Chapter 8
Blockchain as an Enabler for Zero-Trust Architectures

ABSTRACT

From the lessons that can be learned so far in this book, the author justifies why a new strategy is required to refocus our perception and utilization of computerized capabilities in the future. Chapter 8 focuses on the advancement of the cyber security discipline by determining trust-less control-sets – a fourth dimension if you will, comprising blockchain technology. Blockchain has been implemented in fungible forms, such as public bitcoin and Ethereum, and in a non-fungible manner like private keyless signature infrastructure. It is the latter that is of particular interest, where proven implementations have the potential to demonstrably act as a verifiable trust anchor, embellishing cyber security controls in a number of critical areas to ensure (1) preservation of data integrity, (2) digital finger printing of IoT assets to prove the source of data is trustworthy, (3) validation of identity and access management mechanisms, and (4) software provenance in the supply chain for not only traditional code-bases but also AI algorithms.

INTRODUCTION

A trust-less technology like blockchain could be an answer to a considerable number of technical challenges already highlighted over successive chapters in this book. This is because historically systems must apply levels of access control based on trust which is at the center of many security incidents –

DOI: 10.4018/978-1-7998-3979-8.ch008

whether it be human or automated machine processes. Examples already covered include: (a) data losses through insider misuse; (b) abusing or exposing data; and (c) outsiders gaining traction through cyber-attacks against computer systems using privilege elevation to cause nefarious damage or conduct data exfiltration. According to John Kindervag (Greengard, 2018), relying on outdated or improperly thought through trust models has been the main catalyst for most data breaches. He advocates a 'zero-trust' approach that can enable organizations to focus on determining which assets are important and need protecting, such as properly applying a need-to-know and least-privilege model supported by monitoring and log inspection (Greengard, 2018). AWS already advocates an approach in which one set of credentials and privileges do not enable users full trusted access; rather, there is a granular approach for human access control by: (a) roles and groups; (b) MFA; (c) least privilege allocation coupled with permissions; (d) supported by network access control; and (e) auditable logs (Columbus, 2019; Gerritz, 2020).

Gault (2019) justified how a mechanism like PKI requires an additional measure to assure data integrity based on a verifiable state of truth (Gault, 2019a). Integrity is a particularly important control that is generally shrouded by the need for confidentiality, in which the use of cryptography generally covers both aspects. However, this can create a *« double entendre problème »* because encryption can affect performance. Gault makes a compelling case, quoting Schneier (2016) to say that since the 90s, there has been a fixation on the protection of data-in-transit, but there has been less focus on protecting data-at-rest. Consequently, there have been many security breaches or events discussed in the first six chapters of this book, in which attackers or abusers have exfiltrated data. When data-in-transit is protected with mutual authentication and encryption through PKI, for example, there can be a performance hit. This fact is especially true for ICS systems. In some way, this explains some of the weaknesses found in CNI systems, notwithstanding some oversights in secure-by-design architectural deployments that may have also occurred. The TRITON case in Chapter 4 is a perfect example of this.

This chapter focuses on a fourth dimension: the advent of blockchain technology that could become a game changer for cyber security. By focusing on the integrity aspect of the CIA triad, blockchain technology changes the stereotypical confidentiality heavy view of cyber security. The technology also provides a trail of immutable transactions, coupled with transparency in a trust-less manner.