The Problem with (Modern) Networks and the Logical Way Forward

CHRISTOPHER AUTRY, CEO, Iothic, The University of Oxford

INTRODUCTION

This document is a fact based approach supported with references where available, seeking to answer three questions:

1) What is the problem in current modern networks?
2) How are the problems being solved now?
3) Why is dOISP the best way to solve the problem?

1. THE PROBLEM IN CURRENT [MODERN] NETWORKS

Networks can be defined on a spectrum. At one end of the spectrum, there are fully static networks with a single owner. At the other end, there are multiple highly dynamic networks with ever-changing topologies, with multiple owners, that need to interact with one another at unspecified intervals. Within networks, an asset is defined as anything that connects with one or more assets of the same network system. Assets range from highly sophisticated technologically advanced AI enabled gateway servers, to programmable logic controllers (PLCs), to a range of "dumb" (OT) Operating Technologies[1], Industrial Control Systems (ICS), and Supervisory Control and Data Acquisition (SCADA), that encompass a broad range of programmable systems and devices designed to interact with the physical environment.

All networks regardless of where they fall on the static-dynamic spectrum, have three technological obstacles that have prevented the fourth industrial revolution 4IR[2], AI and IoT from advancing rapidly.

1) Disparate operating systems, competing communication protocols, and layers of functional software from multiple vendors are used to control and run, monitor these networks; The expense in deploying and managing these systems is significant[3].
2) Current standard cybersecurity solutions are difficult or impossible to deploy widely[4] particular at the "edges" of these systems[5].
3) There is a severe lack of secure interoperability between assets in the network which acutely limits both functionality, analysis and operation[6]. Networks are architected in a highly centralised client-server model or variations thereof.

In short, there is a large upfront and ongoing cost to secure and operate networks and even then, security solutions are not fully comprehensive, and are a patchwork of various solutions, and as a result, are open to a wide range of attacks[7]. Further, the lack of realtime interoperability between assets in a network even between assets from the same vendor, severely limits network analysis, operation and ultimately restricts overall capability.

The lack of a truly viable solution required to securely bring OT into IT, the inability to comprehensively secure complex dynamic networks from 'edge' to centre, the glaring lack of interoperability between assets in the network in network infrastructures already in place, have lead both the US and EU[8,9,10] to mandate these issues be addressed.

There is no easy solution to address these issues and most people know this, it is the elephant in the room[11]. It is why most cybersecurity "solutions" rely on severely outdated technologies. In place of actual solutions, (AI) detection and mitigation security strategies are fast becoming the norm[12].

2. HOW ARE THE PROBLEMS BEING SOLVED NOW?

Current solutions to the network issues as described above can be classified into three categories:

1. Piecemeal, multi-vendor, often complex, costly software/hardware solutions
2. Network isolation, one-way connectivity, air gapping

[1] https://csrc.nist.gov/Projects/operational-technology-security

[2] https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-are-industry-4-0-the-fourth-industrial-revolution-and-4ir

[3] https://www.smbceo.com/2019/09/04/what-are-the-costs-of-big-data/

[4] https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-137a

[5] https://tinyurl.com/2krb7ku4

[6] Albouq, Sami & Abi Sen, & Almashf, Nabil & Yamin, Mohammad & Alshanqiti, Abdullah & Bahbouh, Nour. (2022). A Survey of Interoperability Challenges and Solutions for Dealing With Them in IoT Environment. IEEE Access. 10. 1-1. 10.1109/ACCESS.2022.3162219.

[7] https://www.cobalt.io/blog/biggest-cybersecurity-attacks-in-history

[8] https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[9] https://www.europarl.europa.eu/doceo/document/A-9-2021-0313_EN.html

[10] https://www.defense.gov/News/Releases/Release/Article/3225919/department-of-defense-releases-zero-trust-strategy-and-roadmap/

[11]https://www.praetorian.com/reports/why-security-programs-fail/

[12] https://www2.deloitte.com/us/en/insights/focus/tech-trends/2022/future-of-cybersecurity-and-ai.html

3. Some combination of 1) and 2); Default security settings; Nothing

Vendor software solutions in general focus on solving for a specific technical network issue. For example, companies like Fortinet[13] claim they integrate OT into IT as one of their service offerings, Onclave[14] claim they can secure the edges of IoT systems, Dragos[15] have a sophisticated detection and reporting platform, AWS Greengrass[16] is an attempt to secure the edges of complex IoT networks. All of these solutions have the commonality of using centralised, software-layer based approaches and often rely on outdated static-certificate based technologies like PKI (Public Key Infrastructure)[17]. In other words, old insufficient technology, new packaging. Therefore, modern networks require multiple software solutions, including staff training, ongoing maintenance and support over the lifespan of the network. Deployment often can entails substantial operational interruption.

In the absence of truly viable solutions, many, particularly in the critical security spaces, players in critical national infrastructure (CNI) for example, have opted for isolating or segmenting parts of their networks, including air gapping[18]. Other solutions might include the use of data diodes[19] for the flow of one-way only data connectivity.

Lastly, the problem may be solved be some combination of piecemeal software, network isolation and using default security setting like TLS (Transport Layer Security), or other "built-in" security technologies.

Given that there are existing competitors trying to solve this problem, our solution (dOISP) needs to be easily incorporated anywhere existing technologies are already in place, or to sell it to companies for whom their existing technologies do not adequately solve the problem. We have a large number of companies telling us that there is a problem to solve, and that dOISP solves that problem.

3. WHY IS dOISP THE BEST WAY TO SOLVE THE PROBLEM?

Iothic has taken a novel approach to solving these key networking challenges, including deploying comprehensive post-quantum resistant security from 'edge' to centre, bringing OT into IT easily, adding full interoperability between network assets, creating fully decentralised network capabilities (no kingdom to get the keys to), and allows for secure communication between disparate networks that themselves can evolve over time. dOISP runs in parallel to other all technologies including other existing security technologies and is universally deployable on existing infrastructure on existing network architectures.

Three key factors differentiate dOISP from other solutions in addition to solving the aforementioned technical challenges.

1) dOISP is not a software layer

All current software solutions attempt to solve technological issues with a layer of functionality superimposed on assets that alter the functionality of the assets themselves. dOISP uses the existing TCP/IP model of network communication and alters how the network itself interacts with the assets. The dOISP code running on the assets directly or on a virtual or actual machine alters the TCP/IP model directly. dOISP works at L3 or network packet layer of the TCP/IP (OSI) model. Further, so long as the assets can connect with each other no central internet connectivity is required to run dOISP. Most traditional software requires central internet connectivity to function.

2) No human management required

One deployed there is no management of dOISP as it become intrinsic to the network on which it is deployed. There are no stored databases, no key management, and no trusted third-parties (TTPs) involved. Further, dOISP uses NIST[20] standards and can be easily integrated into existing systems on existing hardware.

3) Deployable in days not months

dOISP has been engineered to be deployed on complex networks including Critical National Infrastructure (CNI), in factories, buildings, and other complex networks (mesh, swarm, etc) in theoretically days, not months, by any corporation or government agency themselves without interrupting current operations. dOISP can be run as code directly network assets, on P-quant relays (hardware) or virtual instances of P-quant relays running locally making deployment easy and straightforward. dOISP has been engineered to be deployed quickly in complex network environments by anyone anywhere.

"This is the technology that everyone has been waiting for"— *Former CIO of the DHS (Department of Homeland Services), USA.*

[13] https://www.fortinet.com/

[14] https://onclavenetworks.com/

[15] https://www.dragos.com/

[16] https://aws.amazon.com/greengrass/

[17] https://www.spiceworks.com/it-security/security-general/guest-article/top-5-public-key-infrastructure-pki-pitfalls-and-how-to-overcome-them/

[18] https://www.armis.com/home-faqs/what-is-air-gap-in-network-security/

[19] https://owlcyberdefense.com/blog/what-is-data-diode-technology-how-does-it-work/

[20] https://www.nist.gov/