OpenSSH Internals for PowerShell Pros

Anthony E. Nocentino

Anthony E. Nocentino

Consultant and Trainer

Founder and President of Centino Systems

- Specialize in system architecture and performance
- Microsoft MVP - Data Platform - 2017-2018
- Linux Foundation Certified Engineer
- Microsoft Certified Professional

email: aen@centinosystems.com

Twitter: @nocentino

Blog: www.centinosystems.com/blog

Pluralsight Author: www.pluralsight.com

Agenda

- Remote Access Concepts and OpenSSH Architecture
- Authentication Methods
- Configuration

- Covering Installation and Remoting Tomorrow!
  - PowerShell Remoting - Installing and Troubleshooting in a Multiplatform Environment
  - Anthony Nocentino and Richard Siddaway
  - Wednesday - 9:00am – 11:00am

PowerShell + DevOps Global Summit

Remote Access Concepts and OpenSSH Architecture

OpenSSH or: How I learned to stop worrying and love remote access

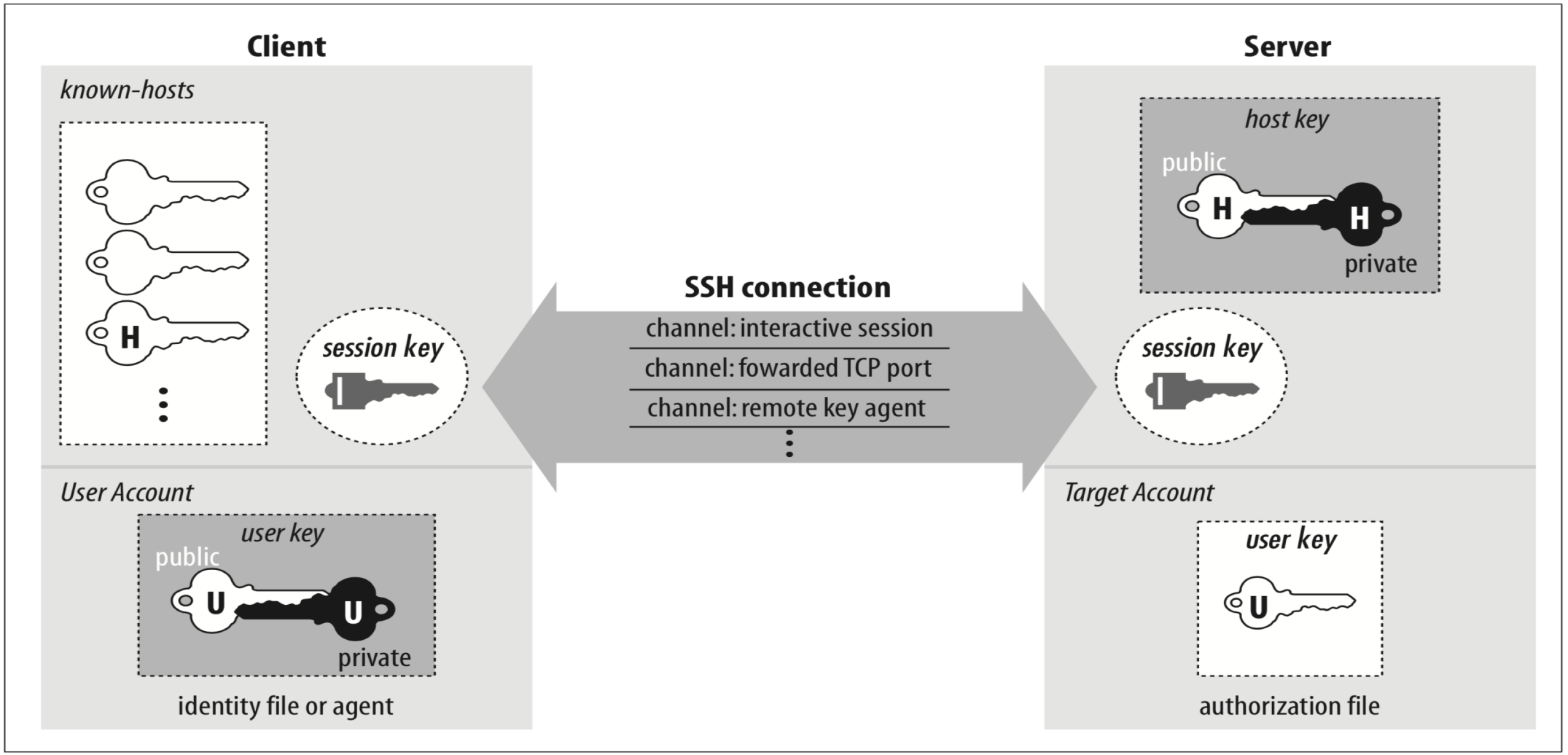
Photo Credit: Public Domain

Remote Access Concepts

- Authentication – verifying identity
- Authorization – granting access
- Integrity – ensuring what’s sent is what’s received

OpenSSH Architecture

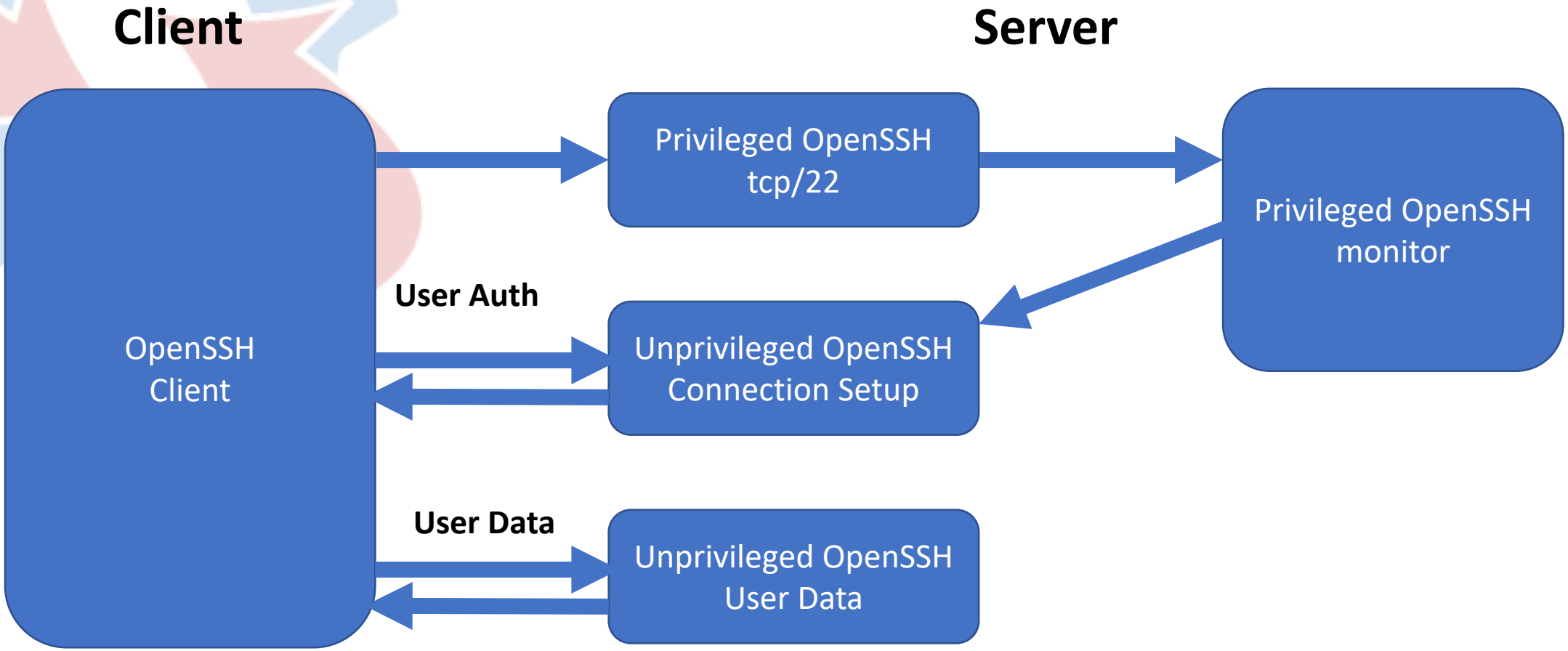
From: SSH, the Secure Shell
The Definitive Guide. O'Reily 2009

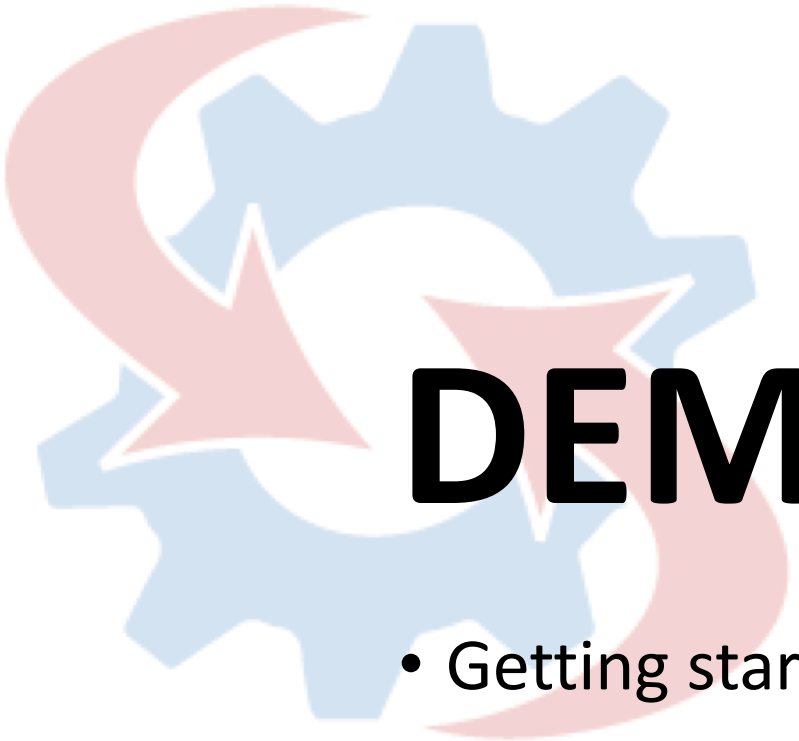


Key OpenSSH Functionality

- Secure client to server to communication
- Remote command execution
- Secure file copy
- Tunneling of arbitrary TCP Services (firewall evasion)
- Ensures remote system is who it says it is
- Message Integrity

OpenSSH Process Model – Privilege Separation





DEMO

- Getting started with OpenSSH
- Host keys
- Privilege separation

Authentication Methods

Getting your users on your servers!

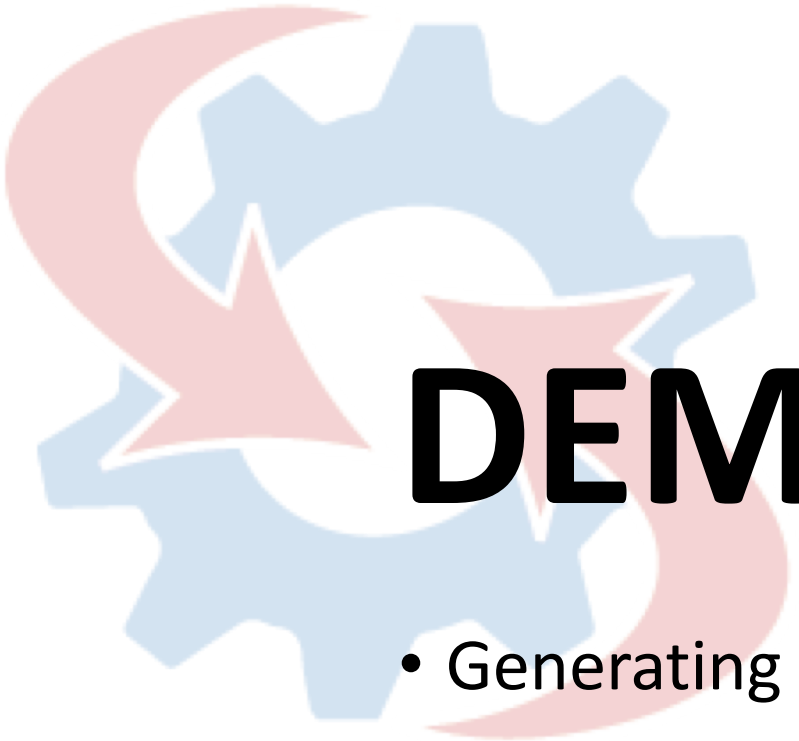
Authentication Methods

- GSSAPI – Kerberos
- Host based - based on which client
- Public key – based on a per user key pair
- Challenge response – two factor
- Password – p4ssword?
- Processed in this order at login

- Come to tomorrow’s session for more on this…

Key Based Authentication

- Generating user keys
  - `ssh-keygen`
  - Public key – `id_rsa.pub or potato.pub`
  - Private key – `id_rsa`
- Getting keys out to servers
  - Copy with `ssh-copy-id`
  - PowerShell - http://www.centinosystems.com/blog/powershell/distributing-ssh-user-keys-via-powershell/
  - DSC
  - Actual PKI - https://code.facebook.com/posts/365787980419535/scalable-and-secure-access-with-ssh/



DEMO

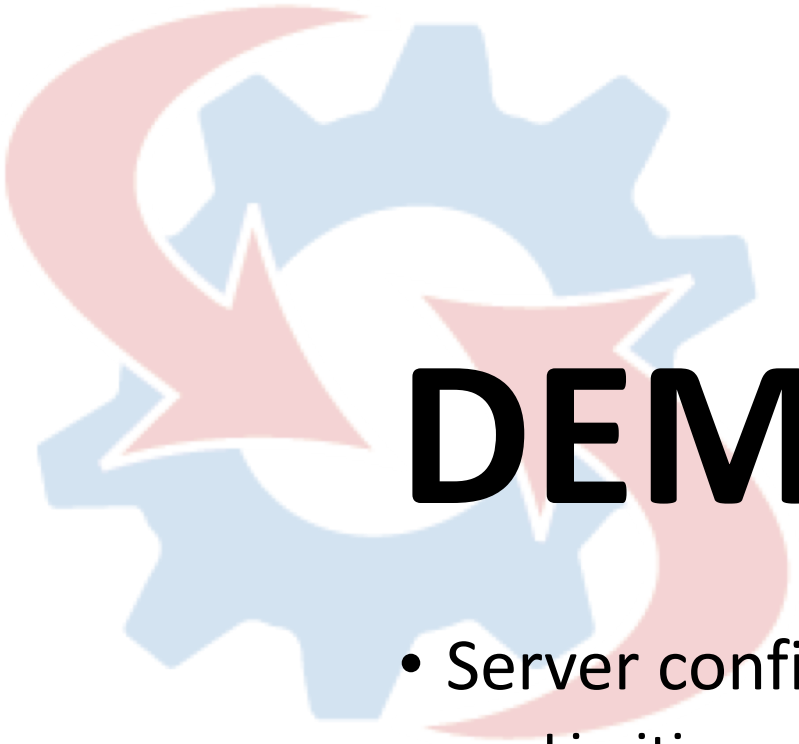
- Generating and distributing a key
- Using a specific key for authentication

OpenSSH Configuration

Your users, your servers

OpenSSH Configuration

- Server
  - `/etc/ssh/sshd_config`
  - `%programdata%/sshd_config`
  - `man sshd_config`
- Client
  - `/etc/ssh/ssh_config`
  - `~/.ssh/config`
  - `%userprofile%/.ssh/config`
  - `man ssh_config`



DEMO

- Server configuration overview
  - Limiting access to a user or group
- Client configuration overview
  - Configure an alias and using a specific key

Agenda

- Remote Access Concepts and OpenSSH Architecture
- Authentication Methods
- Configuration

- Covering Installation and Remoting Tomorrow!
  - PowerShell Remoting - Installing and Troubleshooting in a Multiplatform Environment
  - Anthony Nocentino and Richard Siddaway
  - Wednesday - 9:00am – 11:00am

More data?

- **Come see me in room 403!**
- **Email:** aen@centinosystems.com
- **Twitter:** @nocentino
- **Blog:** www.centinosystems.com/blog

- **Understanding and Using Essential Tools for Enterprise Linux 7**
  - Installation, command execution, bash basics, file system and permissions
- **LFCE: Network and Host Security**
  - OpenSSH
  - Copying files, remote command execution and tunneling TCP

THANK YOU!

Please use the event app or Sched.com to submit a session rating!

PowerShell + DevOps Global Summit