OpenSSH For Windows Pros

Anthony E. Nocentino

aen@centinosystems.com

@nocentino

Centino systems

Anthony E. Nocentino

- Consultant and Trainer
- Founder and President of Centino Systems
  - Specialize in system architecture and performance
  - Microsoft MVP - Data Platform – 2017/2018
  - Friend of Redgate - 2015-2017
  - Linux Foundation Certified Engineer
  - Microsoft Certified Professional
- email: aen@centinosystems.com
- Twitter: @nocentino
- Blog: www.centinosystems.com/blog
- Pluralsight Author: www.pluralsight.com

Centino systems

Agenda

- Remote Access Concepts and OpenSSH Architecture
- Installing OpenSSH on Windows and Linux
- Authentication Methods
- Authenticating Users
- OpenSSH Configuration

Remote Access Concepts and OpenSSH Architecture

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

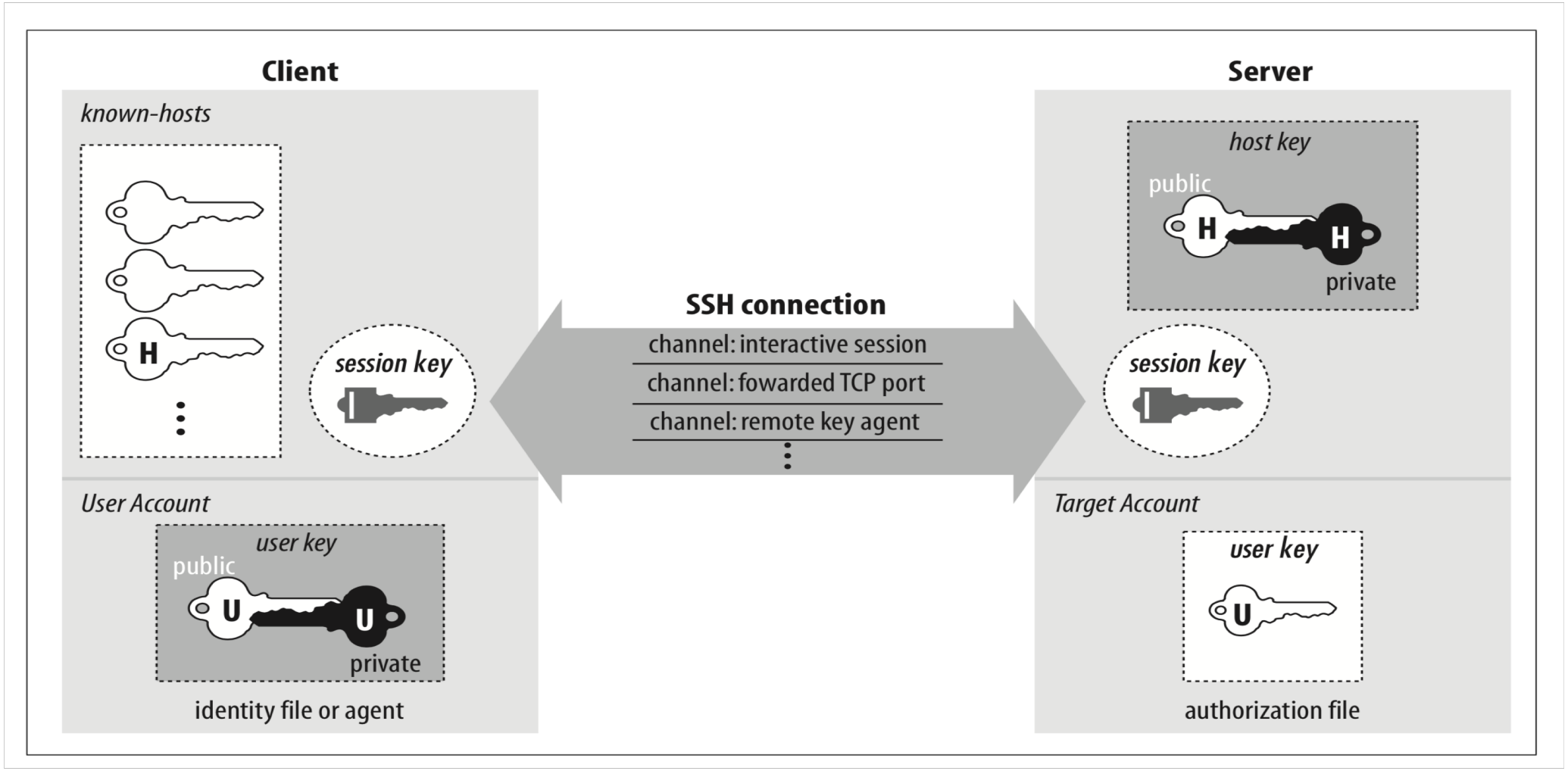
Centino systems

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

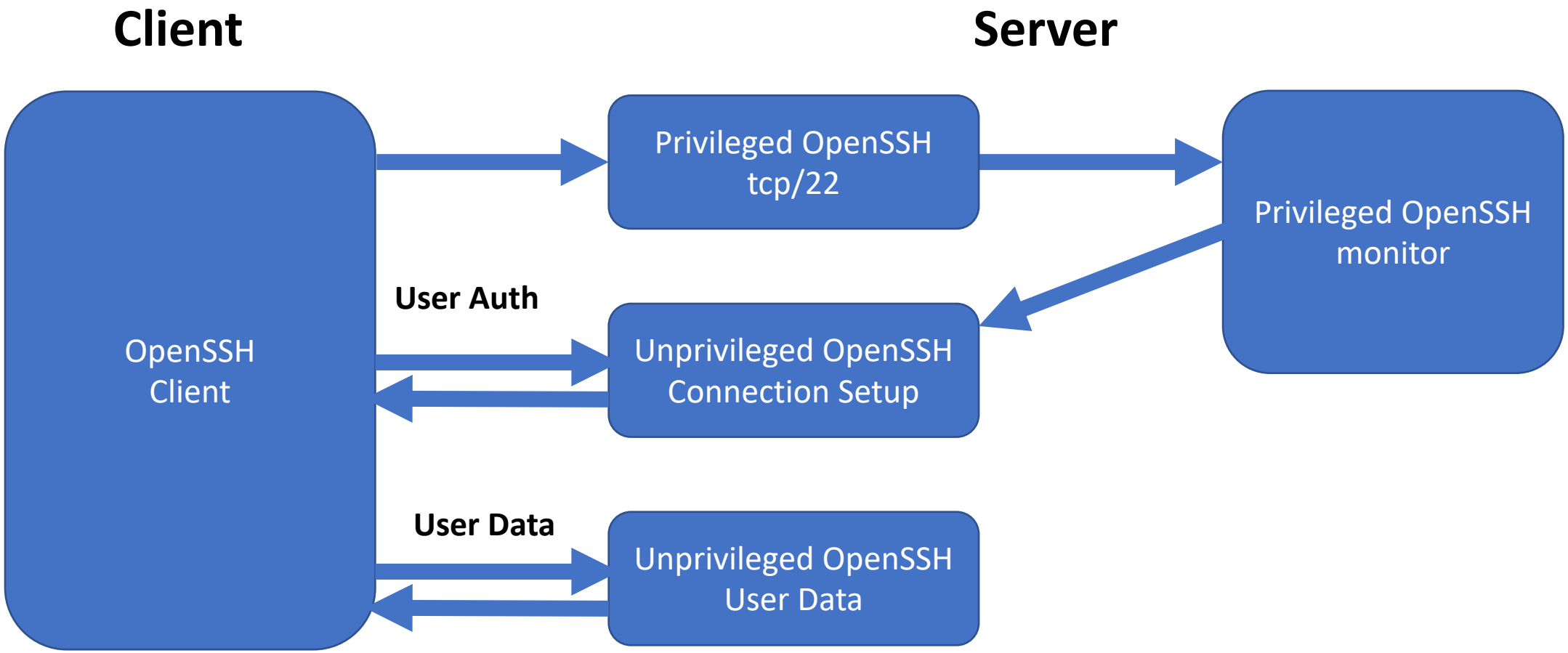


Centino systems

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
- This is a transport layer for PowerShell Core Remoting!

OpenSSH Process Model – Privilege Separation



Centino systems

DEMO

- Getting started with OpenSSH
- Host keys
- Privilege separation
- Remote command execution

- **DC1** – Domain Controller
- **CENTOS-W1** – Linux management workstation
- **CENTOS-S1** – Linux server
- **WINDOWS-S1** – Windows server

Installing OpenSSH on Windows and Linux

Yea, seriously…OpenSSH on Windows!

Installing OpenSSH on Windows

- PowerShell team managed GitHub project
  - https://github.com/PowerShell/Win32-OpenSSH/wiki/Install-Win32-OpenSSH
  - Gonna get your hands dirty
- Windows Feature
  - Fall Creators Update and Windows Server 1709
    - https://blogs.msdn.microsoft.com/powershell/2017/12/15/using-the-openssh-beta-in-windows-10-fall-creators-update-and-windows-server-1709/
    - Add-WindowsCapability -Online -Name OpenSSH.Client~~~~0.0.1.0
    - Add-WindowsCapability -Online -Name OpenSSH.Server~~~~0.0.1.0
- Windows Services for Linux
- Windows Server 2019…

Installing OpenSSH on Linux

- LOL

DEMO

- Installing OpenSSH on Windows Server 2016

- **DC1** – Domain Controller
- **CENTOS-W1** – Linux management workstation
- **CENTOS-S1** – Linux server
- **WINDOWS-S1** – Windows server

Centino systems

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

Authenticating Users

- Local user account databases
  - On Windows
  - On Linux
- Active Directory Authentication
  - Can be used on Windows and Linux
  - LDAP – User lookup
  - Kerberos – User and host authentication
  - System Security Services Daemon (SSSD) – user lookup & brokers authentication

  - **`ssh centos-s1 -l aen@lab.centinosystems.com`**
  - **`ssh aen@lab.centinosystems.com@centos-s1`**

Centino systems

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 Resource
  - Actual PKI

DEMO

- Generating and distributing a key
- Using a specific key for authentication
- Configuring AD authentication on a Linux system

OpenSSH Configuration

Your users, your servers

OpenSSH Configuration

- Server
  - `/etc/ssh/sshd_config`
  - `%programdata%/ssh/sshd_config`

- Client
  - `/etc/ssh/ssh_config`
  - `~/.ssh/config`
  - `%userprofile%/.ssh/config`

Troubleshooting

- **Step 1 – make sure SSH works!**
  - `ssh -v user@servername`
  - Server side debugging on Windows hosts
    - Set `LogLevel DEBUG3` in `sshd_config`
      - https://github.com/PowerShell/Win32-OpenSSH/wiki/Troubleshooting-Steps
    - Currently logs to files. Logs to ETW in 7.6.1.0
      - https://github.com/PowerShell/Win32-OpenSSH/wiki/Logging-Facilities
- Host key mismatch
- Permissions on `authorized_keys` because of `StrictModes`

DEMO

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

More data?

- **Email:** aen@centinosystems.com
- **Twitter:** @nocentino
- **Blog:** www.centinosystems.com/blog

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