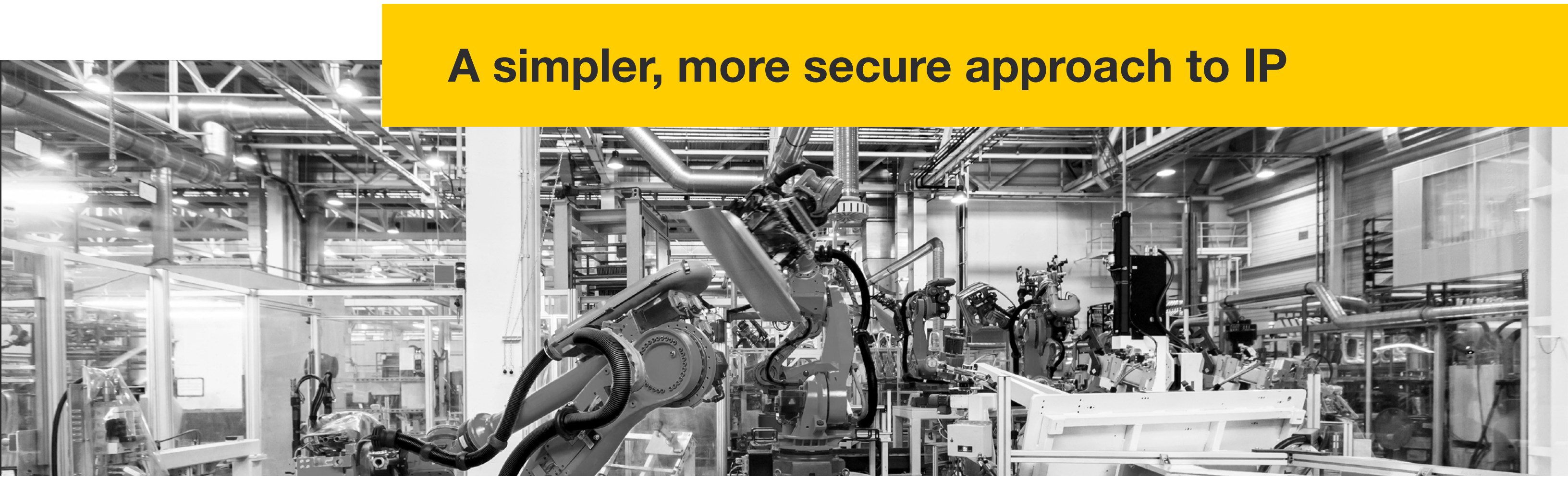
whitepaper

Tempered

Primer on Host Identity Protocol

A simpler, more secure approach to IP



Creating a new standard for network security

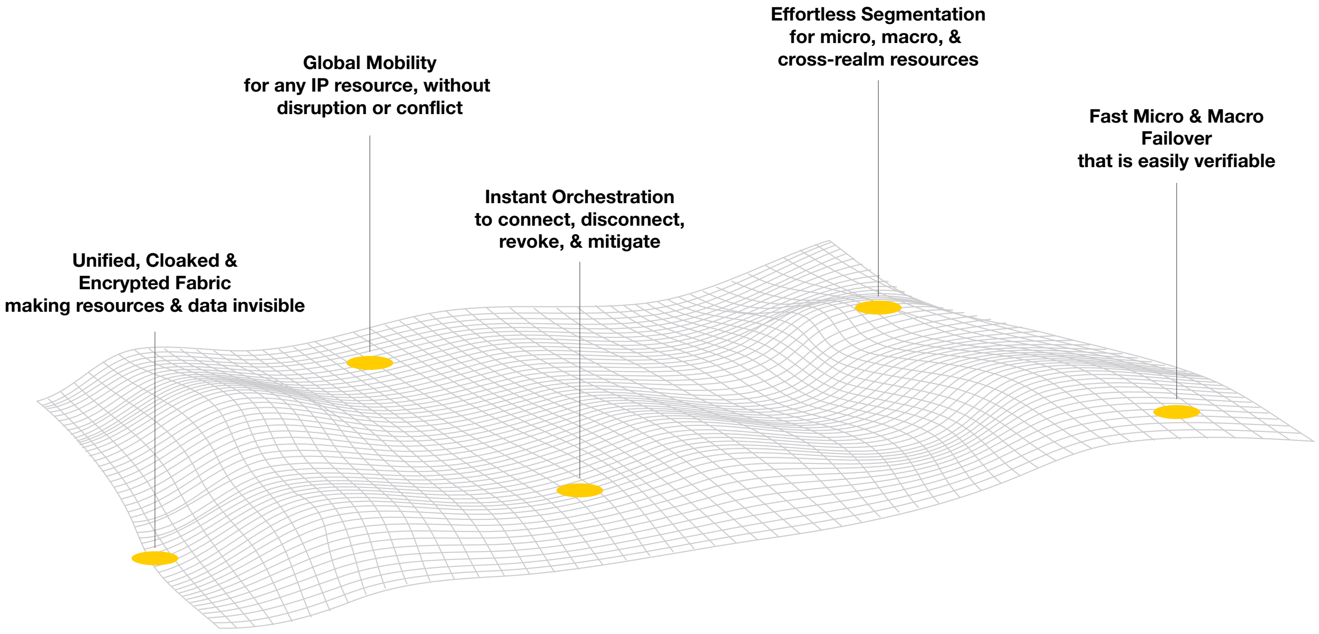
Host Identity Protocol (HIP) is a standard-track network security protocol, approved by the leading standards organization in the Internet, the Internet Engineering Task Force, in 2015. That event crowned over 15 years of HIP development, testing and deployment in coordination with several large companies (such as Boeing, Ericsson, Nokia, Verizon, TeliaSonera) and standard bodies (Trusted Computing Group, IEEE 802).

Recognized by the Internet Engineering Task Force (IETF) community as a fundamental improvement in secure IP architecture, HIP was first deployed within the defense and aerospace industry as a cost-efficient and scalable solution to address growing threat environments and the complexity of security policy management and implementations. The protocol has been in use for over 10 years in mission-critical environments of all scale and complexity, including where downtime exceeds $1 million per hour, and nation-state cyber attacks occur on a regular basis. Tempered Networks now offers the leading, proven HIP implementation by layering on simplified management, various end-point protection form factors and scalability for a variety of use cases and network environments.

Secure by design

HIP fundamentally provides a secure overlay fabric over existing network infrastructures and introduces a new cryptographic host identifier separate from the usual IP address. The fact that IP addresses include both route information and host IDs has complicated security policy management for decades. The new HIP ID allows for simplified, centralized management of end-point access control policies. The creation of a secure overlay network and the encrypted identifier renders hosts completely invisible to unauthorized users and potential attacks. Rather than probing an IP device for vulnerabilities, attackers will never know of the existence of the host on the network. To them, the device is completely cloaked.

HIP provides an alternative key exchange protocol for creating secure encrypted tunnels, enabling transparent and legacy-compatible security for all TCP/IP applications without modification. HIP introduces the concept of an identifier-locator split (separating the role of IP addresses as host identity and topological location in the Internet), where hosts are identified using strong cryptographic identities in the form of 2048-bit RSA public keys.



HIP secure mesh fabrics provide several advantages over traditional security infrastructure like firewalls and VLANs

Internet location is determined by the IPv4 or IPv6 address assigned to the host. However, with the unique cryptographic identity provided by HIP, the device can change locations and not suffer a change or require a policy update. Hosts can change their physical location, but retain their strong cryptographic identity. HIP remains compatible with IPv4 and IPv6 applications, utilizing a customized IPsec tunnel mode for confidentiality, authentication, and integrity of the network applications.

Since hosts and network devices can use the cryptographic ID for identification rather than dynamic IP addresses, features and use cases such as host and network mobility, single sign-on, and multihoming are easily implemented.

Furthermore, in contrast to TCP, HIP was designed from the start to be robust against the Denial-of-Service (DoS) and Man-in-the-Middle (MiTM) attacks plaguing the internet by deploying a clever cryptographic puzzle mechanism (based on Diffie-Hellman key exchange) and stateless server approach in the authentication phase.

A radically different approach

The internet today remains a playground for hackers, and government-backed groups engaging in cyber warfare. Near complete lack of accountability and trust coupled with the ease of spoofing IP and MAC addresses, as well as open access to network perimeters and increasingly common mobile and remote workforces have significantly increased the available threat surface.

Today, most enterprises attempt to stop this using traditional tools such as firewalls and intrusion detection systems (IDS) – relying on traffic analysis and easily spoofed identifiers such as TCP ports, IP or MAC addresses – making for a fragile foundation that is tedious and costly to manage.

Tempered takes a radically different approach, addressing one of the root causes of present internet attacks – the lack of robust host identities and open availability of exploitable systems. The cryptographic host identity becomes the primary operational unit in host access control and network traffic filtering. Recognizing the difficulty of patching legacy Internet devices, such as printers or industrial equipment, Tempered introduces gatekeepers known as Airwall Gateways in front of any IP-connected device, which require no changes to the underlying network.

In contrast to traditional firewalls with static traffic filtering rules, or IPsec gateways that encapsulate all traffic through tunnels, Airwall Gateways use a stronger approach. They establish secure tunnels over public internet to deliver vulnerable user traffic safely, and they employ white-listing of hosts that govern use of these tunnels between cryptographic identities, protecting against unauthenticated malicious traffic.

By partitioning and isolating the network into trusted micro-segments, Tempered completely cloaks vulnerable infrastructure from outside users, without the difficulty of having to individually update each connected device. Devices that are cloaked are undetectable from the underlying network. Combined with a powerful and scalable management interface, this provides an amazingly easy and highly efficient protection of internet communication. Though multiple companies have attempted to benefit from using HIP, none have been as successful in productizing the various components into an extremely reliable and easy to deploy and manage solution as Tempered Networks.

Raising the bar on cybersecurity

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." Providing strong cryptographic host identities enables HIPswitches to robustly filter out all unauthorized traffic, eliminating the danger of DoS or impersonation attacks. Combined with military-grade AES-256 encryption and SHA-256 authentication of data packets, the bridged HIP traffic presents an insurmountable obstacle even for the most capable attacker on the internet.

Compared to VPN solutions relying on layer-4 security, namely SSL, the use of HIP enables network security deep in the network protocol stack, alleviating known application-level attacks. As such, SSL operates on top of the TCP transport protocol, which itself is highly insecure and vulnerable to attacks such as SYN flooding or reset attacks. A malicious user can interrupt a secure session employing TCP-level weaknesses. Furthermore, relying on public authorities for approving SSL level certificates was shown to be unreliable with compromised root CAs. Exploits in the SSL/TLS protocol enabled attackers to not only compromise the confidentiality and integrity of communication, but also leverage DDoS attacks.

How Tempered uses HIP

Even though HIP provides the highest level of network security, it initially introduced some deployment overhead. One of the key challenges had been the difficulty of configuring the rules in the HIP controller or policy management devices, which involved manual editing of XML files and the synchronization among multiple devices.

Tempered has solved this problem using an easy-to-use centralized graphical management console, which enables adding or removing user devices from a trusted list with a few clicks. Indeed, usability has always been an Achilles' heel of any proposed security solution and Tempered has addressed this by focusing on providing an all-in-one platform, with easy centralized management.

The Tempered solution has been successfully deployed in mission-critical industrial domains such as aircraft manufacturing, utilities sector, oil and gas, and electricity generation, as well as enterprise domains such as isolating ticketing machines running out-of-support systems. The unique distinction of the Tempered platform is that it is purpose-built to provide secure connectivity and new use cases are realized everyday by its customers.
In the future, this secure architecture could be applied to new domains such as:

- Energy SmartGrids, where customers generate and share electricity
- Connecting datacenters and providing centralized control with Software-Defined Networking (SDN)
- Revolution in manufacturing, combining plentiful data from sensors in industrial machinery with cloud-based data mining and learning for increased efficiency

Indeed, security of physical systems and devices has been quoted by leading industry experts as the main obstacle hindering the connectivity of industrial equipment. To that end, Tempered can accomplish a great deal by expanding the domains of its solution to cloaking anny physical end-point or IoT device.

Dr. Andrei Gurtov, Aalto University, Finland

Andrei Gurtov received his M.Sc (2000) and Ph.D. (2004) degrees in Computer Science from the University of Helsinki, Finland. He is presently a Principal Scientist at the Helsinki Institute for Information Technology HIIT, and a senior member of IEEE and ACM.

He is also adjunct professor at Aalto University, University of Helsinki and University of Oulu, and was a Professor at University of Oulu in the area of Wireless Internet in 2010-12. Previously, he worked at TeliaSonera, Ericsson NomadicLab, and University of Helsinki, and was a visiting scholar at the International Computer Science Institute (ICSI), Berkeley in 2003, 2005 and 2013.

Dr. Gurtov is a co-author of over 150 publications including three books, research papers, patents, and five IETF RFCs. He has contributed to HIP standardization at the IETF, where he co-led the HIP Research Group at the Internet Research Task Force (IRTF), co-authoring RFC 6538 summarizing experiences of early HIP experiments and deployments. His book on HIP was placed on IEEE "Best Readings" list in Communications and Information Systems Security (CIS).

Leverage Host Identity Protocol to secure your business.

Schedule a meeting with our experts to learn more.

experts@tempered.io | +1 206.452.5500