Chapter 7
A Rethink of Network Security Through Zero Trust Architecture

Emefa Ama Apaloo
http://orcid.org/0009-0009-1956-6649
Illinois Institute of Technology, USA

Mohithaa Ekambaram
http://orcid.org/0009-0007-0108-1497
Illinois Institute of Technology, USA

ABSTRACT

The growing complexity and decentralization of modern network environments have revealed critical limitations in traditional perimeter-based security models that rely on implicit trust within network boundaries. This chapter examines Zero Trust Architecture as a transformative security paradigm that eliminates inherent trust by enforcing continuous identity verification and least-privilege access based on dynamic contextual factors. By synthesizing existing literature and comparing firewall-centric approaches with identity-driven Zero Trust frameworks, the chapter highlights the necessity of this shift in addressing contemporary threat landscapes. It further outlines an implementation roadmap that considers technical, organizational, and policy challenges associated with deploying Zero Trust across hybrid cloud, edge computing, and distributed systems. The chapter concludes with practical recommendations for security practitioners and identifies key areas for future research to advance the effectiveness and scalability of Zero Trust security models.

DOI: 10.4018/979-8-3373-8252-4.ch007

INTRODUCTION

The Evolving Threat Landscape

The fast-paced development of information technologies, together with widespread cloud, edge, and IoT platform usage, has created a completely new network security environment. Modern organizations experience an increasing threat of complex cyberattacks that strike with high speed, while attackers launch distributed attacks that generate more than 100,000 daily security events regardless of business scale. Security systems no longer protect against threats because these threats now appear in greater numbers with advanced characteristics.

The current threat methods of advanced persistent threats combine AI technology with machine learning to identify system vulnerabilities before executing automated cyber attacks. Ransomware attacks now target vital infrastructure systems as well as medical facilities and banking institutions. The transition to remote work operations has created an enormous new attack area that standard security systems fail to protect against newly introduced threats. The connected nature of systems becomes vulnerable to attacks when trusted third-party relationships are exploited, which breaks down the security model based on perimeter defense.

Limitations of Traditional Perimeter Security

The security model based on perimeter boundaries trusts all users and devices that manage to cross the network boundary. The method worked effectively in centralized computing systems, which had their resources located inside established physical limits. The current model does not function properly in modern distributed systems, which include cloud computing, mobile employees, and connected business networks.

The security measures that protect perimeters fail to protect workers who work remotely, third-party vendors, and cloud-based applications. The trust system operating within the perimeter boundary produces major security vulnerabilities. The network perimeter becomes exposed to attackers who use phishing attacks, steal credentials, or exploit vulnerabilities, which enables them to move between systems with little opposition. The lack of ongoing verification allows attackers to keep control of compromised accounts, which results in data theft, backdoor creation, and major system damage.

The perimeter model based on traditional security methods becomes ineffective when organizations need to defend against attacks that originate from their internal network. The system allows authorized users to misuse their privileges, which results in internal accounts being compromised into dangerous tools for attackers. Organi-