Postprint: Sorting Out Cybersecurity Defenses from the Core of the Internet

Authors:

Date: 2023-10-08T00:00:00+00:00

Abstract

ly speaking, the foundation of computing rests upon 0s and 1s—no matter how complex a system, everything ultimately reduces to binary digits. Similarly, cybersecurity fundamentally revolves around attack and defense, while network architecture consists of endpoints and connections. Regardless of complexity, all networks can be distilled to these basic elements. Consequently, the Internet, mobile Internet, and IoT are essentially indistinguishable at their core.

Full Text

Preamble

ChinaXiv Cooperative Journal: Media Watchtower Special Feature
Building Cybersecurity Defenses from the Core of the Internet

Editor's Note: The development of the Internet and mobile Internet has brought tremendous convenience to human life while simultaneously introducing new security risks.

In recent years, industrial advancement has ushered in an era of IoT (Internet of Things) where everything is interconnected. This connectivity dissolves boundaries and dismantles information barriers, accelerating industrial informatization on one hand while making security an indispensable and critical component on the other. How can we construct a robust cybersecurity defense line to provide security guarantees for the development of the industrial Internet? At the 2018 Annual Conference of the Information Security Professional Committee of China Information Industry Association and the 8th High-End Forum on Cybersecurity Innovation Development, He Yueying, Deputy Director of the Third Research Office of the National Network Information Security Technology Research Institute and Deputy Director of the National Engineering Laboratory for Cybersecurity Emergency Technology, traced the essence of the Internet to

outline cybersecurity protection strategies. This issue excerpts key portions of his presentation for our readers.

The Fundamental Nature of Networks

From the Internet to mobile Internet and then to IoT, IT technology has remained at the core. Before the emergence of the Internet, there existed communication networks and industrial networks, but these were isolated systems with their own standards, operating within separate domains. Abstractly speaking, the foundation of computing rests upon 0s and 1s—no matter how complex a system, everything ultimately reduces to binary digits. Similarly, cybersecurity fundamentally revolves around attack and defense, while network architecture consists of endpoints and connections. Regardless of complexity, all networks can be distilled to these basic elements. Consequently, the Internet, mobile Internet, and IoT are essentially indistinguishable at their core.

Why IoT Security Demands Attention

IoT has garnered widespread attention because it intimately connects with every individual. We inhabit not only a physical world but also a cyberspace realm. From an attack perspective, the IoT era introduces threats directly targeting human beings—pacemakers can be compromised, smart refrigerators may be attacked, and industrial facilities face similar vulnerabilities. As mobile Internet entered its advanced stages, a simplified application platform emerged: cloud-pipe-endpoint. In mobile Internet, the endpoint was the smartphone; in IoT, endpoints become diverse objects. As networks grow increasingly complex, individuals become fully integrated, seamlessly blending the physical and digital worlds.

Three Perspectives on IoT Security

Network Perspective

From a network standpoint, the Internet represents fixed network connections—including computer networks and industrial networks—whereas mobile Internet involves mobile network connections, and IoT embodies ubiquitous connectivity. The most significant transformation is that IoT development has eliminated the traditional distinction between internal and external networks, making network segregation exceedingly difficult.

Cloud Perspective

From a cloud perspective, the primary distinction between general cloud computing and IoT cloud lies in control functionality. In general cloud environments, connected machines run programs; with IoT development, control capabilities must be added. For instance, in networked elevator experiments—elevators being traditional equipment—the cloud platform can initiate and stop their

operation. Consequently, one of the gravest threats in IoT security is remote manipulation via cloud platforms, making endpoint protection particularly challenging.

On cloud platforms, beyond business platform security and cloud architecture security, data security assumes paramount importance. While the traditional Internet primarily contains user information, industrial IoT encompasses critical industrial data, rendering data protection even more crucial.

Endpoint Perspective

With IoT development, an increasing number of devices are connecting. From the endpoint perspective, traditional equipment must first undergo fundamental cybersecurity testing to establish a security baseline. Subsequently, security monitoring should be implemented on cloud platforms. Overall, security must return to the fundamentals of network composition—understanding the network's structure and characteristics.

Fragmentation Challenges

First, from the endpoint perspective, hardware and software in the IoT era exhibit fragmented characteristics. Both industrial IoT and industrial control systems are broad concepts; different industries such as tobacco, petrochemicals, and power grids maintain their own standards and platforms. From a security standpoint, this fragmentation presents a significant challenge.

Interconnected Security Implications

IoT security and communication network security are intertwined and mutually influential. Threats are not unidirectional—attacks can originate from the Internet targeting IoT devices, but conversely, IoT devices can also be leveraged to attack communication networks. This bidirectional vulnerability represents a second critical concern.

Note: Figure translations are in progress. See original paper for figures.