

Charting The SSH Multiverse

HD MOORE | APRIL 26, 2025

BSIDES SAN FRANCISCO 2025

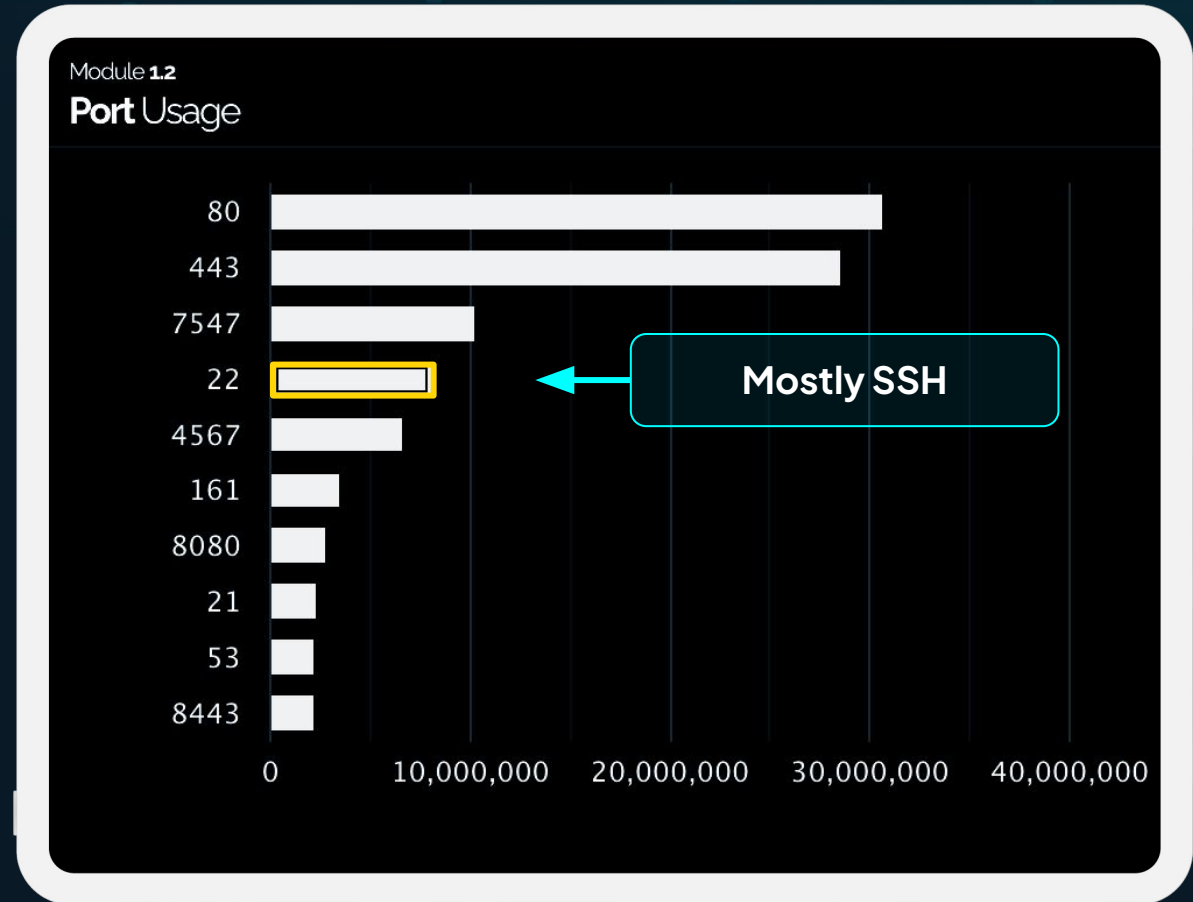
With contributions from Rob King

1

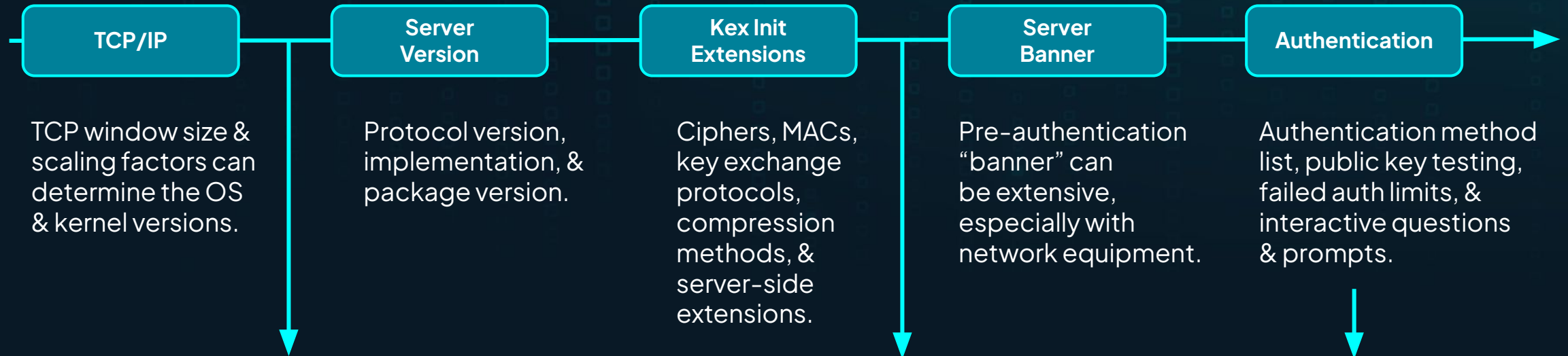


SSH is everywhere

- Second-most common remote admin service behind HTTP
- Enabled by default in clouds
- Part of every major OS
- Embedded & servers
- Even mobile!



SSH pre-authentication information exposure



TCP window size & scaling factors can determine the OS & kernel versions.

Protocol version, implementation, & package version.

Ciphers, MACs, key exchange protocols, compression methods, & server-side extensions.

Pre-authentication "banner" can be extensive, especially with network equipment.

Authentication method list, public key testing, failed auth limits, & interactive questions & prompts.

Platform	Version	SSH banner	v4 tcp.win	v4 MSS	MSS Multiplier	v4 Window Scale
CentOS Linux	7.1	SSH-2.0-OpenSSH_6.6.1	14480	1460	10	7
CentOS Linux	7.2	SSH-2.0-OpenSSH_6.6.1	28960	1460	20	7
CentOS Linux	7.3		28960	1460	20	7
CentOS Linux	7.4	SSH-2.0-OpenSSH_7.4	28960	1460	20	7
CentOS Linux	7.5		28960	1460	20	7
Oracle Linux Server	7.7		28960	1460	20	7
CentOS Linux	7.9	SSH-2.0-OpenSSH_7.4	28960	1460	20	7
Oracle Linux Server	7.9		28960	1460	20	7
Scientific Linux	7.9	SSH-2.0-OpenSSH_7.8	28960	1460	20	7
CentOS Linux	8.0		28960	1460	20	7
Oracle Linux Server	8.0	SSH-2.0-OpenSSH_7.8	28960	1460	20	7

```

    /
    . ydo
    o./dddy"
    'y/ dddddd.
    .hy o d d d d d d d
    :dd/ :h d d d d d d /
    +d d d s
    s d d d d d y' /s o - y y"
    `y d d d d d d y y d d d d s :s
    .h d d d d d d y o - /h d d d d d d o : :
    : d d h s / - / o y d d d d d d d d d d +
    : - - / o y d d d d d d d d d d d d d d d h /

    -----
    Axon Body 3 X60931450 v1.31.94 ECM-US2 Axon Enterprise, Inc.

    -----
    AUTHORIZED USE ONLY!

    This system is for the use of authorized users only. Unauthorized access to
    this computer system and software is prohibited by Title 18, United States
    Code, Section 1030, Fraud and Related Activity in Connection with Computers.

    Individuals using this computer system without authority, or in excess of
    their authority, are subject to having all of their activities on this
    system monitored and recorded by system personnel.

    Disclosure of information found in this system for any unauthorized use is
    STRICTLY PROHIBITED.
  
```

```

    Incorrect passcode. Please try again.
    Duo two-factor login for root

    Enter a passcode or select one of the following options:

    1. Duo Push to +XX XXXXX X5721
    2. SMS passcodes to +XX XXXXX X5721 (next code starts with: 1)

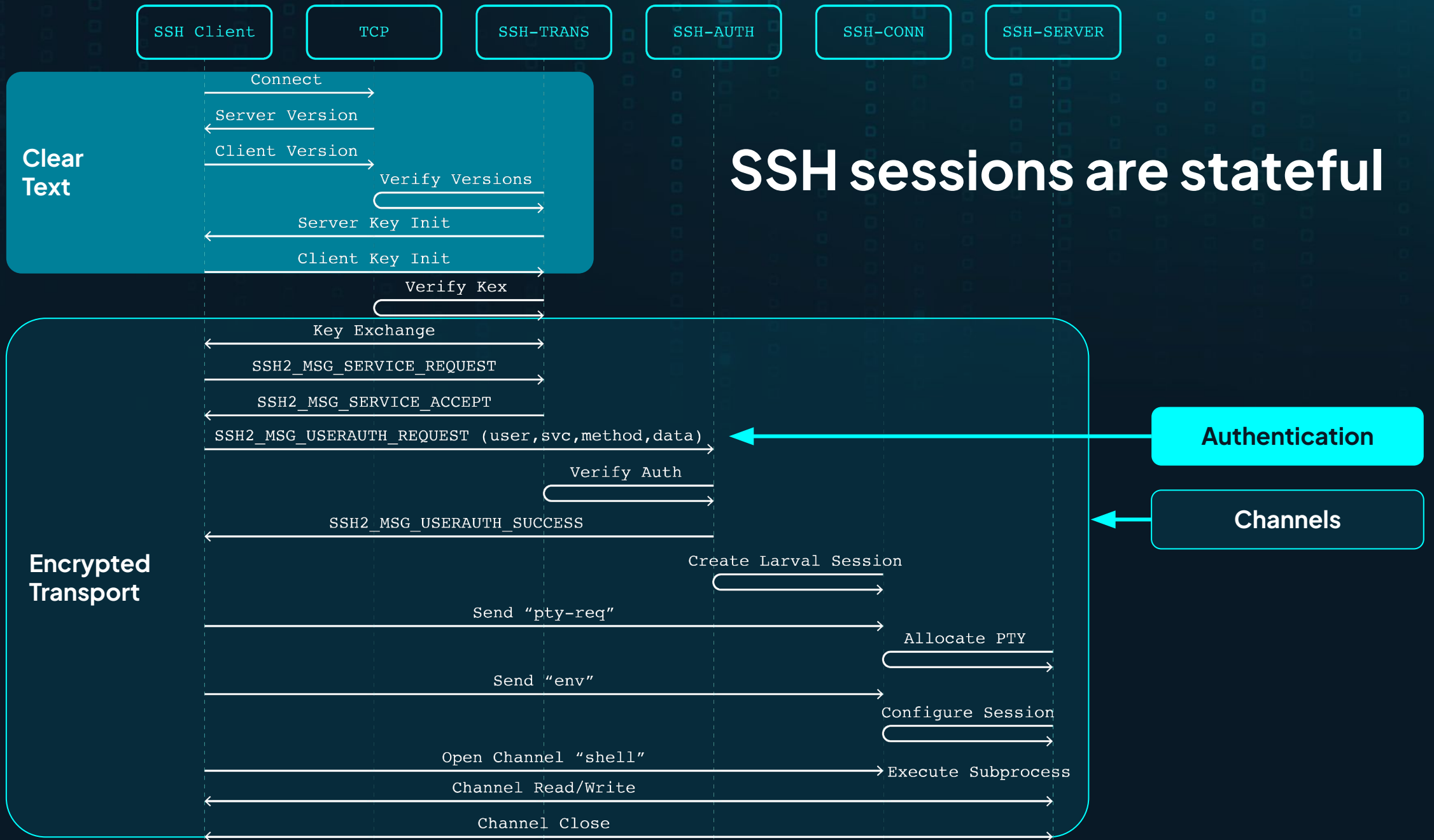
    Passcode or option (1-2):
  
```

Public key authentication is two-stage

An SSH client can confirm if a public key is valid for a given user

- Metasploit support since 2012, but still not widely known
- Great for hunting down bad actors with poor opsec
- Keys via GitHub, Launchpad, firmware, and malware

```
/* XXX fake reply & always send PK_OK ? */  
/*  
* XXX this allows testing whether a user is allowed  
* to login: if you happen to have a valid pubkey this  
* message is sent. the message is NEVER sent at all  
* if a user is not allowed to login. is this an  
* issue? -markus  
*/
```



SSH sessions are stateful

SSH provides transport & authentication

Version exchange & kex init in the clear

- Version: **SSH-2.0**
OpenSSH-9.8p1
deb13u3
- Ciphers, MACs, Compressions, Languages, etc

Key exchange to negotiate secure transport

- Diffie-Hellman & friends pinned with server host key(s)
- Algorithm picked by kex init agreement

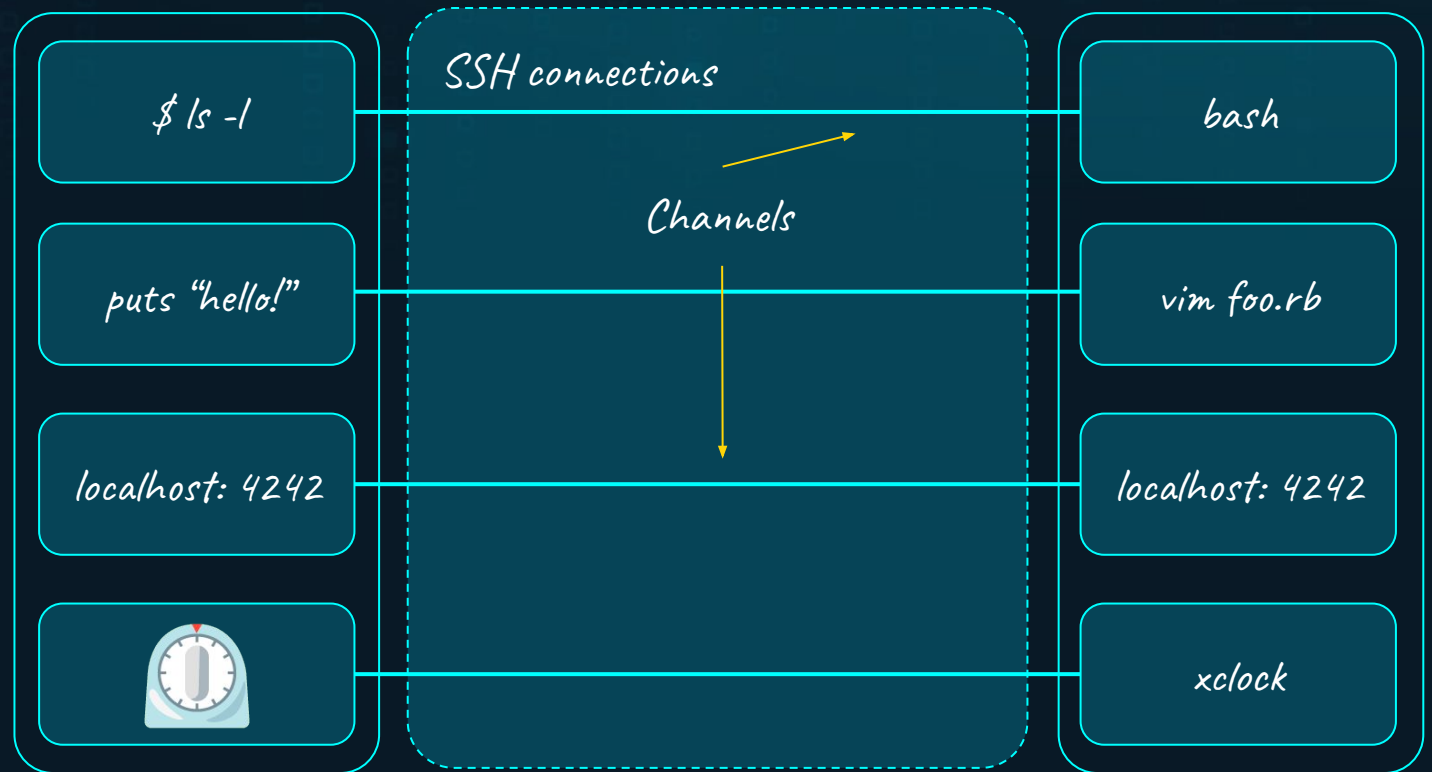
Authentication using one or more methods

- Passwords, public keys, kerberos, & more
- PK uses the session ID for proof signing

Similar to TLS

SSH post-authentication is multiplexed

- Interactive shells
- Command execution
- File transfer (SCP, SFTP)
- TCP forwarding
- Unix socket forwarding
- X11 display forwarding
- Agent forwarding



SSH is effectively the other secure transport

An alternative to TLS, but not exactly the same

- Server key management can be, but usually isn't CA-based
- Authentication is a core stage of the protocol
- Multiplexer & session commands are unique
- SSH uses the first algorithm sent by the client & supported by the server



Compliance schemes gloss over SSH

- Vendors point to strong cipher/mac + authentication similar to TLS
- SSH specifics are often missing, assume best practices
- Key management is the biggest gap

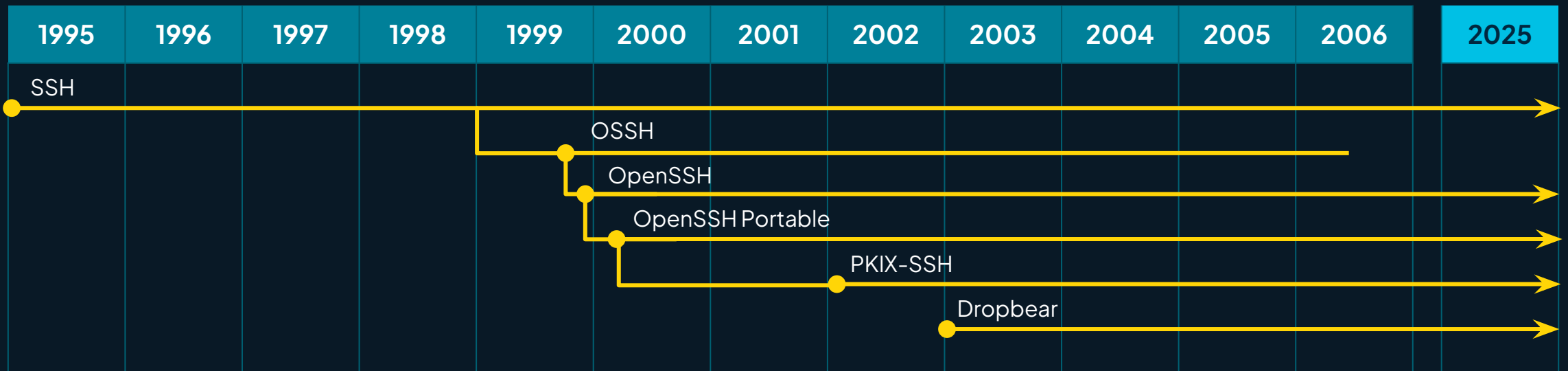
SSH Ecosystem





In the beginning was SSH

Tatu Ylönen created SSH v1 in 1995 as freeware

- Continued development as the proprietary SSH.com (now Tectia)
- Björn Grönvall forked Ylönen's free SSH v1.2.12 as OSSH
- OpenBSD forked OSSH into OpenSSH in 1999



SSH is mostly* OpenSSH & Dropbear

OpenSSH	14,876,142	
Dropbear sshd	678,520	
Cisco IOS	148,007	
Mikrotik	125,545	
Linksys WRT45G modified dropbear sshd	34,694	
lancom sshd	29,559	
HP Integrated Lights-Out mpSSH	6,145	
SCS sshd	6,085	
ZyXEL ZyWALL sshd	5,293	
WeOnlyDo sshd	4,384	
DrayTek Vigor 2820n ADSL router sshd	1,462	
Cisco/3Com IPSSHd	1,388	

Not-OpenSSH/Dropbear are important

Firewall, networking, & storage

- Cisco, NetScreen, Adtran, ComWare, Lancom

OT/ICS equipment

- Siemens, NetPower, Mocana, CradlePoint, Digi

Sensitive applications

- MOVEIT, CrushFTP, GlobalScape, JSCAPE
- BitVis, GoAnywhere, ConfD (Erlang)
- Gerrit, Forgejo, Gitlab

Other implementations





Standalone product examples

- PKIX-SSH — popular in networking equipment, forked from OpenSSH
- WolfSSH — small implementation popular in embedded systems
- Cisco SSH — proprietary implementation for IOS, IOS-XE, NX-OS
- lsh — an old implementation that predates OpenSSH Portable

SSH library examples

- C: libssh (with many bindings)
- Go: x/crypto/ssh & wrappers
- Java: Apache MINA SSH
- Python: Paramiko
- Erlang: SSH

OpenSSH diverges substantially by platform

Name	Changes	Notes
Apple macOS	Light	Changes are limited to macOS compatibility, support for the Keychain, the macOS PKCS helper, & endpoint event logging support.
Debian/Ubuntu Linux	Moderate	Systemd support & much more (36+ patches) 
Red Hat Linux	Moderate	Systemd support & much more (~60 patches) 
PKI-X SSH	Major	Forked in 2002 for X509 support, commonly found in networking gear and FIPS-compliant network appliances. Generally follows OpenSSH changes, but not exactly.
Microsoft Windows	Extreme	Over 350 files changed. Replaces fork with subprocesses, removes chroot support & log sanitization. Logs to Windows Events. Sends telemetry containing SSH-encrypted values. Password authentication uses Lsa* functions. Lags behind upstream for dev and even longer for Windows Updates.

2024 Highlights

Terrapin Attack

Breaking SSH Channel Integrity by Sequence Number Manipulation

Fabian Bäumer

Research Assistant, Ruhr University Bochum

CVE-2023-48795



XZ Utils backdoor

A multi-year campaign started in 2021 and triggered in 2024

- “Jia Tan” persona was likely the product of a state actor
- Nearly-perfect Nobody-But-Us backdoor in SSH
- Backdoor targeted SSH via systemd patches
- Limited to Debian/RHEL-based distros

Caught at the last possible moment by Andres Freund

- Noticed that sshd was using more CPU than it should
- Backdoor made it into rolling releases only

CVE-2024-3094



RegreSSHion

Incredible work by the Qualys Threat Research Unit

- Regression of a signal re-entrance vulnerability
- Unauthenticated remote root code execution
- Tough to exploit due to ASLR & timing

CVE-2024-6387



Related issue discovered by Solar Designer

- Specific to Red Hat builds of OpenSSH
- Limited to the non-root privsep user

CVE-2024-6409

MOVEit & IPWorks SSH

Another MOVEit vulnerability, but this time in SSH

- watchTower Labs reversed the MOVEit patch for CVE-2024-3094
- The attacker's unauthenticated public key blob is opened as a file
- File path supports UNC and was used for authentication
- Root cause was the third-party IPWorks library
- Threaded a dozen needles to bypass auth

CVE-2024-5806



SSHamble

- A research tool for SSH implementations
- Quickly scans and gathers detailed data
- Interesting attacks against authentication
- Post-session authentication attacks
- Pre-authentication state transitions
- Post-session enumeration
- Easy timing analysis

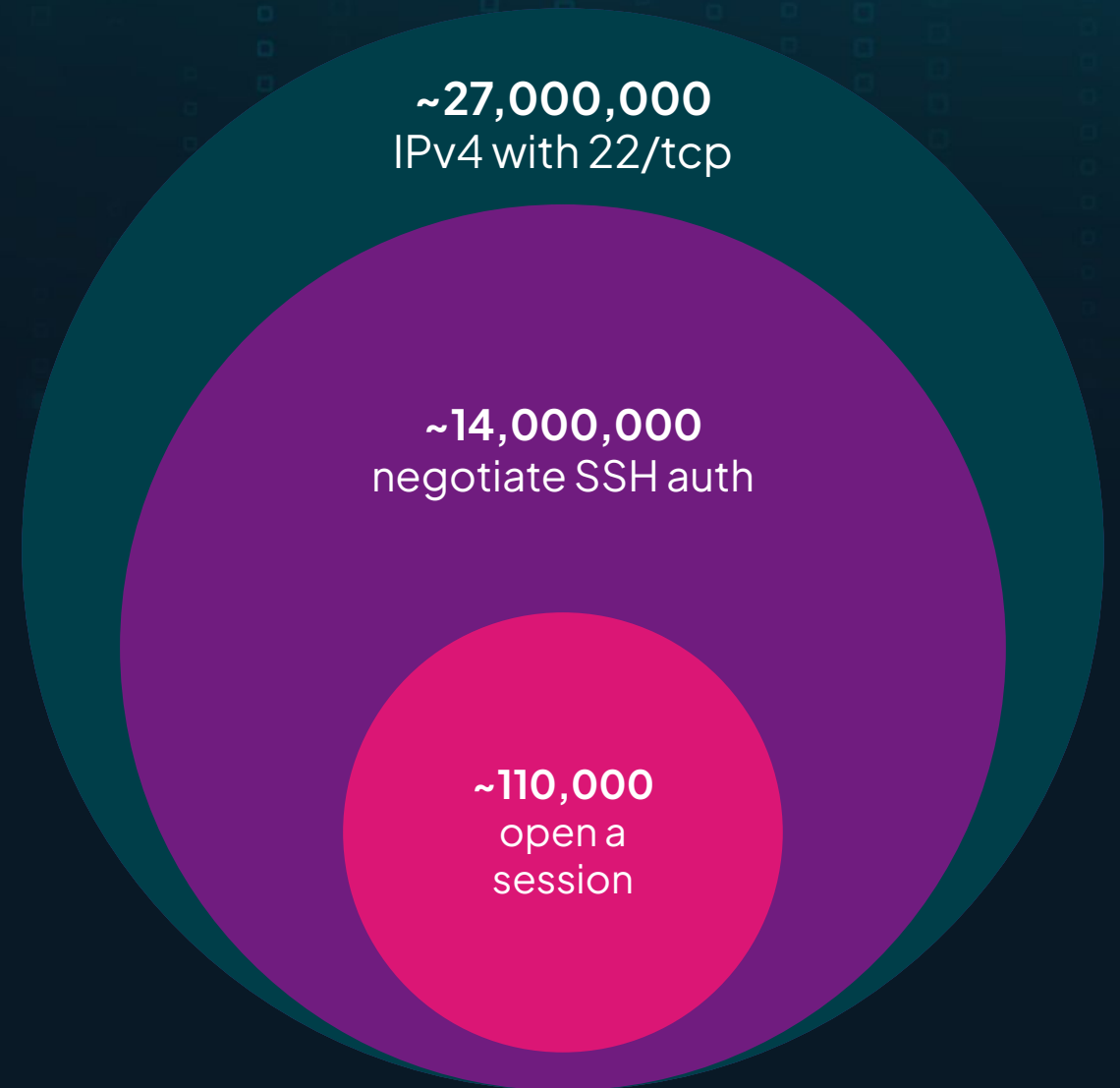


<https://SSHamble.com>

Shaking out the shells

A lot of broken SSH on the internet

- Tons of tarpits & buggy systems
- ~14 million reach ssh-auth state
- ~110k resulted in a session
- ~9 unique vulnerabilities



SSHamble Detection (2024)

Product	Impact
Ruckus Wireless APs	Unauthenticated root command execution
Digi TransPort Gateways	Unauthenticated remote CLI access as SUPER
Panasonic Ethernet Switches	Unauthenticated remote CLI access as admin
Realtek ADSL Gateways	Unauthenticated remote CLI access as admin
Soft Serve	Authenticated remote code execution
GOGS	Authenticated remote command execution
OpenSSH for Windows	Unauthenticated OOB memory leak / comparison bug
ION Networks Service Access Point	Unauthenticated TCP forwarding
Multiple Products	Unlimited public key testing

Recent Research

OpenSSH MiTM & DoS

More amazing work by the Qualys Threat Research Unit

- Successful machine-in-the-middle (MitM) against OpenSSH clients
- Abuses VerifyHostKeyDNS error handling with memory exhaustion
- Pre-auth denial of service via “ping” messages

CVE-2025-26465

CVE-2025-26466



Go SSH Authentication Bypass

Platform.sh team identified a footgun in Go's x/crypto/ssh

- Public key handler is called for each key presented by the attacker
- Buggy applications can use the wrong key for authentication
- Best documented case is the NetApp Telegraf Agent
- Footgun partially fixed via Go x/crypto/ssh update



CVE-2024-45337

BadKeys.info

Hanno Böck's amazing key analyzer & database

- Includes a scanner for common protocols (SSH, TLS, etc)
- Dynamic analysis for cryptographic issues
- Massive lookup database for known keys
- Includes some sensitive/leaked key sets
- Fast lookups via b-search



Erlang OTP SSH Remote Code Execution

Fabian Bäumer, Marcus Brinkmann, Marcel Maehren, & Jörg Schwenk (Ruhr University Bochum)

CVE-2023-48795

- State machine bug, the fix limits acceptable message types by session state
- Exploitable after the version and kex init, even before encryption starts, easy one-liner exploit
- Direct remote evaluation of Erlang code



Erlang OTP SSH Remote Code Execution

Why did we miss this with SSHamble?

- Erlang doesn't reply to the channel open or exec in this state, causing SSHamble to timeout. Unfortunately neither do a lot of non-vulnerable things, so tests have to be Erlang/ConfD specific.

CVE-2023-48795

Real-world impact

- Few instances of Erlang-SSHD in the wild
- Cisco NETCONF ConfD is based on Erlang
- Direct RCE on Cisco NSO / ConfD systems
- Not port 22, check 830, 2022, & 2024
- No patch planned until May 2025
- Patch it yourself with ``ssh:stop().``



```
23:00:38.907100 <0.106.0> Server Channel info returned:  
{noreply,"#state{}}"
```

Introducing **SSHamble v2**

New features in SSHamble!

- Automatic badkeys.info blocklist lookups
- Additional authentication bypass methods
- Wider algorithm and host key support
- Experimental blind exec vuln checks
- Target filtering with --skip-versions

<https://SSHamble.com>



SSHamble v2 == v0.2.x

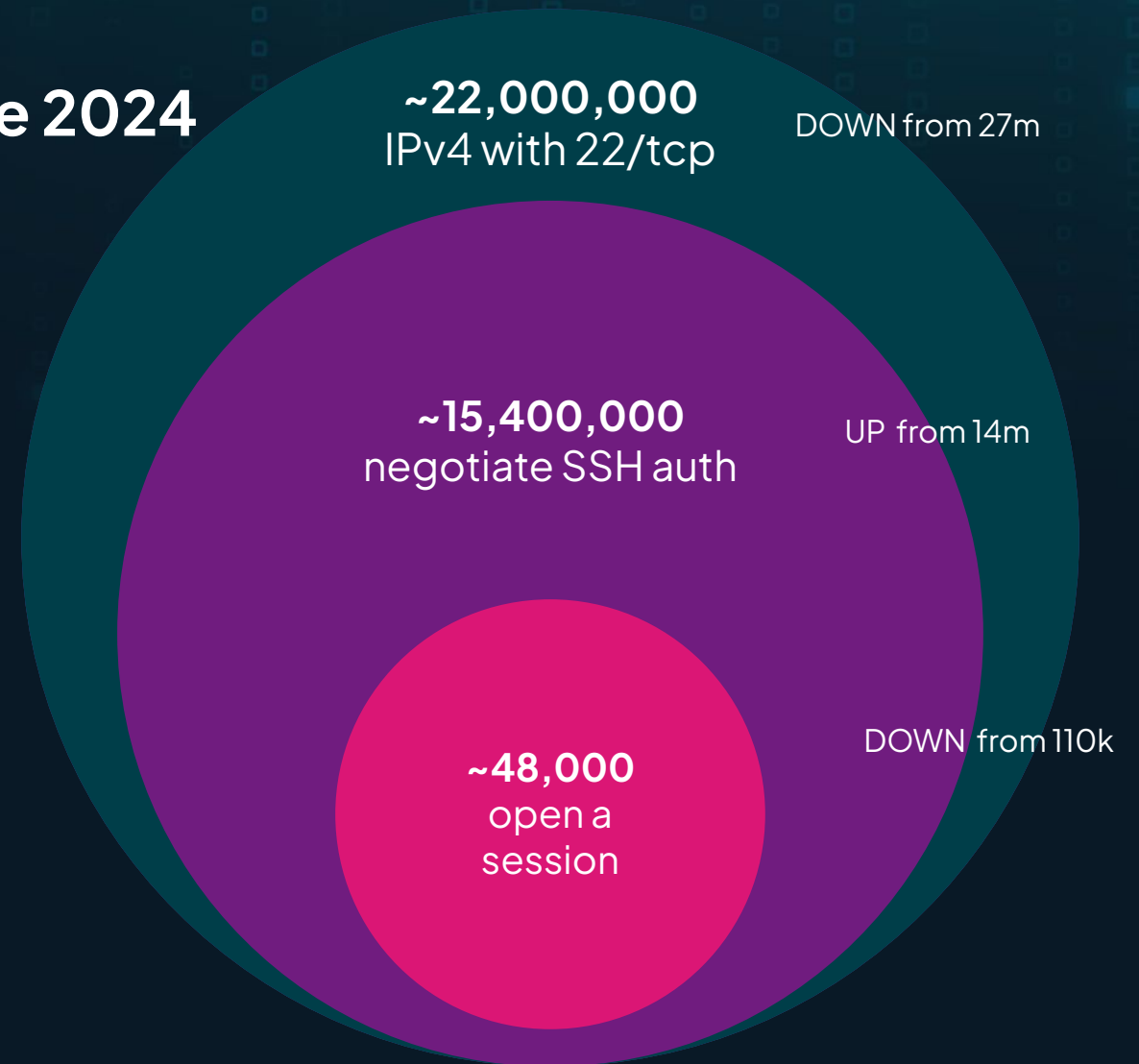
Major changes in internet SSH exposure

Less total port 22 on the internet since 2024

- More valid SSH servers, less tarpits
- ~15.4 million reach auth state
- ~48k resulted in a session
- ~3 common issues

Excluding “missing patch” bugs

- Use of hardcoded/reused host keys
- Authentication bypasses
- Pre-auth port forwarding



Built-in checks

bypass	auth-none	skip-auth	auth-success
	method-null	method-empty	skip-pubkey-any
publickey	pubkey-any	pubkey-any-half	user-key
	half-auth-limit	pubkey-hunt	—
password	pass-any	pass-empty	pass-null
	pass-user	pass-change-empty	pass-change-null
keyboard	kbd-any	kbd-empty	kbd-null
	kbd-user	—	—
gss-api	gss-any	—	—
userenum	timing-none	timing-pass	timing-pubkey
vulns	vuln-tcp-forward	vuln-generic-env	vuln-softserve-env
	vuln-gogs-env	vuln-ruckus-password-escape	vuln-exec-skip-auth
	badkeys-blocklist	—	—

Getting started

Start a network scan

```
$ sshamble scan -o results.json 192.168.0.0/24
```

Analyze the results

```
$ sshamble analyze -o output results.json
```

Specify ports, usernames, passwords, public keys, private keys, and more

```
$ sshamble scan -o results.json 192.168.0.0/24 \  
  --users root,admin,4DGift,jenkins \  
  --password-file copilot.txt \  
  -p 22,2222 \  
  --pubkey-hunt-file admin-keys.pub \  
  --privkey-hunt-file admin-keys.priv
```

Open an interactive shell for sessions

```
$ sshamble scan -o results.json 192.168.0.0/24 \  
  --interact first --interact-auto "pty,env LD_DEBUG=all,shell"
```


The interactive shell

Enter the sshamble shell with `^E`. Commands:

exit		- Exit the session (aliases 'quit' or '.')
help		- Show this help text (alias '?')
env	a=1 b=2	- Set the specified environment variables (-w for wait mode)
pty		- Request a pty on the remote session (-w for wait mode)
shell		- Request the default shell on the session
exec	cmd arg1 arg2	- Request non-interactive command on the session
signal	sig1 sig2	- Send one or more signals to the subprocess
tcp	host port	- Make a test connection to a TCP host & port
unix	path	- Make a test connection to a Unix stream socket
break	milliseconds	- Send a 'break' request to the service
req	cmd arg1 arg2	- Send a custom SSH request to the service
sub	subsystem	- Request a specific subsystem
send	string	- Send string to the session
sendb	string	- Send string to the session one byte at a time

sshamble>

Happy scanning!

I



Bonus: **excrypto**

SSL 3.0 through TLS 1.3 (and soon PQC)

Merge of zcrypto with Go tip and SSHamble tweaks

- Easily test ancient and bleeding edge TLS in one library
- Parse broken x509 certificates anyways
- Extract hard-to-see fields

<https://github.com/runZeroInc/excrypto>

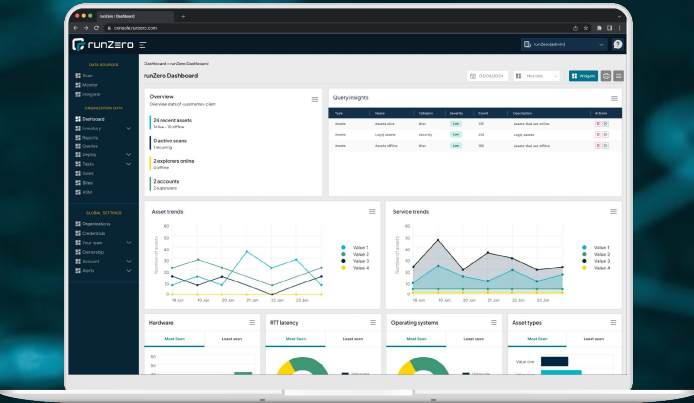
Thank you!



runZero.com

research@runZero.com

SSHamble.com



References 1/2

- <https://boehs.org/node/everything-i-know-about-the-xz-backdoor>
- <https://github.com/ssh-mitm/ssh-mitm>
- <https://ssh-comparison.quendi.de/comparison/hostkey.html>
- <https://words.filippo.io/ssh-whoami-filippo-io/>
- <https://github.com/badkeys/badkeys>
- Metasploit: `ssh_identify_pubkeys` (2012)
- regreSSHion: <https://www.qualys.com/2024/07/01/cve-2024-6387/regresshion.txt>
- Terrapin: <https://terrapin-attack.com/>
- <https://labs.watchtowr.com/auth-bypass-in-un-limited-scenarios-progress-moveit-transfer-cve-2024-5806/>
- <http://thetarpit.org/2018/shithub-2018-06>
- <https://helda.helsinki.fi/server/api/core/bitstreams/471f0ffe-2626-4d12-8725-2147232d849f/content>
- <https://github.blog/2023-03-23-we-updated-our-rsa-ssh-host-key/>
- Kannisto, J., Harju, J. (2017). The Time Will Tell on You: Exploring Information Leaks in SSH Public Key Authentication. In: Yan, Z., Molva, R., Mazurczyk, W., Kantola, R. (eds) Network and System Security. NSS 2017. Lecture Notes in Computer Science(), vol 10394. Springer, Cham. https://doi.org/10.1007/978-3-319-64701-2_22
- West, J.C., Moore, T. (2022). Longitudinal Study of Internet-Facing OpenSSH Update Patterns. In: Hohlfeld, O., Moura, G., Pelsser, C. (eds) Passive and Active Measurement. PAM 2022. Lecture Notes in Computer Science, vol 13210. Springer, Cham. https://doi.org/10.1007/978-3-030-98785-5_30
- Neef, S. (2022). Source & result datasets for "Oh SSH-it, what's my fingerprint? A Large-Scale Analysis of SSH Host Key Fingerprint Verification Records in the DNS" [Data set]. Zenodo. <https://doi.org/10.5281/zenodo.6993096>

References 2/2

- <https://www.openwall.com/lists/oss-security/2025/04/16/2>
- <https://platform.sh/blog/uncovered-and-patched-golang-vulnerability/>
- <https://blog.qualys.com/vulnerabilities-threat-research/2025/02/18/qualys-tru-discovers-two-vulnerabilities-in-openssh-cve-2025-26465-cve-2025-26466>
- <https://badkeys.info/> & <https://github.com/badkeys/badkeys>
- <https://github.com/runZeroInc/sshamble>
- <https://github.com/runZeroInc/excrypto>
- <https://www.runzero.com/blog/inside-out-attack-surface-management/>