Practical Guidelines for End Users to Enhance Cybersecurity in Remote Computing

Marcelo Ponce, Ramses van Zon

May 16, 2023

https://github.com/cybersec-BestPractices/cybersec-RemoteComputing

Connections, forwarding & tunneling	

connection to remote system	`ssh username@remote.system.IP`
	`ssh username@remote.system.IP -p PORTnbr`

with graphics-forwarding	`ssh -X username@remote.system.IP`
	`ssh -Y username@remote.system.IP`

tunneling	`ssh -R remPort:remote_host:locPort username@remote.system.IP`
	`ssh -L locPort:remote_host:remPort username@remote.system.IP`
	`ssh -fN -[R|L] port:remote_host:port username@remote.system.IP`

remote execution	`ssh username@remote.system.IP "remote_cmd_to_exec"`
Keys	

generation	`ssh-keygen -t ed25519`
	`ssh-keygen -t rsa -b 4096`

	`# key generation with comments and specified location`
	`ssh-keygen -t ed25519 -C "USER@laptop␣cluster-X" -f $HOME/.ssh/USER_clusterX_ed25519`
	`# ssh using specific key file`
	`ssh -i $HOME/.ssh/USER_clusterX_ed25519 USERNAME@clusterX.IP.address`

transfer	`ssh-copy-id  -i $HOME/.ssh/id_ed25519.pub  USERNAME@remote.system.ip`
	`# copying over keys to remote system`
	`cat $HOME/.ssh/id_ed25519.pub \| ssh USERNAME@remote.system.ip "cat␣>>␣$HOME/.ssh/authorized`

agent to recall key	`ssh-add key-file`
	`ssh-add key-file -t life`

Troubleshooting	

debugging (verbose mode)	`# -v activates the "verbose mode": resulting in printing debugging messages`
	`# helpful in diagnosing connection, authentication, and configuration problems`
	`# Multiple -v options increase the verbosity, the maximum is 3.`
	`ssh -v  USERNAME@remote.system.ip`
	`ssh -vv USERNAME@remote.system.ip`
	`ssh -vvv USERNAME@remote.system.ip`

Table 1: Summary of different `ssh` functionalities and commands.

Action	Description	Mitigation
keep software up-to-date	keep your devices updated with all software updates, including OS and applications	zero-day exploits, bugs, known vulnerabilities mitigates the risk of the remote computing system being compromised via the end user workstation
use `ssh` to connect to remote systems	de-facto tool to connect to remote systems using asymmetric encryption	MITM attacks, packet interception (sniffing)
use ssh-keys	more efficient and convenient way to authenticate	key-loggers, stolen credentials
use ssh-keys + MFA	enhanced way to authenticate	stolen private key
verify fingerprint of remote system	checks validity and authenticity of remote system by comparing system's fingerprints with publicly reported ones	MITM attacks, IP spoofing
connect through VPN	improves network protection and privacy by creating an encrypted channel over unsecured networks such as the Internet	MITM attacks, sensitive data exposure
use an antivirus	local protection against wide spectrum of malware	multiple types of malware mitigates the risk of the remote computing system being compromised via the end user workstation
use a passwords manager	specialized tool to more securely (i.e. using encryption) store passwords and generate strong passwords, which is useful if SSH keys as an authentication method is not available	password stealing, password brute-force

Table 2: Summary of some best practices for end users to enhance cybersecurity in remote computing.

In your *local system*:

- □ use an anti-virus
- □ keep software up-to-date with the latest patches, including the ones for the Operating System (OS)
- □ be mindful of emails, malicious attachments and links:
    - □ do not enter sensitive data in unknown websites,
    - □ verify for https connections and SSL certificates
- □ do not plug any type of devices of unkown origin or source, e.g. USB-devices, etc.
- □ use a password manager, do not store passwords in plain-text and use a different password for each service
- □ encrypt sensitive data

When connecting to *remote systems*:

- □ use ssh keys, with passphrases
- □ use MFA
- □ use VPN
- □ check the information provided by the remote system (usually at the moment of logging in), about when have you connected and from which locations
- □ consider using "private browsing" and set restrictions on *cookies* policies in your web browser and when visiting websites with tracking and third party cookies

Table 3: Cyber-security *checklist*: main elements to take into consideration to enhance the cyber-security in your local and remote work spaces.