computers

Editorial

From Mean Time to Failure to Mean Time to Attack/Compromise: Incorporating Reliability into Cybersecurity

Leandros Maglaras [1,2]

[1] School of Computer Science and Informatics, De Montfort University, Leicester LE1 9BH, UK
[2] Blockpass ID Lab, Edinburgh Napier University, Edinburgh EH10 5DT, UK

Around the world, numerous companies strive to successfully facilitate digital transformation. One of the key goals of many countries around the globe is the development of its digital infrastructure [1]. Whether in the public or private sectors, achieving data and infrastructure security is crucial to the success of any digital transformation. To guarantee a smooth and secure digital transformation, IT system security in all enterprises requires specific attention. People are becoming more reliant on ICT technology to do daily tasks at home or at work as a result of the digital revolution [2]. Systems that support essential elements of this intelligent way of living are classified as critical, and their security level is higher than that of other systems. The idea of digitally managed services, which include security monitoring, managed network services, or the outsourcing of business processes that are essential to the operation, dependability, and availability of critical national infrastructures, has been introduced by novel cybersecurity regulations. Following the COVID-19 epidemic, which compelled practically all daily operations to go digital, this shift is being emphasized more than before [3]. This unexpected transformation has an impact on almost every industry, including critical infrastructures, education and others. Furthermore, because of the lockdown brought on by the Coronavirus epidemic, online and remote working are now crucial. However, because many companies were not prepared to employ e-working technologies, several difficulties arose while attempting to digitize the business processes, including the lack of cybersecurity preparedness [4].

There are already a variety of frameworks on the market that businesses may use to increase the effectiveness of their cybersecurity [5]. These frameworks encourage both individual and corporate action. As emphasized already [6,7], there is a high significance of providing employees with training and information security awareness in order for any security improvement program chosen by an organization to be successful and secure [8]. Teaching front-end users will act as the first line of defense against attackers, thus this should be incorporated into the risk/security assessment plan followed by all levels of administration [9].

A system's or infrastructure's cybersecurity posture can be evaluated using a number of techniques, such as vulnerability assessment [10], risk management, maturity assessment, or posture assessment. An enterprise can create a successful information management system, standardize cybersecurity rules, and increase the security of an organization by using well-known cybersecurity frameworks like NIST or ISO. These frameworks can be incredibly effective in aiding organizations in comprehending the dangers they face, analyzing their vulnerabilities, and organizing their security countermeasures and mitigation plans. To better represent the system processes and operations, those models still need to be modified for use in specialized fields like banking, healthcare, maritime [11,12], education [13] or vital components like critical infrastructures [14] and industrial systems [15]. Many of the proposed frameworks define a set of metrics for gauging organizational maturity or competency in terms of a collection of widely accepted best practices, competencies, or

Citation: Maglaras, L. From Mean Time to Failure to Mean Time to Attack/Compromise: Incorporating Reliability into Cybersecurity. *Computers* **2022**, *11*, 159. https://doi.org/10.3390/computers11110159

Received: 4 November 2022
Accepted: 7 November 2022
Published: 8 November 2022

standards. To conduct a gap analysis against several security requirements, MAFs may combine the General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI DSS), and Data Security and Protection Toolkit (DSPT), among others, depending on the business processes of the business sector. The metrics used can be classified into groups and expressed in terms of performance. The measurable transitions between levels are usually based on empirical data that have been validated in practice, and each level in the model is more mature than the previous level. Although the existing maturity models have managed to incorporate several directives, regulations and frameworks, and have been tailored to specific sectors, they still fail to incorporate the reliability aspect of a system [16,17].

On the other hand, reliability is a metric used to gauge a system's capacity to execute in accordance with its requirements under given temporal and operational conditions. The possibility that the system will function properly for a set amount of time is known as reliability [18]. The system's ability to meet the needs of the application is dependent on those requirements. We must have a thorough grasp of the system's constituent parts and how they function in order to determine the system's reliability. Calculating the dependability of each subsystem or entity, as well as their connections and inter-dependencies, is necessary to determine a system's reliability. The Mean Time to Failure (MTTF) and Mean Time to Repair (MTTR), among other measures, are used to measure the system's reliability. For many years, extremely critical systems have been developed with a focus on reliability, efficiency, and optimization. The robustness of a system can be supported by the use of reliability theory in analyzing the behavior of complicated systems and creating ones that are incredibly stable. By embracing the fundamental ideas of reliability, securability can be used as a metric to show how well a system can function in accordance with the demands of the services it is being supplied [19–22].

Since faults and failures are elements that affect the system's proper operation, they can and ought to be considered in the analysis of securability [23]. The triptych of analysis, prediction, and optimization is where the concept of security is found. The operation of the system under analysis could be modeled using terms like Mean Time to Attack (MTTA), Mean Time to Compromise [24] and Mean Time to Recovery (MTTR), which are based on current incident response and mitigation plans. Using patterns that combine security and dependability and attack prediction using Markov models, some initial steps in this approach have already been taken [25]. New methodologies that could define the system requirements by incorporating security (and privacy) with reliability (and safety), however, are still lacking and are anticipated to be introduced in the upcoming years. These methodologies would also introduce a new research area under the umbrella term of securability.

Another interesting concept would be to manage to integrate the reliability analysis as a part of a maturity assessment framework, like the risk analysis element that already is incorporated in many MAFs. The idea of including a probabilistic model of the behavior of a part (or the whole system) in terms of tentative failures or errors could provide a better picture of the system in analysis and a prediction of future states [21]. As an example lets imagine that we are trying to analyze a system's behavior (from a high level perspective) when the also have a disaster recovery facility in place. Data and computer processing must be replicated at an off-premises location unaffected by the incident for disaster recovery to work. A business must restore lost data from a backup location when servers go down due to a natural disaster, equipment malfunction, or cyberattack. In order to maintain operations, a company should be able to move its computer processing to that distant site as well, thus managing to continue to offer the services to the clients [26].

The main system is represented as MS and the Disaster Recovery Site as DR. Working in an abstract level, we can represent the states of the system using a Markov chain (See Figure 1), where

- State A is when both the system and the DR site are operating normally.
- State B is when the system is down due to a malfunction or attack.

- State C is when the DR site is off.
- State D is when both S and DR are off.

and

- λ_{MS} is the failure rate of the system, and
- λ_{DR} is the error rate of the Disaster Recovery Site.

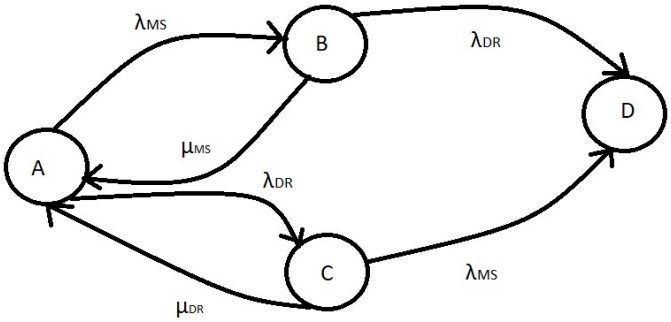

Figure 1. State transition rate diagram of a system.

The transition from State B or State C to State A is done with rates μ_{MS} and μ_{DR}, respectively, representing the repair/restore rate of the system/DR. In order for the organization to be able to offer the service 24/7, the λ rates must be smaller compared to μ rates. Using the Markov model of Figure 1, we can calculate the MTTF (Mean Time to Failure) or MTTA (or Mean Time to Attack) and the MTTR (Mean Time to Restore, Respond or Repair depending on the model we are using). The correct values of the these rates demand a thorough analysis of the components of the systems, their inter-dependencies [27], along with an up to date threat assessment. This analysis is demanding and must be done in several steps following a top-down approach. The main system can be divided into sub-systems. A state transition diagram must be created for each sub-system along with a general model that will represent the dependencies among subsystems in the general form r out of n (r-out of n:G). In this model, the at least r subsystems (or elements) must be in a good state in order for the system to be operational [28]. When incorporating cybersecurity into this reliability analysis, the calculation of the failure probability of each component must include failures as well as possible attacks.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Data sharing not applicable.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Shenglin, B.; Simonelli, F.; Ruidong, Z.; Bosc, R.; Wenwei, L. Digital infrastructure: Overcoming the digital divide in emerging economies. *G20 Insights* **2017**, *3*, 1–36.
2. Corallo, A.; Lazoi, M.; Lezzi, M. Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. *Comput. Ind.* **2020**, *114*, 103165. [CrossRef]
3. Pranggono, B.; Arabo, A. COVID-19 pandemic cybersecurity issues. *Internet Technol. Lett.* **2021**, *4*, e247. [CrossRef]
4. Norris, D.F.; Mateczun, L.; Joshi, A.; Finin, T. Cyberattacks at the grass roots: American local governments and the need for high levels of cybersecurity. *Public Adm. Rev.* **2019**, *79*, 895–904. [CrossRef]
5. Sulistyowati, D.; Handayani, F.; Suryanto, Y. Comparative analysis and design of cybersecurity maturity assessment methodology using nist csf, cobit, iso/iec 27002 and pci dss. *JOIV Int. J. Inform. Vis.* **2020**, *4*, 225–230. [CrossRef]
6. Chouliaras, N.; Kittes, G.; Kantzavelou, I.; Maglaras, L.; Pantziou, G.; Ferrag, M.A. Cyber ranges and testbeds for education, training, and research. *Appl. Sci.* **2021**, *11*, 1809. [CrossRef]

7. Karagiannis, S.; Ntantogian, C.; Magkos, E.; Ribeiro, L.L.; Campos, L. PocketCTF: A fully featured approach for hosting portable attack and defense cybersecurity exercises. *Information* **2021**, *12*, 318. [CrossRef]
8. Zwilling, M.; Klien, G.; Lesjak, D.; Wiechetek, Ł.; Cetin, F.; Basim, H.N. Cyber security awareness, knowledge and behavior: A comparative study. *J. Comput. Inf. Syst.* **2022**, *62*, 82–97.
9. He, Y.; Camacho, R.S.; Soygazi, H.; Luo, C. Attacking and defence pathways for intelligent medical diagnosis system (IMDS). *Int. J. Med. Inform.* **2021**, *148*, 104415. [CrossRef]
10. Kioskli, K.; Polemi, N. Estimating Attackers' Profiles Results in More Realistic Vulnerability Severity Scores 2022. In Proceedings of the 13th International Conference on Applied Human Factors and Ergonomics (AHFE 2022), San Francisco, CA, USA, 20–24 July 2022.
11. Boullauazan, Y.; Sys, C.; Vanelslander, T. Developing and demonstrating a maturity model for smart ports. *Marit. Policy Manag.* **2022**, 1–19. [CrossRef]
12. Papastergiou, S.; Polemi, D. Securing maritime logistics and supply chain: The medusa and mitigate approaches. *Marit. Interdiction Oper. J.* **2017**, *14*, 42–48.
13. Aliyu, A.; Maglaras, L.; He, Y.; Yevseyeva, I.; Boiten, E.; Cook, A.; Janicke, H. A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom. *Appl. Sci.* **2020**, *10*, 3660. [CrossRef]
14. Drivas, G.; Chatzopoulou, A.; Maglaras, L.; Lambrinoudakis, C.; Cook, A.; Janicke, H. A nis directive compliant cybersecurity maturity assessment framework. In Proceedings of the 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC), Madrid, Spain, 13–17 July 2020; IEEE: Piscataway, NJ, USA, 2020; pp. 1641–1646.
15. Janicke, H.; Nicholson, A.; Webber, S.; Cau, A. Runtime-monitoring for industrial control systems. *Electronics* **2015**, *4*, 995–1017. [CrossRef]
16. Kour, R.; Karim, R.; Thaduri, A. Cybersecurity for railways—A maturity model. *Proc. Inst. Mech. Eng. Part F J. Rail Rapid Transit* **2020**, *234*, 1129–1148. [CrossRef]
17. Dube, D.P.; Mohanty, R. The application of cyber security capability maturity model to identify the impact of internal efficiency factors on the external effectiveness of cyber security. *Int. J. Bus. Inf. Syst.* **2021**, *38*, 367–392. [CrossRef]
18. Rajawat, A.S.; Bedi, P.; Goyal, S.; Shaw, R.N.; Ghosh, A. Reliability Analysis in Cyber-Physical System Using Deep Learning for Smart Cities Industrial IoT Network Node. In *AI and IoT for Smart City Applications*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 157–169.
19. Buckley, I.A.; Fernandez, E.B.; Larrondo-Petrie, M.M. Patterns combining reliability and security. In Proceedings of the International Conferences on Pervasive Patterns and Applications, IARIA Conferences, XPS (Xpert Publishing Services), Rome, Italy, 25–30 September 2011; pp. 144–150.
20. Maglaras, L.A.; Ferrag, M.A.; Janicke, H.; Ayres, N.; Tassiulas, L. Reliability, Security, and Privacy in Power Grids. *Computer* **2022**, *55*, 85–88. [CrossRef]
21. Holgado, P.; Villagrá, V.A.; Vazquez, L. Real-time multistep attack prediction based on hidden markov models. *IEEE Trans. Dependable Secur. Comput.* **2017**, *17*, 134–147. [CrossRef]
22. Zhang, Y.; Wang, L.; Xiang, Y.; Ten, C.W. Power system reliability evaluation with SCADA cybersecurity considerations. *IEEE Trans. Smart Grid* **2015**, *6*, 1707–1721. [CrossRef]
23. Stamp, J.; McIntyre, A.; Ricardson, B. Reliability impacts from cyber attack on electric power systems. In Proceedings of the 2009 IEEE/PES Power Systems Conference and Exposition, Seattle, WA, USA, 15–18 March 2009; IEEE: Piscataway, NJ, USA, 2009; pp. 1–8.
24. Leversage, D.J.; Byres, E.J. Estimating a system's mean time-to-compromise. *IEEE Secur. Priv.* **2008**, *6*, 52–60. [CrossRef]
25. Kharchenko, V.; Ponochovnyi, Y.; Ivanchenko, O.; Fesenko, H.; Illiashenko, O. Combining Markov and Semi-Markov Modelling for Assessing Availability and Cybersecurity of Cloud and IoT Systems. *Cryptography* **2022**, *6*, 44. [CrossRef]
26. Ali, K.E.; Mazen, S.A.; Hassanein, E. A proposed hybrid model for adopting cloud computing in e-government. *Future Comput. Inform. J.* **2018**, *3*, 286–295. [CrossRef]
27. Marotta, A. Cybersecurity Dynamics: Mapping Multiple Interdependencies 2021. Available online: ttps://pure.southwales.ac.uk/en/studentTheses/cybersecurity-dynamics-mapping-multiple-interdependencies (accessed on 10 October 2022).
28. Endharta, A.J.; Yun, W.Y.; Ko, Y.M. Reliability evaluation of circular k-out-of-n: G balanced systems through minimal path sets. *Reliab. Eng. Syst. Saf.* **2018**, *180*, 226–236. [CrossRef]