Primer on Host Identity Protocol (HIP)

A Game Changer in IP Communications

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).

I E T F

IEEE

acm

History

HIP or Host Identity Protocol 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 co-ordination with several larger companies (such as Ericsson, Nokia, Verizon, TeliaSonera) and standard bodies (Trusted Computing Group, IEEE 802).

Recognized by the Internet Engineering Task Force (IETF) community as the next possible big change in IP architecture, HIP was first deployed within the defense and aerospace industry as a cost-efficient and scalable solution to address growing threat environments. The protocol has been in use for over 10 years in environments where downtime exceeds $1 million per hour, and nation-state cyber attacks occur on a regular basis.

Technology

HIP provides an alternative key exchange capability for the IPsec protocol, enabling transparent and legacy-compatible security for all TCP/IP applications. 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.

The locator is an IPv4 or IPv6 address, but the identity is not tied to the identity of the host. Hosts can change their IP 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.

HIP provides strong security properties thanks to its time-tested design relying on formal verification of its state machine describing each step of protocol operation. Since hosts and network devices can use the unspoofable cryptographic ID for identification rather than ephemeral IP addresses, functionality 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 present Internet by deploying a clever cryptographic puzzle mechanism and stateless server approach in the key establishment and authentication phase.

How Tempered Networks uses HIP

The Internet today remains a playground for various hackers, ranging from amateur hactivists to government-backed professional 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 availability of unpatched consumer PCs have significantly increased the available threat surface.

A lack of isolated connectivity (known as cloaking) and strong authentication permit a constant barrage of break-ins of corporate and public infrastructures, resulting in compromised private user data and trade secrets. Yet, today most enterprises attempt to stop this using traditional tools such as IDS and firewalls – relying on traffic analysis of easily spoofed identifiers such as TCP ports, IP or MAC addresses – making for a fragile foundation. This is analogous to building a house on a quicksand as nothing prevents hackers from finding yet another exploit in the traditional TCP/IP stack.

Tempered Networks 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 Networks introduces gatekeepers known as HIPswitches 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, HIPSwitches use a stronger approach. They establish secure tunnels over public Internet networks 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 Networks 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 as Tempered Networks products.

The Impact on Cyber 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." Providing strong cryptographic host identities enables HIPswitches to robustly filter out all unauthorized traffic, eliminating the danger of denial or impersonation attacks. Combined with military-grade AES-256 encryption and SHA-256 authentication of data packets, the bridged HIP traffic presents a tough nut to crack 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 DoS 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.

A New Cyber Security Environment

Even though using HIP provides the highest level of network security, in the past it faced deployment difficulties. One of the key problems had been the difficulty of configuring the rules in the HIP middlebox devices, which involved manual editing of XML files and their synchronization among multiple devices.

Tempered Networks has solved this problem using an easy-to-use centralized graphical management interface, 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 Networks has addressed this by focusing on providing an all-in-one platform, with easy centralized management.

The Tempered Networks 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 unsupported Windows XP. The unique distinction of Tempered's 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 home owners 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 cyber-physical systems has been quoted by leading industry experts as the main obstacle hindering the connectivity of industrial equipment. To that end, Tempered Networks can accomplish a great deal by expanding the domains of its operation.

From a researcher's point of view, it will be interesting to follow their adoption for securing a set of lightweight sensors for Internet-of-Things, as well as studying bridge scalability and overhead in large deployments, possibly calling for hierarchical approaches to bridge management.