Cloaking and network micro-segmentation can virtually eliminate TCP-IP's inherent security weaknesses, while dramatically reducing complexity creep.

Come and join us for lunch to hear **Jeff Hussey, CEO, Tempered Networks Inc** talk about how using HIP (Host Identity Protocol) and network micro-segmentation to cloak mission-critical infrastructure and assets from attack can not only eliminate IP address vulnerabilities but dramatically reduce complexity while also reducing attackable surface area in your networks.

Biography of CEO

Jeff Hussey, Co-founder, President & CEO, Tempered Networks Inc.: Jeff Hussey has been the President and CEO of Tempered Networks since August 2014. Hussey, the founder of F5 Networks, is an accomplished entrepreneur with a proven track record in the networking and security markets. He maintains several board positions across a variety of technology, non-profit and philanthropic organizations and currently is the chairman of the board for Carena and chairman and co-owner of Ecofiltro and PuraVidaCreateGood. Hussey also serves on the board for Webaroo and the Seattle Symphony. He was the chairman of the board for Lockdown Networks, which was sold to McAfee in 2008. Hussey received a BA in Finance from SPU and an MBA from the University of Washington.

Who is Tempered Networks?

Tempered Networks is a Seattle-based, enterprise cyber security firm that delivers "cloaking" to protect critical assets and infrastructure from attack, while using a unique, automated orchestration tool to dramatically simplify configuration and deployment. As global organizations continue to automate, digitize and add devices/entities to networks – through normal or inorganic growth; from embracing IOT; or via broader integration of IP-enabled devices – the challenge to manage, configure and secure all of these expands exponentially and has already exceeded human capabilities to cope. This creates major security vulnerabilities and huge network/device management challenges that compound over time.

What do they do?

Tempered Networks advocate the discipline of micro-segmentation using HIP-enabled switches* that cloak critical assets and infrastructure under secure overlay networks, while sitting on larger common networks (e.g. IPVPNs, V-LANs, private WANs). The outcome of this removes these assets/infrastructure from unnecessary interaction with the larger Network and tightly regulates who or which device has access via strict white-list control. All of this is automatically orchestrated with a central administration console that does not require IT enterprise to fully utilize (i.e. Business Unit owners can own and run their security policy). Note: * HIP is the acronym for Host Identity Protocol – a military-grade encryption that uses cryptographic identities instead of hackable IP addresses and AES 256 encryption, with origins in Boeing and the US military.

Secure TCP-IP. Reduce complexity. Lower cost.

Haven't heard of Tempered Networks? Here's what thought-leaders are saying about them…

says Tempered Networks is a "2015 Security Infrastructure Innovator"

says Tempered Networks is the "2014 North American Perimeter Network Security Entrepreneurial Company of the Year"

"provides private overlay networks and a "defence in depth" approach... protects the existing investment a company has made in its security ...without affecting the underlying network infrastructure, configuration and management in any way."

IoT expert, Zeus Kerravala applauds [Tempered's] new technology and its very different approach.

What are the gains for enterprise and industrial customers?

1) TCP-IP is no longer a security vulnerability: by replacing IP addresses with cryptographic identities the hackability of TCP-IP is gone;
2) Human error is all but eliminated: automated orchestration of overlay networks removes the risk of human error (typical of firewall management);
3) Network complexity is dramatically reduced: by micro-segmenting assets/devices into logical overlay networks, administrators are managing groups of devices, not each individual device;
4) Tighter control of device/assets access is realized: white-listing of who/what have access to assets and devices more tightly defines security and reduces attackable surface area;
5) Telecom costs can be significantly reduced: eliminate costly MPLS and/or leased circuit connections to remote offices/sites and replace these with encrypted HIP tunnels over broadband or 3G/4G mobile; and
6) An enterprise's most precious assets are safe because…***you can't hack, what you can't see.***