NAME

monkeysphere - ssh and TLS authentication framework using OpenPGP Web of Trust

DESCRIPTION

Monkeysphere is a framework to leverage the OpenPGP web of trust for OpenSSH and TLS key-based authentication. OpenPGP keys are tracked via GnuPG, and added to the authorized_keys and known_hosts files used by OpenSSH for connection authentication. Monkeysphere can also be used by a validation agent to validate TLS connections (e.g. https).

IDENTITY CERTIFIERS

Each host that uses the **Monkeysphere** to authenticate its remote users needs some way to determine that those users are who they claim to be. SSH permits key-based authentication, but we want instead to bind authenticators to human-comprehensible user identities. This switch from raw keys to User IDs makes it possible for administrators to see intuitively who has access to an account, and it also enables end users to transition keys (and revoke compromised ones) automatically across all **Monkeysphere**-enabled hosts. The User IDs and certifications that the **Monkeysphere** relies on are found in the OpenPGP Web of Trust.

However, in order to establish this binding, each host must know whose cerifications to trust. Someone who a host trusts to certify User Identities is called an Identity Certifier. A host must have at least one Identity Certifier in order to bind User IDs to keys. Commonly, every ID Certifier would be trusted by the host to fully identify any User ID, but more nuanced approaches are possible as well. For example, a given host could specify a dozen ID certifiers, but assign them all "marginal" trust. Then any given User ID would need to be certified in the OpenPGP Web of Trust by at least three of those certifiers.

It is also possible to limit the scope of trust for a given ID Certifier to a particular domain. That is, a host can be configured to fully (or marginally) trust a particular ID Certifier only when they certify identities within, say, example.org (based on the e-mail address in the User ID).

KEY ACCEPTABILITY

The monkeysphere commands work from a set of user IDs to determine acceptable keys for ssh and TLS authentication. OpenPGP keys are considered acceptable if the following criteria are met:

capability
The key must have the ‘authentication’ (‘a’) usage flag set.

validity
The key itself must be valid, i.e. it must be well-formed, not expired, and not revoked.

certification
The relevant user ID must be signed by a trusted identity certifier.

HOST IDENTIFICATION

The OpenPGP keys for hosts have associated ‘service names‘ (OpenPGP user IDs) that are based on URI specifications for the service. Some examples:

ssh: ssh://host.example.com[:port]

https: https://host.example.com[:port]

AUTHOR

Written by: Jameson Rollins <jrollins@finestructure.net>, Daniel Kahn Gillmor <dkg@fifthhorseman.net>

SEE ALSO

monkeysphere(1), **monkeysphere−host**(8), **monkeysphere−authentication**(8), **openpgp2ssh**(1), **pem2openpgp**(1), **gpg**(1), **https://tools.ietf.org/html/rfc4880,** **ssh**(1),

https://tools.ietf.org/wg/secsh/draft−ietf−secsh−scp−sftp−ssh−uri/