The Perfect Storm

Solving critical infrastructure challenges

by evolving today's IP networks

By Tempered Networks

Hardened. Resilient. Simple.™

The Perfect Storm

Today, there is no question that our national infrastructure is under attack.

Earlier this year, Richard H. Ledgett Jr., deputy director of the National Security Agency, concluded that “today, anyone with a computer and a fairly decent level of knowledge and an Internet connection can pose a very serious threat to an individual, a business, a city and a foreign nation" during a keynote address during a dinner at the Joint Service Academy Cyber Security Summit at the U.S. Military Academy in West Point, N.Y.

This keynote came a couple months after the hack against Ukraine’s power grid, which caused a blackout for hundreds of thousands of people. For many, this was an eye-opening event, as it was the first confirmed successful hack against the SCADA networks that controlled the grid. The fallout from this event holds many lessons for power generation plants and distribution centers here in the US, as the rush to connect previously air-gapped systems has opened vulnerabilities across all 16 critical infrastructure sectors identified by DHS. With 209,000 unfilled cyber security jobs in the U.S alone unfilled according to a Peninsula Press analysis of numbers from the Bureau of Labor Statistics, this is not a situation that will be fixed any time soon, which leaves the U.S frightfully exposed.

With the recent leaked NSA Zero Days, where an anonymous group calling itself the Shadow Brokers compromised the NSA and stole previously unknown exploits and zero days, the threat has escalated even more. The hack unleashed some notable vulnerabilities, complete with tips for how to use them, and the security community has already warned they are being used by known hacking groups.

The question then becomes: what does this add up to?

A perfect storm, where the everyday U.S citizen and the U.S economy is merely a targeted attack away from disastrous consequences. Fortunately, Congress is paying attention and has passed legislation, providing funding for initiatives and research for new emerging and unique technologies. For the F-17 budget, we note some general themes:

- Harden existing network defenses
- Obscure vital services and data
- Reduce the ability to traverse the network should an intrusion occur
- Insider threat mitigation

However, legislation is more about directives, and not actual implementation of technologies. Congress can certainly push for our critical infrastructure to be more secure, but for the guys in the trenches, they still don’t have the right technologies to help them.

To address the issue, it’s important to take a historical view on what has led us to this moment, with 2 main trends driving the vulnerable environment we find ourselves in.

1. TCP/IP – the backbone of Internet is inherently unsecure
2. Perimeter-based security strategy is still a common, yet vulnerable approach

TCP/IP is not a methodology for security

Designed in the late 1960's (almost 50 years ago!), the original intent of the Internet was strictly for connectivity. The TCP/IP protocol, the basis for today's Internet, lack even the most basic mechanisms for security, such as authentication or encryption. As connectivity continue to increase, the lack of built-in security has become more and more problematic.

Internet Engineering Task Force (IEFT) further states the historical implementation of TCP/IP along with the inherent flaws in the design:

"While we have seen advancements in Internet technology since it early inception, the Internet's building blocks are basically the same core protocols adopted by the ARPANET, more than two decades ago. During the last twenty years, many vulnerabilities have been identified in the TCP/IP stacks across a number of systems."

Encryption is easy; trust is hard

Trust is the fundamental problem in IP communications across connected networks. It turns out that adding encryption to communications is the easy part. Adding trust, on the other hand, remains an intractable problem. Why? Two reasons. First, access to apps and IPv4 communications are both tied to the same piece of information: the IP address. We do not have a cryptographic identity to use for communications, which is why we have to login to every "secure" application like banks, email, and medical records. Second, there has been no good way to manage trust relationships.

You might argue that the communications are still encrypted. But with whom are they encrypted? Does it matter if you encrypt your password over the network if goes directly to an adversary? Attribution on the Internet is nearly impossible. The browser-based trust model of hundreds of trusted CA certificates does little to assert trust and assurance for the underlying communications.

The perimeter-based strategy is outdated

The perimeter-based security model has often been compared to a medieval castle: a high wall surrounded by a moat, with a single point of entry and exit, all designed to keep out unwanted intruders. Everything on the 'inside' is trusted, and everything outside is dangerous. However, the key assumption of this strategy is no longer true in today's networked environment with users on the inside of the network, outside the network, cloud resources, mobile resources, etc., – essentially we have an erosion of control from the various places where data lives and where they are being accessed.

This new borderless environment is a focus of Google's internal initiative *BeyondCorp*, in which they are re-defining what the internal and external network is, with the idea that:

"One should assume that an internal network is as fraught with danger as the public Internet and build enterprise applications based upon this assumption."

The perimeter-based approach is in many ways a reactive approach, much like the game 'whack-a-mole', where the focus is on what needs to be blocked as they appear. With the shift to a borderless environment, a proactive approach is needed where the focus is on who can be

trusted to access the network, not what needs to be blocked. Simply put, security must be moved from the perimeter to the device.

A new way forward with Host Identity Protocol – an evolution of traditional IP networks

Host Identity Protocol (HIP) is a standard-track network security protocol that provides built-in encryption and authentication, and was approved by the IETF in 2015. That event crowned over 15 years of HIP development, testing and deployment in co-ordination with several larger companies (such as Ericsson, Nokia, Verizon, TeliaSonera) and standard bodies (Trusted Computing Group, IEEE 802).

Recognized by the IETF community as the next possible big change in IP architecture, HIP has been in use for over 10 years as a cost-efficient and scalable solution to address growing threat environments within the defense and aerospace where nation-state cyber attacks occur on a regular basis industry.

Moving from reactive to proactive security

The use of HIP raises the bar on network security with protection against most of today's known threats. In fact, one of the Boeing architects and security experts in the OpenGroup, Richard Paine, wrote a book about HIP deployments: "Beyond HIP: The End to Hacking as We Know It," in which he described how the fundamental building blocks of today's networks needs to evolve to meet the required security needed today.

Figure 1: Cloaking to stop step 1 of Cyber Kill Chain

Along with introducing trusted identities for devices and networks, HIP also introduces the concept of 'cloaking'. Because endpoints have no TCP/IP footprint, they are invisible from the underlying network. This effectively enables HIP to stop step 1 of the Cyber Kill Chain completely, by cloaking endpoints. End result: Attackers cannot attack what they cannot see! And, a reduced attack surface by an order of magnitude.

Conclusion

Today's practices for security and networking are simply unsustainable and requires a new approach that ensure people and networks can scale and keep up with demands. Federal agencies require a cost-effective way to protect any device or system, including legacy and long-lived systems such as HVAC, fuel pumps, and generators. In addition, the ability to safeguard transient and mobile resources, such as warships, planes, vehicles, robots, laptops, in a rapid and seamless fashion is vital.

The Host Identity Protocol fixes this. Going back to the legislative trends we identified earlier, HIP not only hardens existing network defenses and obscure vital services and data, but also reduces an attacker's ability to traverse the network should an intrusion occur.

Agencies and organizations can now deploy a powerful and intelligent approach, where security is “baked in” from the start for a proactive, practical and sustainable implementation.