
Bo Han, Jiangchao Yao, Tongliang Liu, Bo Li, Sanmi Koyejo and Feng Liu
ISBN: 978-1-63828-548-9

Advances in Secure IoT Data Sharing
Phu Nguyen, Arda Goknil, Gencer Erdogan, Shukun Tokas, Nicolas Ferry and Thanh Thao Thi Tran
ISBN: 978-1-63828-422-2

Navigating the Soundscape of Deception: A Comprehensive Survey on Audio Deepfake Generation, Detection, and Future Horizons
Taiba Majid Wani, Syed Asif Ahmad Qadri, Farooq Ahmad Wani and Irene Amerini
ISBN: 978-1-63828-492-5

The Zero-trust Paradigm: Concepts, Architectures and Applications

Charalampos Katsis
Purdue University
ckatsis@purdue.edu

Elisa Bertino
Purdue University
bertino@purdue.edu

the essence of knowledge
Boston — Delft

Foundations and Trends® in Privacy and Security

Published, sold and distributed by:
now Publishers Inc.
PO Box 1024
Hanover, MA 02339
United States
Tel. +1-781-985-4510
www.nowpublishers.com
sales@nowpublishers.com

Outside North America:
now Publishers Inc.
PO Box 179
2600 AD Delft
The Netherlands
Tel. +31-6-51115274

The preferred citation for this publication is

C. Katsis and E. Bertino. *The Zero-trust Paradigm: Concepts, Architectures and Applications*. Foundations and Trends® in Privacy and Security, vol. 8, no. 2, pp. 122–253, 2025.

ISBN: 978-1-63828-573-1

Foundations and Trends® in Privacy and Security
Volume 8, Issue 2, 2025

Editorial Scope

Foundations and Trends® in Privacy and Security publishes survey and tutorial articles in the following topics:

- Access control
- Accountability
- Anonymity
- Application security
- Artifical intelligence methods in security and privacy
- Authentication
- Big data analytics and privacy
- Cloud security
- Cyber-physical systems security and privacy
- Distributed systems security and privacy
- Embedded systems security and privacy
- Forensics
- Hardware security
- Human factors in security and privacy
- Information flow
- Intrusion detection
- Malware
- Metrics
- Mobile security and privacy
- Language-based security and privacy
- Network security
- Privacy-preserving systems
- Protocol security
- Security and privacy policies
- Security architectures
- System security
- Web security and privacy

Information for Librarians

Foundations and Trends® in Privacy and Security, 2025, Volume 8, 4 issues. ISSN paper version 2474-1558. ISSN online version 2474-1566. Also available as a combined paper and online subscription.

Contents

1 Introduction **2**
1.1 Existing Efforts and Application Domains 4
1.2 Challenges in the Application of ZTA 6
1.3 Scope of the Monograph 7
1.4 Organization of the Monograph 7

2 Security Controls and Guidelines **9**
2.1 Security Controls 9
2.2 Guidelines 18

3 Architectures **29**
3.1 A Taxonomy of ZT Architectures 29
3.2 ZT for Conventional Networks 37
3.3 ZT for Software-defined Networks (SDN) 44
3.4 ZT for SDN Networks with Programmable Data Planes . . 58
3.5 ZT for Industrial IoT Networks 68
3.6 Architecture Summary and Concluding Remarks 81

4 The NEUTRON Framework **87**
4.1 Modularizing the Security Policy Using Fine-grained Graphs 87
4.2 Sanity Checks 90
4.3 Pattern Analysis 90

4.4 Translation 91
4.5 Security Policy Regression Testing 93

5 Industry Efforts 98
5.1 Microsoft's Zero-trust Approach 98
5.2 Palo Alto Networks' ZT Approach 101
5.3 Google's BeyondCorp 105
5.4 Aviatrix's Distributed Cloud Firewall 108
5.5 OpenZiti by NetFoundry 110

6 Concluding Remarks and Research Directions 113

Acknowledgements 122

References 123

The Zero-trust Paradigm: Concepts, Architectures and Applications

Charalampos Katsis[1] and Elisa Bertino[2]

[1]*Purdue University, USA; ckatsis@purdue.edu*
[2]*Purdue University, USA; bertino@purdue.edu*

ABSTRACT

The notion of Zero Trust Architecture (ZTA) has been introduced as a fine-grained defense approach. It assumes that no entities outside and inside the protected system can be trusted and, therefore, requires articulated and high-coverage deployment of security controls. However, ZTA is a complex notion that does not have a single design solution; rather, it consists of numerous interconnected concepts and processes that need to be assessed prior to deciding on a solution. In this monograph, we cover the principles and architectural foundations of ZTA, basically following the guidelines by NIST, and provide a detailed analysis of ZT architectures proposed by research and industry. The monograph also describes an approach for the automatic generation of ZT policies based on application communication requirements, network topology, and organizational information. This approach was designed to meet a critical need of ZTA, that is, the generation and implementation of a large number of fine-grained policies. Finally, the monograph discusses several research directions, including the incorporation of threat intelligence into ZT networks and the use of large language models (LLMs).

Charalampos Katsis and Elisa Bertino (2025), “The Zero-trust Paradigm: Concepts, Architectures and Applications”, Foundations and Trends® in Privacy and Security: Vol. 8, No. 2, pp 122–253. DOI: 10.1561/3300000046.

1

Introduction

Existing measures aimed at securing network perimeters have demonstrated insufficiency in preventing breaches within an organization's infrastructure (Mirsky *et al.*, 2018; Navarro *et al.*, 2018; Bertino *et al.*, 2023). This inadequacy stems from the escalating resource capabilities of adversaries and the increasing sophistication of multi-step attack strategies, rendering breaches feasible. In addition, additional challenges have arisen due to the absence of a tangible physical network perimeter in many scenarios. For example, the widespread adoption of remote work settings and the utilization of cloud services have resulted in the dispersion of organizational resources beyond traditional network boundaries. Furthermore, the contemporary landscape of network architecture has witnessed a significant expansion in its attack surface, attributable to the intricate interconnectivity of diverse networks, encompassing IoT devices, autonomous vehicles, and operational technology, among others. Due to those reasons, it is no longer tenable to presume the internal network's safety solely based on perimeter defenses. Consequently, there is an imperative need to adopt more realistic network threat models that acknowledge the possibility that adversaries have already breached conventional defenses and infiltrated the network's core.

Zero-trust architecture (ZTA), also known as perimeter-less security, is a recent paradigm that challenges the conventional notion of network security by considering both internal and external networks as potentially compromised and that threats exist at all times in the network. Unlike traditional defense approaches, which often rely on perimeter defenses, ZTA advocates the deployment of defense mechanisms within the internal network and at its periphery. Such an approach entails a fundamental shift in trust dynamics, where all entities, devices, users, applications, and network flows within the internal network are no longer inherently trusted and thus cannot arbitrarily communicate with other entities. Consequently, strict access control policies are imperative to regulate communication flows. These policies are designed to permit only the essential communication flows necessary for the successful completion of each entity's mission or objectives. By strictly limiting authorized communications to those aligned with the endpoint's mission, ZTA aims to minimize the potential attack surface by reducing the attacker's abilities to move within the network.

In some way, the notion of ZTA can be considered as an application of the well-known security principles by Saltzer and Schroeder (1975), including closed system, least privilege, complete mediation, defense-in-depth, and layered defenses, to which two principles are added:

- no entity in the system can be trusted without proper comprehensive checks;
- access control should be resource-centric and context-aware.

A consequence is that ZTA frameworks should provide functions for (i) authenticating and authorizing, according to the least privilege policy, all entities trying to access the protected resources based on context and a trust assessment of these entities and (ii) continuously monitoring the security of the protected resources.

So, even though ZTA may not be considered novel in all its aspects, the current emphasis on ZTA is important, as it pushes systematic approaches to security. Recent and past attacks clearly show that the security of networks and systems requires systematic, pervasive, fine-grained, and continuous deployment of layered security controls based on those principles.

1.1 Existing Efforts and Application Domains

Because of its relevance, ZTA guidelines and industry-designed frameworks have been developed, and researchers have developed approaches that focus on the application of ZTA to different types of networks and systems.

1.1.1 Guidelines

The US National Institute of Standards and Technology (NIST) has introduced initial guidelines for the adoption of ZTA aimed at federal agencies and the private sector (Stafford, 2020). These guidelines propose an architectural framework where communications are managed through one or more policy enforcement points (PEP). The PEP serves as an intermediary, directing communication requests to a centralized software-defined controller, which then evaluates requests based on factors such as access control models and external threat intelligence to make decisions.

The US Department of Defense (DoD, 2022) has released a long-term strategy for adopting ZTA in their military networks. The DoD presents a strong use case as they manage large-scale networks with different architectures and requirements, such as air, ground, space, and sea networks. A key requirement, according to the released document, is that data and communications must be protected and secured and only accessed by the entities who need it, when they need it, using the least privilege policy.

It is crucial to understand that these documents offer guidelines rather than concrete technical instructions on how to implement ZTA. They outline requirements and overarching visions for future adoption without delving into specific implementation details.

1.1.2 Industrial Approaches

Prominent industry stakeholders are demonstrating considerable interest in the concept of ZTA. BeyondCorp is an architecture developed by Google (Ward and Beyer, 2014), which proposes an approach to enforce access control to enterprise resources from enterprise-controlled (that is, managed) user devices. This model entails directing all requests to an internet-facing access proxy service, necessitating that resources be publicly discoverable through the domain name system (DNS) for access. The service authenticates the user's or device's credentials and the access control model to make a decision. The access proxy service has to be configured for every service/application in the network. Since BeyondCorp operates on the principle of making all applications accessible on the public Internet, some organizations may have concerns about the increased visibility and potential attack surface. Furthermore, BeyondCorp is designed with a cloud-first model in mind. Organizations that still rely heavily on on-premises infrastructure may find it challenging to fully adopt BeyondCorp.

Microsoft (2024) has introduced a framework for ZTA implementation, which encompasses the various components necessary for an integrated solution. These components span from identity management and endpoint protection to network-based policy enforcement. Palo Alto Networks (2022) offers a suite of tools and technologies, such as an identity-based access control engine that allows the definition of security policies and monitoring of various network services.

1.1.3 Application Domains

Most ZTA approaches have been proposed for network systems characterized by open, flexible architectures in which (i) data can be continuously collected; (ii) collected data can be analyzed using data analytic techniques, such as those based on machine learning (ML) (Katsis and Bertino, 2025; Polese *et al.*, 2023; Abu Jabal *et al.*, 2020); (iii) results from these analyses can be used to assess the "trust" of the entities in the system (Bradatsch *et al.*, 2023b); and (i) policies for authentication and authorization can be dynamically generated, modified, and deployed in the system.

Software-defined networks (SDN) represent an interesting environment in which ZTA can be deployed. By properly extending the control plane and the data plane, one would be able to support fine-grained and dynamic access control to network segments, possibly based on communication requirements per application, thus enforcing the least privilege principle (Katsis and Bertino, 2025).

In addition, it has been advocated that ZTA should be extended to secure autonomous systems. Good use case examples are drones, IoT-based manufacturing equipment, operational systems, and even smart cities (Hassija *et al.*, 2019).

1.2 Challenges in the Application of ZTA

The adoption of ZTA necessitates the generation and deployment of fine-grained security policies. Given ZTA's emphasis on strict access control, organizations must define and implement a vast number of policies, a process fraught with several challenges.

First, the communication requirements of various network components—including IoT devices, services, virtual machines, and users—are often unclear. As a result, administrators may resort to overly permissive access control policies to prevent disruptions in communication, inadvertently weakening security.

Second, existing policy frameworks lack mechanisms to precisely define and enforce granular network access controls. This shortcoming forces organizations to manually specify network perimeter policies, a labor-intensive process that is error-prone and time-consuming (Cuppens *et al.*, 2019; Casado *et al.*, 2007; Mai *et al.*, 2011; Cuppens *et al.*, 2004; Bodei *et al.*, 2018; Nelson *et al.*, 2010).

Additionally, the absence of comprehensive visibility into normal network behavior complicates the identification of unauthorized activities. This limitation is particularly problematic for detecting subtle anomalies that mimic legitimate traffic but originate from unknown domains. For instance, while flooding attacks exhibit distinctive patterns, other forms of misuse may blend seamlessly with benign flows, making them difficult to discern.

Another major challenge is translating high-level security policies into enforceable rules across diverse enforcement points. Policies that are intuitive to administrators must be converted into configurations for firewalls and network switches, whether deployed on-premises or in distributed cloud environments. This translation process is complex due to variations in vendor-specific configurations, interface differences, and enforcement capabilities. Moreover, policies must account for the dynamic locations of end systems to ensure proper enforcement without unintended disruptions.

1.3 Scope of the Monograph

This monograph sets out to provide a rigorous and comprehensive examination of Zero-Trust principles, with the goal of clarifying what constitutes a ZTA and what technical requirements are essential to its realization. We begin by defining Zero-Trust in precise terms and identifying the critical security controls it entails, including identity management and access control mechanisms tailored to distinct domains such as end systems and networks. The monograph explores how these controls are leveraged by existing guidelines to shape the design and implementation of ZTA.

A core contribution of this work is a systematic analysis of the current state-of-the-art Zero-Trust architectures, drawing from both academic research and industrial practice. We examine how foundational ZTA requirements are translated into concrete architectural frameworks, highlighting the specific problems each approach addresses, the architectural components involved, and the underlying trust assumptions.

In addition to discussing existing efforts, the monograph identifies key gaps and challenges that remain unresolved. We conclude by outlining promising research directions aimed at advancing the development and deployment of robust, scalable, and adaptable Zero-Trust systems.

1.4 Organization of the Monograph

The rest of this monograph is organized as follows. Section 2 introduces basic security controls, including authentication and access control; the pervasive and fine-grained deployment of these controls is the goal of the ZT paradigm. Section 2 also covers ZT guidelines provided by governmental organizations, namely the US NIST and the US DoD. Section 3 is the core section of the monograph; it provides a comprehensive taxonomy of the various architectural approaches that can be used to deploy the functional components of the ZT paradigm. Section 3 also describes in detail the ZT architectures proposed for different types of networks. Section 4 presents an overview of an end-to-end pipeline for the specification, analysis, and deployment of ZT policies. This pipeline addresses the problem of automatically generating ZT policies starting from application communication requirements, network topology and organizational information. Section 5 complements the discussion in Section 3 by providing an overview of industrial ZT architectures. Section 6 outlines concluding remarks and discusses research directions.

References

Abu Jabal, A., E. Bertino, J. Lobo, M. Law, A. Russo, S. Calo, and D. Verma. (2020). "Polisma-a framework for learning attribute-based access control policies". In: *Computer Security–ESORICS 2020: 25th European Symposium on Research in Computer Security, ESORICS 2020, Guildford, UK, September 14–18, 2020, Proceedings, Part I 25*. Springer. 523–544.

Ameer, S., M. Gupta, S. Bhatt, and R. Sandhu. (2022). "Bluesky: Towards convergence of zero trust principles and score-based authorization for iot enabled smart systems". In: *Proceedings of the 27th ACM on symposium on access control models and technologies*. 235–244.

Ameer, S., L. Praharaj, R. Sandhu, S. Bhatt, and M. Gupta. (2024). "ZTA-IoT: A Novel Architecture for Zero-Trust in IoT Systems and an Ensuing Usage Control Model". *ACM Transactions on Privacy and Security*.

Anjum, I., D. Kostecki, E. Leba, J. Sokal, R. Bharambe, W. Enck, C. Nita-Rotaru, and B. Reaves. (2022). "Removing the reliance on perimeters for security using network views". In: *Proceedings of the 27th ACM on Symposium on Access Control Models and Technologies*. 151–162.

Anjum, I., J. Sokal, H. R. Rehman, B. Weintraub, E. Leba, W. Enck, C. Nita-Rotaru, and B. Reaves. (2023). "MSNetViews: Geographically Distributed Management of Enterprise Network Security Policy". In: *Proceedings of the 28th ACM Symposium on Access Control Models and Technologies*. 121–132.

Aviatrix. (2024). "Aviatrix DCF Documentation v7.1". URL: https://docs.aviatrix.com/documentation/v7.1/network-security/index.html.

Aviatrix. (2025a). "Distributed Cloud Firewall". URL: https://aviatrix.com/distributed-cloud-firewall/.

Aviatrix. (2025b). "Secure Cloud Networking Products". URL: https://aviatrix.com/secure-cloud-networking-products/.

Axiomatics. (2025). "Abbreviated Language for Authorization (ALFA)". URL: https://axiomatics.com/resources/reference-library/abbreviated-language-for-authorization-alfa.

Bajaber, O., B. Ji, and P. Gao. (2024). "P4Control: Line-Rate Cross-Host Attack Prevention via In-Network Information Flow Control Enabled by Programmable Switches and eBPF". In: *2024 IEEE Symposium on Security and Privacy (SP)*. IEEE Computer Society. 147–147.

Berde, P., M. Gerola, J. Hart, Y. Higuchi, M. Kobayashi, T. Koide, B. Lantz, B. O'Connor, P. Radoslavov, W. Snow, *et al.* (2014). "ONOS: towards an open, distributed SDN OS". In: *Proceedings of the third workshop on Hot topics in software defined networking*. 1–6.

Bertino, E., H. Lee, M. Huang, C. Katsis, Z. Shen, B. Ribeiro, D. De Mello, and A. Kundu. (2023). "A Pro-Active Defense Framework for IoT Systems". In: *2023 IEEE 9th International Conference on Collaboration and Internet Computing (CIC)*. IEEE. 125–132.

Blockcerts. (2024). "Blockcerts: Open Standard for Verifiable Credentials". URL: https://www.blockcerts.org/.

Bloom. (2020). "BloomID: A Guide to Your Secure Identity". URL: https://bloom.co/blog/bloomid-a-guide-to-your-secure-identity/.

Bodei, C., P. Degano, L. Galletta, R. Focardi, M. Tempesta, and L. Veronese. (2018). "Language-independent synthesis of firewall policies". In: *Proceedings of the 2018 IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE. 92–106.

Bradatsch, L., M. Haeberle, B. Steinert, F. Kargl, and M. Menth. (2022). "Secure service function chaining in the context of zero trust security". In: *2022 IEEE 47th Conference on Local Computer Networks (LCN)*. IEEE. 123–131.

Bradatsch, L., O. Miroshkin, and F. Kargl. (2023a). "ZTSFC: a service function chaining-enabled zero trust architecture". *IEEE Access*. 11: 125307–125327.

Bradatsch, L., O. Miroshkin, N. Trkulja, and F. Kargl. (2023b). "Zero Trust Score-based Network-level Access Control in Enterprise Networks". In: *2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. IEEE. 1422–1429.

California State Assembly. (2018). "California Consumer Privacy Act (CCPA)". URL: https://oag.ca.gov/privacy/ccpa.

Casado, M., M. J. Freedman, J. Pettit, J. Luo, N. McKeown, and S. Shenker. (2007). "Ethane: Taking control of the enterprise". *ACM SIGCOMM computer communication review*. 37(4): 1–12.

CISA. (2014). "Federal Information Security Modernization Act (FISMA)". URL: https://www.cisa.gov/topics/cyber-threats-and-advisories/federal-information-security-modernization-act.

Csikor, L., S. Ramachandran, and A. Lakshminarayanan. (2022). "ZeroDNS: Towards Better Zero Trust Security using DNS". In: *Proceedings of the 38th Annual Computer Security Applications Conference*. 699–713.

Cuppens, F., N. Cuppens-Boulahia, and J. Garcia-Alfaro. (2019). "Misconfiguration management of network security components". *arXiv preprint arXiv:1912.07283*.

Cuppens, F., N. Cuppens-Boulahia, T. Sans, and A. Miège. (2004). "A formal approach to specify and deploy a network security policy". In: *IFIP World Computer Congress, TC 1*. Springer. 203–218.

Datta, R., S. Choi, A. Chowdhary, and Y. Park. (2018). "P4guard: Designing p4 based firewall". In: *MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM)*. IEEE. 1–6.

Dimitrakos, T., T. Dilshener, A. Kravtsov, A. La Marra, F. Martinelli, A. Rizos, A. Rosetti, and A. Saracino. (2020). "Trust aware continuous authorization for zero trust in consumer internet of things". In: *2020 IEEE 19th international conference on trust, security and privacy in computing and communications (TrustCom)*. IEEE. 1801–1812.

DoD. (2022). "DoD Zero Trust Strategy". *DoD Office of Prepublication and Security Review*.

Eberz, S., K. B. Rasmussen, V. Lenders, and I. Martinovic. (2017). "Evaluating behavioral biometrics for continuous authentication: Challenges and metrics". In: *Proceedings of the 2017 ACM on Asia conference on computer and communications security*. 386–399.

Escobedo, V., B. Beyer, M. Saltonstall, and F. Zyzniewski. (2017). "BeyondCorp: The user experience". *login*. 42(3): 38–43.

European Parliament. (2016). "General Data Protection Regulation (GDPR)". URL: https://gdpr.eu/.

Ferraiolo, D., L. Feldman, and G. Witte. (2016). "Exploring the next generation of access control methodologies". URL: https://www.nist.gov/publications/exploring-next-generation-access-control-methodologies.

Ferraiolo, D. F., R. Sandhu, S. Gavrila, D. R. Kuhn, and R. Chandramouli. (2001). "Proposed NIST standard for role-based access control". *ACM Transactions on Information and System Security (TISSEC)*. 4(3): 224–274.

Gao, K., T. Nojima, H. Yu, and Y. R. Yang. (2020). "Trident: Toward distributed reactive SDN programming with consistent updates". *IEEE Journal on Selected Areas in Communications*. 38(7): 1322–1334.

Géant. (2024). *eduroam*. URL: https://eduroam.org/ (accessed on 09/30/2024).

Gonçalves, G., K. O'Malley, M. Saltonstall, *et al.* (2023). "BeyondCorp and the long tail of Zero Trust".

Hassija, V., V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar. (2019). "A survey on IoT security: application areas, security threats, and solution architectures". *IEEe Access*. 7: 82721–82743.

Hu, V. C., D. Ferraiolo, R. Kuhn, A. R. Friedman, A. J. Lang, M. M. Cogdell, A. Schnitzer, K. Sandlin, R. Miller, K. Scarfone, *et al.* (2013). "Guide to attribute based access control (abac) definition and considerations (draft)". *NIST special publication*. 800(162): 1–54.

Hughes, J. and E. Maler. (2005). "Security assertion markup language (saml) v2. 0 technical overview". *OASIS SSTC Working Draft sstc-saml-tech-overview-2.0-draft-08*. 13: 12.

Jabal, A. A., M. Davari, E. Bertino, C. Makaya, S. Calo, D. Verma, A. Russo, and C. Williams. (2019). "Methods and tools for policy analysis". *ACM Computing Surveys (CSUR)*. 51(6): 1–35.

Janosko, M., H. King, M. Saltonstall, *et al.* (2018). "Beyondcorp 6: Building a healthy fleet". *login*. 43(3): 24–30.

Jones, M. B., J. Bradley, and N. Sakimura. (2015). "JSON Web Token (JWT)".

Kang, Q., L. Xue, A. Morrison, Y. Tang, A. Chen, and X. Luo. (2020). "Programmable {In-Network} security for context-aware {BYOD} policies". In: *29th USENIX Security Symposium (USENIX Security 20)*. 595–612.

Katsis, C. and E. Bertino. (2025). "ZT-SDN: An ML-powered Zero-Trust Architecture for Software-Defined Networks". *ACM Transactions on Privacy and Security*. 28(2): 1–35.

Katsis, C., F. Cicala, D. Thomsen, N. Ringo, and E. Bertino. (2021). "Can i reach you? do i need to? new semantics in security policy specification and testing". In: *Proceedings of the 26th ACM Symposium on Access Control Models and Technologies*. 165–174.

Katsis, C., F. Cicala, D. Thomsen, N. Ringo, and E. Bertino. (2022). "NEUTRON: a graph-based pipeline for zero-trust network architectures". In: *Proceedings of the Twelfth ACM Conference on Data and Application Security and Privacy*. 167–178.

Katz, J. and Y. Lindell. (2008). *Introduction to Modern Cryptography*. CRC Press. 70.

Kelsey, J., B. Schneier, and N. Ferguson. (1999). "Yarrow-160: Notes on the design and analysis of the yarrow cryptographic pseudorandom number generator". In: *International Workshop on Selected Areas in Cryptography*. Springer. 13–33.

Krisler, B., P. Pal, Z. Bertilson, and D. Thomsen. (2019). "Secure Desktop Computing in the Cloud". In: *2019 6th IEEE International Conference on Cyber Security and Cloud Computing (CSCloud)/2019 5th IEEE International Conference on Edge Computing and Scalable Cloud (EdgeCom)*. IEEE. 107–112.

Lawal, S., X. Zhao, A. Rios, R. Krishnan, and D. Ferraiolo. (2024). "Translating Natural Language Specifications into Access Control Policies by Leveraging Large Language Models". In: *2024 IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA)*. IEEE. 361–370.

Lee, K., S. Sjöberg, and A. Narayanan. (2022). "Password policies of most top websites fail to follow best practices". In: *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. 561–580.

Lockheed Martin Corporation. (2025). "Cyber Kill Chain". URL: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

Mai, H., A. Khurshid, R. Agarwal, M. Caesar, P. B. Godfrey, and S. T. King. (2011). "Debugging the data plane with anteater". *ACM SIGCOMM Computer Communication Review*. 41(4): 290–301.

Merkle, R. (1979). "Merkle tree patent".

Microsoft. (2024). *Embrace proactive security with Zero Trust*. URL: https://www.microsoft.com/en-us/security/business/zero-trust (accessed on 04/09/2024).

Microsoft Corporation. (2021). "Evolving Zero Trust: How Real-World Deployments and Attacks Are Shaping the Future of Zero Trust Strategies". *Tech. rep.* URL: https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Evolving-Zero-Trust-Microsoft-Position-Paper.pdf.

Microsoft Corporation. (2024). "Decentralized Identifier Overview - Microsoft Entra Verified ID". URL: https://learn.microsoft.com/en-us/entra/verified-id/decentralized-identifier-overview.

Microsoft Corporation. (2025). "Zero Trust Strategy and Architecture". URL: https://www.microsoft.com/en-us/security/business/zero-trust.

Mirsky, Y., T. Doitshman, Y. Elovici, and A. Shabtai. (2018). "Kitsune: an ensemble of autoencoders for online network intrusion detection". *arXiv preprint arXiv:1802.09089*.

MITRE Corporation. (2025a). "Common Vulnerabilities and Exposures (CVE)". URL: https://cve.mitre.org/.

MITRE Corporation. (2025b). "MITRE ATT&CK Enterprise Matrix". URL: https://attack.mitre.org/matrices/enterprise/.

Monsanto, C., J. Reich, N. Foster, J. Rexford, and D. Walker. (2013). "Composing software defined networks". In: *10th USENIX Symposium on Networked Systems Design and Implementation (NSDI 13)*. 1–13.

Naik, N. and P. Jenkins. (2021). "Sovrin network for decentralized digital identity: Analysing a self-sovereign identity system based on distributed ledger technology". In: *2021 IEEE International Symposium on Systems Engineering (ISSE)*. IEEE. 1–7.

National Institute of Standards and Technology (NIST). (2025). "National Vulnerability Database (NVD)". URL: https://nvd.nist.gov/vuln.

Navarro, J., A. Deruyver, and P. Parrend. (2018). "A systematic survey on multi-step attack detection". *Computers & Security*. 76: 214–249.

Nayak, A. K., A. Reimers, N. Feamster, and R. Clark. (2009). "Resonance: Dynamic access control for enterprise networks". In: *Proceedings of the 1st ACM workshop on Research on enterprise networking*. 11–18.

Nelson, T., C. Barratt, D. J. Dougherty, K. Fisler, and S. Krishnamurthi. (2010). "The margrave tool for firewall analysis". In: *Proceedings of the 24th Large Installation System Administration Conference (LISA 10)*.

Nginx, I. (2024). *NJS Scripting Language*. URL: https://nginx.org/en/docs/njs/.

OASIS. (2013). "eXtensible Access Control Markup Language (XACML) Version 3.0 Core Specification". URL: https://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html.

ONF. (2024). "ONOS: Open Network Operating System". URL: https://onosproject.org/.

Open Information Security Foundation. (2025). "Suricata - Open Source Threat Detection Engine". URL: https://suricata.io/.

Open Networking Foundation. (2015). "OpenFlow Switch Specification (version 1.5.1)". *Tech. rep.*

OpenBSD. *PF Manual Page*. URL: https://man.openbsd.org/pf (accessed on 06/20/2021).

OpenID Foundation. (2014). "OpenID Connect Core 1.0". URL: https://openid.net/specs/openid-connect-core-1_0.html.

OpenZiti. (2025a). "Introduction to OpenZiti". URL: https://openziti.io/docs/learn/introduction/.

OpenZiti. (2025b). "OpenZiti Components". URL: https://openziti.io/docs/learn/introduction/components.

Osborn, B., J. McWilliams, B. Beyer, and M. Saltonstall. (2016). "Design to deployment at Google". *Usenix Login*. 41(1): 28–35.

Palo Alto Networks. (2022). *Zero Trust Enterprise: Design Guide*. URL: https://www.paloaltonetworks.com/resources/guides/zero-trust-overview.

Peck, J., B. Beyer, C. Beske, and M. Saltonstall. (2017). "Migrating to BeyondCorp: maintaining productivity while improving security". *login*. 42(2): 1–7.

Pöhn, D. and W. Hommel. (2020). "An overview of limitations and approaches in identity management". In: *Proceedings of the 15th International Conference on Availability, Reliability and Security*. 1–10.

Polese, M., L. Bonati, S. D'oro, S. Basagni, and T. Melodia. (2023). "Understanding O-RAN: Architecture, interfaces, algorithms, security, and research challenges". *IEEE Communications Surveys & Tutorials*. 25(2): 1376–1411.

Rabitti, F., E. Bertino, W. Kim, and D. Woelk. (1991). "A model of authorization for next-generation database systems". *ACM Transactions on Database Systems (TODS)*. 16(1): 88–131.

Rais, R., C. Morillo, E. Gilman, and D. Barth. (2024). *Zero Trust Networks: Building Secure Systems in Untrusted Networks*. " O'Reilly Media, Inc."

Saltzer, J. H. and M. D. Schroeder. (1975). "The protection of information in computer systems". *Proceedings of the IEEE*. 63(9): 1278–1308.

Salvador, S. and P. K. Chan. (2004). "FastDTW: Toward Accurate Dynamic Time Warping in Linear Time and Space". In: URL: https://api.semanticscholar.org/CorpusID:6226669.

Sandhu, R. S. (1998). "Role-based access control". In: *Advances in computers*. Vol. 46. Elsevier. 237–286.

Shah, A. and J. Roberts. (2019). "Policy Machine Core". URL: https://github.com/usnistgov/policy-machine-core.

Singh, J., H. Ram, and D. J. Sodhi. (2013). "Improving efficiency of apriori algorithm using transaction reduction". *International Journal of Scientific and Research Publications*. 3(1): 1–4.

Singla, A. and E. Bertino. (2018). "Blockchain-based PKI solutions for IoT". In: *2018 IEEE 4th international conference on collaboration and internet computing (CIC)*. IEEE. 9–15.

Spear, B., B. Beyer, L. Cittadini, and M. Saltonstall. (2016). "Beyond corp: the access proxy". *Login*. 41(04): 28–33.

Stafford, V. (2020). "Zero trust architecture". *NIST special publication*. 800: 207.

Thomsen, D. and E. Bertino. (2018). "Network policy enforcement using transactions: The neutron approach". In: *Proceedings of the 23nd ACM on Symposium on Access Control Models and Technologies*. 129–136.

Torres, J., M. Nogueira, and G. Pujolle. (2012). "A survey on identity management for the future network". *IEEE Communications Surveys & Tutorials*. 15(2): 787–802.

Trinsic. (2025). "Trinsic: Decentralized Identity Ecosystem". URL: https://trinsic.id/.

Ward, R. and B. Beyer. (2014). "Beyondcorp: A new approach to enterprise security". *; login:: the magazine of USENIX & SAGE*. 39(6): 6–11.

Won, J., A. Singla, E. Bertino, and G. Bollella. (2018). "Decentralized public key infrastructure for internet-of-things". In: *MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM)*. IEEE. 907–913.

Yusop, M. I. M., N. H. Kamarudin, N. H. S. Suhaimi, and M. K. Hasan. (2025). "Advancing Passwordless Authentication: A Systematic Review of Methods, Challenges, and Future Directions for Secure User Identity". *IEEE Access*.

Zanasi, C., S. Russo, and M. Colajanni. (2024). "Flexible zero trust architecture for the cybersecurity of industrial IoT infrastructures". *Ad Hoc Networks*. 156: 103414.

Zeilenga, K. (2006). "Lightweight Directory Access Protocol (LDAP): The Protocol".