SSH Communications Security Rolls Out Free Discovery Tool to Identify Risks in Secure Shell Environments

SSH Risk Assessment Tool Enables Auditors and Security Teams to Quickly Collect and Report on SSH-Related Access Compliance Issues

LONDON – April 23, 2013 – SSH Communications Security, known the world over as the inventor of the ubiquitous Secure Shell and SFTP protocols, today announced the launch of SSH Risk Assessor (SRA), a free tool that provides users with a clear report on risk and compliance exposures in SSH environments.

SSH Risk Assessor Key Facts:

- **Access Compliance**: Identifies organization-specific compliance status with relevant standards
- **Identity and Access Governance**: Assesses actions needed to achieve compliance
- **SSH Risk Assessment**: Industry-first key location and risk-assessment technology available for free
- **SSH Key Discovery**: Provides broad problem-scope capabilities to provide an understanding of the current state of the Secure Shell environment

The unmanaged proliferation of SSH user keys has emerged a major cyber security risk for enterprises and government agencies of all types and sizes. Lack of proper key management – including centralized creation, rotation and removal – leaves organizations vulnerable to attack and in violation of current and emerging compliance mandates including SOX, PCI, NIST & FISMA.

SRA enables internal and external audit and security teams to quickly collect SSH key information across the environment and provides an assessment of risk exposure. The tool report highlights known vulnerabilities in the environment, basic statistics on SSH keys deployed and specific violations of best current practices. The SRA tool gives security auditors and administrators valuable decision support with respect to identity and access governance in SSH environments.

“Companies are being flagged for compliance violations under general guidelines relating to SSH access control,” said Tatu Ylönen, CEO and founder of SSH Communications Security. “SRA provides an easy way for enterprises and government agencies to determine if there are risk and compliance issues with respect to who has access to what information in their SSH environment. With compliance authorities preparing to create specific requirements regarding access controls in SSH environments, SRA is a critical tool that will help auditors and security teams scope the size of the issue and create awareness with IT executives.”

SRA will be available in May 2013.

Supporting Resources:

- IDC White Paper: A Gaping Hole in Your Identity and Access Management Strategy: Secure Shell Access Controls

About SSH Communications Security

Founded in 1995, SSH Communications Security is the company that invented the SSH protocol - the gold standard protocol for data-in-transit security solutions. Today, over 3,000 customers across the globe - including seven of the Fortune 10 - trust our Information Assurance Platform to secure the path to their information assets. We enable and enhance business for thousands of customers in multiple industries in the private and public sectors around the world. A fast-growing company, SSH Communications Security operates in the Americas, Europe, and APAC regions, with headquarters located in Helsinki, Finland. The company shares (SSH1V) are quoted on the NASDAQ OMX Helsinki.

For more information on SSH Communications Security please visit http://www.ssh.com