Secure Communication Networks and Distributed Systems for a Resilient Society (TC 11 Briefing Paper)

Mathias Fischer[a], Joaquin Garcia-Alfaro[b], Dogan Kesdogan[c], Zoltán Ádám Mann[d]

[a] *University of Hamburg, Hamburg, Germany*
[b] *SAMOVAR, Télécom Sudparis, Institut Polytechnique de Paris, 91120 Palaiseau, France*
[c] *University of Regensburg, Regensburg, Germany*
[d] *University of Münster, Münster, Germany*

Abstract

Given the central role of modern digital technologies, it is crucial that digital infrastructures and information systems be resilient. Unfortunately, communication networks and interconnected IT systems are not always secure nor reliable. They are susceptible to design and implementation flaws, which make them vulnerable to attacks. This briefing paper aims to examine the root causes of this problem and how we could address them. We start by exploring some practical scenarios that demonstrate failures in the construction of secure networks and distributed systems. We then explore technical and non-technical challenges as potential root causes of these failures and conclude with a call to action to address the issues. We find that several stakeholder groups – particularly researchers, developers, decision-makers, and policy-makers – must take action to ensure that networks and distributed systems become more secure and resilient in the future.

Keywords: Network security, Distributed system security, Cybersecurity, Security requirements, Security risk assessment.

1. Introduction

Communication networks and distributed software applications have transformed our society. Activities such as reading and writing e-mails, collecting information from the web, connecting with friends via social media, performing online financial transactions, video streaming, and online shopping would not be possible without the ubiquitous connectivity to which we have become accustomed. As a result, our societies are becoming increasingly dependent on this connectivity. Unfortunately, the increasing complexity and size of today's networks and distributed systems make them more error-prone [1]. They also become increasingly attractive targets for adversarial actors [2]. There is an ongoing arms race between those who try to secure networks and distributed systems and those who try to attack them [3].

There is a large amount of literature on the security of computer networks and distributed systems, including vulnerabilities, attacks, and defense techniques. For example, recent literature reviews have focused on cybersecurity in specific domains, such as cyber-physical systems [4] and smart grids [5], or security using certain technologies, such as malware classification [6] and deep reinforcement learning [7].

Despite all previous efforts, the security of computer networks and distributed systems is still problematic. Apparently, there are fundamental, recurring problems. This paper focuses on those fundamental problems. Some of these problems may be well known or intuitively clear. Yet, we need to investigate and address them to be able to build more secure networks and distributed systems.

This briefing paper aims to reflect on the security of networks and distributed systems. We want to understand to what extent such systems can reliably support societal goals. We also aim to identify the root causes of cybersecurity challenges and the fundamental issues of network and distributed system security.

This paper makes two key contributions. First, we identify a set of technical and non-technical challenges that fundamentally impact the security of networks and distributed systems. Second, we describe what different stakeholder groups need to do to address the identified challenges.

To this end, in Section 2 we first examine some example scenarios in which security is flawed. We then analyze the challenges that lead to these and other security failures in Section 3. Despite the many promising security solutions proposed so far, these challenges persist because they are linked to intrinsic trade-offs between conflicting goals. In Section 4 we close this briefing paper with a call to action, outlining the responsibilities of various stakeholders to enable more secure networks and distributed systems in the future.

2. Sample scenarios

In this section, we sketch some practical scenarios to show how developers and researchers have failed so far in building secure communication networks and distributed applications. The insecurity of these networks and distributed systems can be explained by different reasons. Some were designed with a focus on functionality and ease of use, rather than security. Others suffer from a high complexity, creating a large attack surface with new threats emerging regularly. Some also suffer from misaligned incentives, with vendors and service providers prioritizing profit over security. All in all, important security objectives are clearly not met in each of the scenarios. The examples also illustrate that security requirements are quite complex, making it necessary to consider many technical and nontechnical aspects in the design of secure systems. These scenarios will be used to drive the analysis of subsequent sections.

2.1. Scenario 1: availability of Internet routing services

The Border Gateway Protocol (BGP) is the de facto routing standard of the Internet, enabling large networks, called Autonomous Systems (ASes), to exchange routing information. When it was designed in the early days of the Internet, security was not considered in its design. This reflects a broader problem in the early days of the Internet, where functionality and convenience were prioritized over security. As a result, the protocol is a constant cause of security problems as it enables Denial-of-Service (DoS) attacks as well as to hijack and redirect traffic destined for other networks [8]. In the last years, BGP attacks caused outages of major web services, e.g., YouTube, Facebook, or Spotify, and were used to redirect and eavesdrop on sensitive communication [9].

2.2. Scenario 2: encryption of network traffic and privacy loss

The rise of ubiquitous traffic encryption is essential for protecting data confidentiality and integrity. This protection can be realized by a wide range of network security protocols that can operate at different layers of the Internet model. On the network layer, protocols like IPsec or WireGuard are available. As transport layer protocols, TLS and QUIC can be used. On the application layer, application-specific protocols like PGP (email encryption) or the signal protocol (instant messaging) can protect the data end-to-end[1]. However, such security protocols regularly expose vulnerabilities. For example, TLS as the most important protocol for web security, already experienced plenty of inherent protocol vulnerabilities and implementation bugs [10]. As TLS and the libraries implementing it, e.g., OpenSSL, are used in a plethora of applications, such vulnerabilities can be devastating and can put the whole Internet ecosystem at risk.

The end-to-end encryption principle assumes that all individuals may use encryption to protect their privacy, without interference or backdoors from third parties, e.g., criminals or law enforcement agencies. End-to-end encryption ensures that only the sender and the intended recipient can access the plaintext data, making it a crucial component of online security and privacy. However, solutions and protocols for end-to-end encryption remain vulnerable to various security threats, including implementation vulnerabilities, inappropriate key management, side-channel attacks, and bad protocol design in general.

Similar issues also apply to other privacy-enhancing technologies. An example from the business world is the implementation of differential privacy by Apple Inc., a concept with deep academic roots that has attracted attention as a promising method for collecting user data with formal privacy guarantees [11]. The announcement of Apple about the introduction of differential privacy mechanisms in their products was initially welcomed as a step forward. However, academic researchers and the EFF civil liberties group later questioned Apple's implementation and the way user behavior was being analyzed [12]. This type of discrepancy is widespread in network security, where security requirements are often confronted by economic interests.

2.3. Scenario 3: insecurity of connected cars

While there are already many connected IoT devices, connected cars are especially interesting, combining safety, security, and privacy concerns. The way they connect with each other, with the road infrastructure, and with backend services promises a wide array of benefits, including improved road safety, improved efficiency, and improved convenience. Connected cars and the backend infrastructure form a large-scale distributed system, also including web interfaces. Even if substantial research in the topic has been conducted [13] and relevant vendors have implemented innovative features, the connected cars ecosystem continues to create security problems, as demonstrated by the following recent examples:

- Volkswagen Group:[2] several terabytes of data about electric cars of the Volkswagen Group (Volkswagen, Seat, Audi, and Skoda) leaked. The data provided detailed movement information of about 800,000 cars. In many cases, the cars could be linked to their owners, revealing movement patterns of those individuals.

- Kia:[3] researchers were able to gain access to personal information of Kia owners, including name, phone number, email address, and physical address, as well as the car's location. In addition, they were able to remotely control some functions of the victim car, including locking and unlocking the car and starting and stopping the engine. The attack was made possible by vulnerabilities in the backend systems for Kia dealers.

- Subaru:[4] security experts found a way to remotely start, stop, lock, unlock, and retrieve the current location of any connected Subaru vehicle, and retrieve the vehicle's complete location history from the past year. The attack was possible using a poorly protected employee portal for administration of the backend of Subaru's in-vehicle infotainment system.

2.4. Summary of the scenarios

The described scenarios cover a wide range of security objectives (availability, integrity, confidentiality, privacy), and even touch upon potential implications on safety. Also, they cover a

[1] The meaning of "end-to-end" may depend on the layer. E.g., while TLS protects communication end-to-end between a client and a server, this may not be enough for application-level end-to-end protection of communication between clients relayed by a server.

[2] https://europarl.europa.eu/doceo/document/E-10-2025-000182_EN.pdf

[3] https://samcurry.net/hacking-kia

[4] https://samcurry.net/hacking-subaru

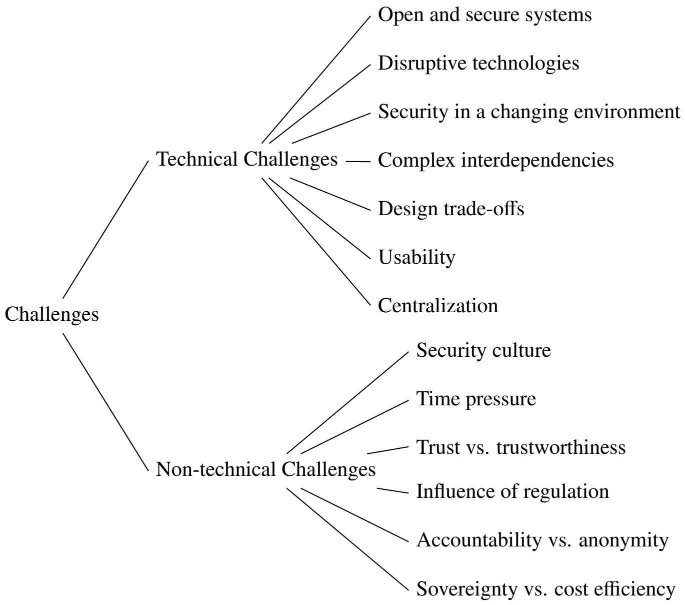

Figure 1: Challenges potentially affecting the construction of secure networks and distributed systems.

wide range of technologies, from network routing through encryption to web interfaces. Thus, they provide a representative set of scenarios for our further investigations. What is common across the three scenarios is that they are all high-stakes applications, built by experts. Still, they exhibit significant security problems, making them particularly suitable for identifying fundamental security challenges.

In the sequel, we explore the challenges that may explain the types of security failures in the scenarios presented above.

3. Challenges

The security of networks and distributed systems has been investigated for several decades. Large amounts of both theoretical knowledge and practical experience has been collected about possible attacks and countermeasures. Researchers have developed sophisticated methods to enhance security. Despite all this progress, attackers regularly manage to infiltrate networks and compromise distributed systems of all scales. Apparently, we are still not able to ensure the security of our networks and distributed systems. The mismatch between attacker models considered during system design and found in practice, as well as discrepancies between design and implementation of security solutions, are just a few examples. Some other potential answers are provided next. We classify them as technical and non-technical challenges, briefly outlined in Figure 1. Some of these challenges are specific to the domain of networks and distributed systems, while others are more general.

3.1. Technical challenges

The design, development, and operation of secure networks and distributed systems faces many technical challenges. In the following, we list those challenges that we find especially critical. Notice that classical security goals like confidentiality, integrity, and availability [14] are related to all of them. In addition, since distributed systems increasingly process personal data, also privacy has become a major goal.

Open and secure systems. Networks and specifically current network protocols are designed to be open, which also is a reason for their success and widespread deployment. They are open to new devices, new clients etc., whose technical specification cannot be fully anticipated. This makes it difficult to ensure security in all configurations that might arise. Furthermore, distributed applications, e.g., modern web applications built on top of these networks use open standards and open protocols as well, thus facing similar security challenges.

The need for open systems that promote interoperability, transparency, and accessibility often conflicts with security requirements focusing on confidentiality and integrity. Open systems are by design easily accessible, also by malicious users, and thus have a bigger threat surface. When designs and specifications are open, vulnerabilities are visible to everyone, including malicious actors [15]. In principle, community resources can help identify vulnerabilities early on and fix them before malicious actors could exploit them. However, not every open-source project receives enough public scrutiny to make this happen.

Disruptive technologies. Attackers can make use of new technologies to perform attacks more effectively. Sometimes, disruptive new technologies render old assumptions behind security models obsolete. For example, attackers can now use generative AI models to bypass authentication methods that were considered secure in the past [16]. As another example, attackers might be able to use quantum technologies in the future to break cryptographic procedures that were assumed to be secure [17]. Defenders may also use the potential of the same disruptive technologies to increase security, although at the cost of new security challenges. For instance, both AI models and quantum technologies that defenders could use are prone to new security threats, including injection of poisoned data [18] and malicious entanglement attacks [19], for which no bullet-proof countermeasures exist.

Security in a changing environment. Many networks and distributed systems evolve over years, or even decades. Even if a system is designed to be secure at the time it enters production, it is difficult to keep it secure in spite of all the changes in its environment, including changes in hardware, software, security knowledge, regulations etc., during its life cycle [20]. Some changes in the environment may be handled with manual updates, while others are so fast that they require an automatic reaction. Automated reaction to changes also introduces risks, as shown for example by the 2024 CrowdStrike-related global IT outages [21] as a collateral damage of enabling automatic patches due to the fast changes of the CrowdStrike Endpoint Detection and Response (EDR) tools.

Complex interdependencies. Modern networks and distributed systems comprise many different components that interact with each other in non-trivial ways. An allegedly small change in one component may have significant unforeseen effects on another component. This makes it very difficult to ensure overall system security and, in particular, to ensure that changes during the system life cycle do not lead to new vulnerabilities. The secure composition of components that are secure in themselves remains a major challenge.

Design trade-offs. When a system is designed, security is just one of many requirements. In many cases, rich functionality, high performance, and low costs are considered, explicitly or implicitly, more important than security. For example, when designing a distributed system, architects may opt for using a centralized database, because this allows more powerful and more efficient data analytics. On the other hand, keeping data decentralized could offer advantages in terms of security, e.g., better availability and better privacy. By choosing the centralized option, architects give preference – often without even an explicit consideration – to functionality and performance over security and privacy.

Usability. In many cases, security measures make systems more complex, making it also more complicated to work with them. This may put additional burden on users. For example, forcing users to solve CAPTCHAs to fight bots may degrade the user experience significantly [22, 23]. While usable systems favor simplicity, security may impose multiple new layers which, again, increase complexity, decrease usability, and can even augment the overall threat surface. As a result, users and developers may circumvent security measures or choose insecure options to simplify their interaction with technology. For instance, password recovery methods, while improving usability, may lead to additional attack vectors. Likewise, legally enforced user notifications regarding leveraged cookies, while improving privacy via transparency, may disturb users who, unaware of long-term implications, may in the end accept or reject cookies by mistake. Thus, the challenge is to create secure and usable systems, by resolving conflicting goals in terms of security vs. usability.

Centralization. A central deployment of services eases their deployment and operation. It simplifies data management and keeping data consistent. Regulators favor this approach as it also eases oversight. Decentralization in turn strengthens resilience to failures and attacks. It induces a distributed storage and processing of data, which is, as mentioned above, beneficial for security and privacy as well. However, not everything can be reasonably decentralized, especially when consistency is required. Decentralization may also increase redundancy and affect scalability properties. In distributed systems, the CAP theorem [24] formulates a fundamental limit. It forces developers to choose at most two out of the three desirable properties of consistency, availability, and partition tolerance. All three cannot be realized jointly, even though mitigation approaches for different application scenarios exist. Thus, the possibilities for decentralization are limited, even if decentralization would be favorable from a security and privacy point of view.

3.2. Non-technical challenges

Beside the technical challenges, the security of networks and distributed systems also faces several non-technical challenges. The boundary between technical and non-technical challenges is not always clear-cut. Nevertheless, we find the distinction important, also to emphasize that security (or the lack thereof) is affected by technical and non-technical aspects alike. We list here the ones that seem most critical to us.

Security culture. In many cases, technical solutions to improve security are available, but they are not used or not properly used [25]. The reasons for this phenomenon are wide-ranging and are rooted in education, incentives, company policies and processes, and role models, among other things. Without concerted and sustained efforts to nourish a culture in which security requirements are considered important by all involved stakeholders and are fully enforced, insecure products will continue to be created.

Time pressure. Often, pushing a new system or a system update into production is considered urgent. This may prohibit certain time-consuming measures to enhance security, such as thorough security testing, security audits, or formal security proofs. Omitting these activities can lead to the deployment of immature solutions, pushing users into the role of beta testers, and potentially leading to significant damage by exploits of zero-day vulnerabilities.

Trust vs. trustworthiness. Trust refers to the *belief* that another party will act reliably, in accordance with our expectations [26]. This belief may or may not be justified, as a trusted party may or may not be *trustworthy*. In networks and distributed systems, trustworthiness of remote entities is difficult to establish. Indirect mechanisms such as collecting information about reputation based on past interactions may help make informed decisions about which parties to trust, but such mechanisms do not give real assurance about the other parties' trustworthiness. Thus, there is a residual risk that trusted entities may actually be untrustworthy, leading to potentially serious vulnerabilities [27]. Assessing these risks is critical, but is often difficult in practice. Also, these risks may dynamically change over time. For example, suppliers of hardware or software components that were considered trustworthy in the past may suddenly become untrustworthy because of a take-over or geo-political changes.

Influence of regulation. Cybersecurity-related regulation aims at both compliance and implementation of rules to ensure that a given technology operates in a safe and fair way. It targets as well how societal interests and political purposes must be met [28]. In the end, it shall ensure a proper balance between the way a technology must be used and the effects it may generate. Yet, challenges may appear at the inception of the regulatory process itself, since it may take place after a specific technology has already been put in use or it is already widely adopted. As with any other system designed to enforce high-level rules, cybersecurity-related regulation can be attacked. Enforcement of rules may suffer from issues with consistency and completeness, hence leading to flaws. Powerful attackers can target and exploit such flaws and put a limit to the objectives of the regulatory process [29].

Accountability vs. anonymity. Freedom of speech is a foundation of democracy and is threatened all over the world. Anonymous communication over networks ensures that networks cannot be turned into tools of mass surveillance and used for suppressing critical opinions. At the same time, there is a valid interest, e.g., from law enforcement authorities, to identify the originators of certain malicious actions. This requires knowing where data packets originate and keeping track of user actions to hold individual users accountable. Anonymity and accountability may both be desirable, but they are conflicting requirements that cannot be satisfied at the same time.

Solutions like "balanced network anonymity" [30] offer anonymity by default but under the control of a trusted public authority. If needed, the public authority can deanonymize users, but everyone else cannot. This allows to deanonymize users in case of misbehavior. A naive implementation of this scheme is to store mappings of IP addresses to users at Internet Service Providers (ISPs), as already implemented in several countries. Governmental authorities can request access if needed, e.g., after a court order. However, this approach does not protect against a malicious public authority, so that this solution also comes with risks.

Sovereignty vs. cost efficiency. Technical sovereignty ensures independence from external actors for critical technologies. Pursuing greater sovereignty entails foregoing the cost efficiencies gained through the economies of scale that large global providers achieve via extensive scaling and resource pooling. Preferring local providers that do not have these scale benefits means that the costs increase. Ensuring sovereignty may require the implementation of additional features like data residency or local control, which may negatively affect performance, beyond costs. It may require special infrastructure, local data centers and custom solutions that all can drive up costs compared to standardized cloud services.

3.3. Summary of findings

Table 1 provides a potential (but non-exhaustive) mapping between the scenarios provided in Section 2 and the challenges discussed in Sections 3.1–3.2. Many of the described challenges impact the scenarios mentioned earlier, thus potentially contributing to the security problems encountered in those scenarios. It is also interesting to note that many challenges stem from conflicts among the societal values that drive the requirements for networks and distributed systems (e.g., accountability vs. anonymity) [31].

There is a pool of accumulated knowledge in the field of network security research that could be used in new technologies such as traffic analysis, anomaly detection, encryption, and privacy protection [32]. However, the maturity and dissemination of corresponding security products often lag behind the academic breakthroughs. While the research community publishes innovative methods with solid theoretical guarantees, the implementation of these methods often remains weak due to diverging and contradicting economic interests. For instance, users have a strong interest in cost-effective technology and in informational sovereignty, but due to the free web culture, users are reluctant to pay for services, software, or information. The industry has a strong economic interest in equipping people with more and more digital devices that support nearly every aspect of daily life, from communication and health monitoring to navigation and entertainment. However, when it comes to information sovereignty, this pattern is often reversed. Rather than providing users with clear, accessible, and actionable security information, companies often place greater value on customer loyalty and ecosystem lock-in. Providing tools and knowledge that would enable users to make independent and privacy-conscious decisions is often not consistent with commercial goals. As a result, transparency, configurability, and user education are all too often neglected, creating systems in which individuals are dependent rather than sovereign.

Table 1: Challenges of Section 3 that may impact the scenarios of Section 2

Challenge	Scenario		
	Internet routing	Encryption & privacy	Connected cars
Technical			
Open and secure systems	✓		✓
Disruptive technologies		✓	✓
Security in a changing environment		✓	✓
Complex interdependencies	✓		✓
Design trade-offs	✓	✓	✓
Usability		✓	
Centralization	✓		✓
Non-technical			
Security culture	✓		✓
Time pressure			✓
Trust vs. trustworthiness		✓	
Influence of regulation		✓	✓
Accountability vs. anonymity	✓		✓
Sovereignty vs. cost efficiency		✓	

4. Call to action

As shown in the previous section, the security of communication networks and distributed systems faces many challenges. Fortunately, many approaches have been proposed in recent years to make networks and distributed systems more secure. Examples of promising new developments include the use of advanced artificial intelligence techniques in network security [33], proactive defense mechanisms like moving target defense [34], and the transition to zero-trust architectures [35]. However, these techniques are no silver bullets. As shown in Section 3, we must deal with a wide variety of fundamental challenges that specific technologies alone cannot solve. To make substantial improvements, we need concerted efforts from different stakeholders. This section thus contains different calls to action for different stakeholders at different levels, to jointly enhance the security of our modern communication and IT systems.

Researchers need to develop methods that help manage the complexity of networks and distributed systems. We need more research on resolving conflicting goals, allowing the design of systems that are secure and efficient at the same time. Researchers also need to engage with policy-makers to explain to them the need for security measures and their consequences, thus contributing to better policy-making.

Developers are responsible for implementing security by design and privacy by design, thus avoiding that security becomes an afterthought that cannot be integrated easily anymore (e.g., as was the case with BGP). In the systems they create, developers should aim at minimizing the need for trust as much as possible, preferring technologies with guaranteed security properties instead. Developers should aim to limit the complexity of their systems and be mindful of trade-offs between security and other goals.

Decision makers, such as corporate management executives, are responsible for establishing and maintaining a security culture in their organization, by prioritizing security in budget decisions, job profiles and employee skill development, as well as incentives and performance reviews. They need to make sure that sufficient time and sufficient resources are allocated to security aspects in product development and maintenance. Decision makers should communicate the importance of security and act accordingly on the strategic, tactical, as well as operative level.

Policy makers need to align closely with researchers and other technology experts to develop a deep understanding of the needs and possibilities of the field, which is the basis for creating useful legislation. In particular, they need to understand the technical implications of different policy options. For example, efforts by policy makers to undermine end-to-end encryption to provide better observability for law enforcement are understandable, but they put the whole Internet ecosystem at risk. In addition, a general security awareness is needed among policy makers to ensure that security is included from the beginning in regulating all network-related technologies.

Acknowledgements

The authors would like to thank the participants of the 2025 International Workshop on Network and Distributed Systems Security (WNDSS 2025) for their inputs. In addition, the authors would like to thank the members of IFIP Working Group 11.4 “Network & Distributed Systems Security”, in particular Dave Singelée and Alexandra Dmitrienko, for feedback on an earlier draft of the paper.

Declaration of Competing Interest

This paper is produced by members of the IFIP Technical Committee 11 and has undergone an internal review process by independent reviewers from within the TC.

There are no conflicts of interest.

References

[1] L. Mariani, M. Pezzè, O. Riganelli, R. Xin, Predicting failures in multi-tier distributed systems, Journal of Systems and Software 161 (2020). doi:10.1016/j.jss.2019.110464.

[2] F. Heiding, S. Katsikeas, R. Lagerström, Research communities in cyber security vulnerability assessments: A comprehensive literature review, Computer Science Review 48 (2023). doi:10.1016/j.cosrev.2023.100551.

[3] C. T. Do, N. H. Tran, C. Hong, C. A. Kamhoua, K. A. Kwiat, E. Blasch, S. Ren, N. Pissinou, S. S. Iyengar, Game theory for cyber security and privacy, ACM Computing Surveys (CSUR) 50 (2) (2017). doi:10.1145/3057268.

[4] Z. Lian, P. Shi, M. Chen, A survey on cyber-attacks for cyber-physical systems: Modeling, defense and design, IEEE Internet of Things Journal 12 (2) (2025) 1471–1483. doi:10.1109/JIOT.2024.3495046.

[5] H. T. Reda, A. Anwar, A. N. Mahmood, Z. Tari, A taxonomy of cyber defence strategies against false data attacks in smart grids, ACM Computing Surveys 55 (14s) (2023). doi:10.1145/3592797.

[6] S. Yan, J. Ren, W. Wang, L. Sun, W. Zhang, Q. Yu, A survey of adversarial attack and defense methods for malware classification in cyber security, IEEE Communications Surveys & Tutorials 25 (1) (2022) 467–496. doi:10.1109/COMST.2022.3225137.

[7] T. T. Nguyen, V. J. Reddi, Deep reinforcement learning for cyber security, IEEE Transactions on Neural Networks and Learning Systems 34 (8) (2021) 3779–3795. doi:10.1109/TNNLS.2021.3121870.

[8] T. Holterbach, T. Alfroy, A. Phokeer, A. Dainotti, C. Pelsser, A system to detect Forged-Origin BGP hijacks, in: 21st USENIX Symposium on Networked Systems Design and Implementation (NSDI 24), 2024, pp. 1751–1770.

[9] A. Mitseva, A. Panchenko, T. Engel, The state of affairs in BGP security: A survey of attacks and defenses, Computer Communications 124 (2018) 45–60. doi:10.1016/j.comcom.2018.04.013.

[10] J. Ahn, R. Hussain, K. Kang, J. Son, Exploring Encryption Algorithms and Network Protocols: A Comprehensive Survey of Threats and Vulnerabilities, IEEE Communications Surveys & Tutorials (2025). doi:10.1109/COMST.2025.3526605.

[11] C. Dwork, Differential privacy, in: International Colloquium on Automata, Languages, and Programming, Springer, 2006, pp. 1–12. doi:10.1007/11787006_1.

[12] J. Tang, A. Korolova, X. Bai, X. Wang, X. Wang, Privacy loss in Apple’s implementation of differential privacy on macOS 10.12, arXiv preprint arXiv:1709.02753 (2017). doi:10.48550/arXiv.1709.02753.

[13] X. Sun, F. R. Yu, P. Zhang, A survey on cyber-security of connected and autonomous vehicles (CAVs), IEEE Transactions on Intelligent Transportation Systems 23 (7) (2021) 6240–6259. doi:10.1109/TITS.2021.3085297.

[14] M. Nieles, K. Dempsey, V. Y. Pillitteri, An Introduction to Information Security, NIST Special Publication 800-12, Revision 1 (2017). doi:10.6028/NIST.SP.800-12r1.

[15] G. Schryen, Is open source security a myth?, Communications of the ACM 54 (5) (2011) 130–140. doi:10.1145/1941487.1941516.

[16] C.-Z. Yang, J. Ma, S. Wang, A. W.-C. Liew, Preventing DeepFake Attacks on Speaker Authentication by Dynamic Lip Movement Analysis, IEEE Transactions on Information Forensics and Security 16 (2020) 1841–1854. doi:10.1109/TIFS.2020.3045937.

[17] D. Joseph, R. Misoczki, M. Manzano, J. Tricot, F. D. Pinuaga, O. Lacombe, S. Leichenauer, J. Hidary, P. Venables, R. Hansen, Transitioning organizations to post-quantum cryptography, Nature 605 (7909) (2022) 237–243. doi:10.1038/s41586-022-04623-2.

[18] Z. Tian, L. Cui, J. Liang, S. Yu, A Comprehensive Survey on Poisoning Attacks and Countermeasures in Machine Learning, ACM Computing Surveys 55 (8) (2022). doi:10.1145/3551636.

[19] T. Satoh, S. Nagayama, S. Suzuki, T. Matsuo, M. Hajdušek, R. Van Meter, Attacking the Quantum Internet, IEEE Transactions on Quantum Engineering 2 (2021) 1–17. doi:10.1109/TQE.2021.3094983.

[20] Z. Á. Mann, F. Kunz, J. Laufer, J. Bellendorf, A. Metzger, K. Pohl, RADAR: Data protection in cloud-based computer systems at run time, IEEE Access 9 (2021) 70816–70842. doi:10.1109/ACCESS.2021.3078059.

[21] W. Khern-am nuai, Key lessons learned for technology managers from CrowdStrike global IT outage, IEEE Engineering Management Review 53 (4) (2025) 25–27. doi:10.1109/EMR.2024.3452090.

[22] M. Motoyama, K. Levchenko, C. Kanich, D. McCoy, G. M. Voelker, S. Savage, Re: CAPTCHAs – understanding CAPTCHA-solving services in an economic context, in: 19th USENIX Security Symposium (USENIX Security 10), 2010, pp. 435–452.

[23] B. Ousat, E. Schafir, D. C. Hoang, M. A. Tofighi, C. V. Nguyen, S. Arshad, S. Uluagac, A. Kharraz, The Matter of Captchas: An Analysis of a Brittle Security Feature on the Modern Web, in: Proceedings of the ACM Web Conference 2024, 2024, p. 1835–1846. doi:10.1145/3589334.3645619.

[24] S. Gilbert, N. Lynch, Brewer's conjecture and the feasibility of consistent, available, partition-tolerant web services, ACM SIGACT News 33 (2) (2002) 51–59. doi:10.1145/564585.564601.

[25] A. Naiakshina, A. Danilova, E. Gerlitz, E. Von Zezschwitz, M. Smith, "if you want, I can store the encrypted password": A password-storage field study with freelance developers, in: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, 2019, p. paper 140. doi:10.1145/3290605.3300370.

[26] N. Luhmann, Familiarity, confidence, trust: Problems and alternatives, in: D. Gambetta (Ed.), Trust: Making and Breaking Cooperative Relations, Oxford University Press, 2000, Ch. 6, pp. 94–107.

[27] P. C. Van Oorschot, Computer Security and the Internet (Chapter 1. Security Concepts and Principles), 2nd Edition, Springer, 2021. doi:10.1007/978-3-030-83411-1.

[28] D. Markopoulou, V. Papakonstantinou, The regulatory framework for the protection of critical infrastructures against cyberthreats: Identifying shortcomings and addressing future challenges: The case of the health sector in particular, Computer Law & Security Review 41 (2021). doi:10.1016/j.clsr.2020.105502.

[29] B. Schneier, A Hacker's Mind: How the Powerful Bend Society's Rules, and How to Bend Them Back (Chapter 30. Undermining Regulations), W. W. Norton, 2023.

[30] Y. Xia, R. Chen, J. Su, H. Zou, Balancing anonymity and resilience in anonymous communication networks, Computers & Security 101 (2021). doi:10.1016/j.cose.2020.102106.

[31] Z. Á. Mann, J. Petit, S. M. Thornton, M. Buchholz, J. Millar, SPIDER: Interplay assessment method for privacy and other values, in: 2024 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), IEEE, 2024, pp. 1–8. doi:10.1109/EuroSPW61312.2024.00007.

[32] S. Jajodia, P. Samarati, M. Yung, Encyclopedia of Cryptography, Security and Privacy, Springer, 2025. doi:10.1007/978-3-030-71522-9.

[33] G. Apruzzese, P. Laskov, E. Montes de Oca, W. Mallouli, L. Brdalo Rapa, A. V. Grammatopoulos, F. Di Franco, The role of machine learning in cybersecurity, Digital Threats: Research and Practice 4 (1) (2023) 1–38. doi:10.1145/3545574.

[34] Z. Rehman, I. Gondal, M. Ge, H. Dong, M. Gregory, Z. Tari, Proactive defense mechanism: Enhancing IoT security through diversity-based moving target defense and cyber deception, Computers & Security 139 (2024). doi:10.1016/j.cose.2023.103685.

[35] W. Yeoh, M. Liu, M. Shore, F. Jiang, Zero trust cybersecurity: Critical success factors and a maturity assessment framework, Computers & Security 133 (2023). doi:10.1016/j.cose.2023.103412.