Wireless Keystroke Injection
An Attack Vector During Physical Assessments

- Vulnerability analysis
- Demonstration
- Attack through the eyes of the “Black Hat”
- Relevance of the attack
- Q/A

Sergei Simonovi

DEEPSEC.NET

ქავქასიის უნივერსიტეტი
CAUCASUS UNIVERSITY

SCIENTIFIC CYBER SECURITY ASSOCIATION

Rubber Duckie usage

Victim

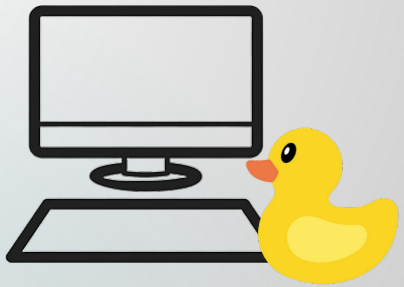
Attacker

Rubber Duckie usage

Victim

Attacker

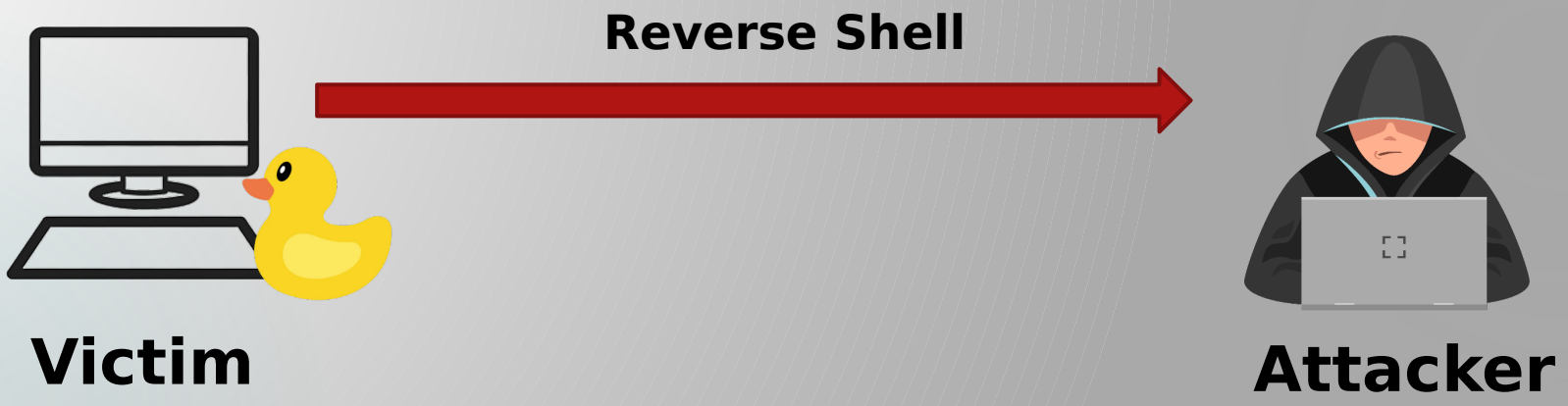
Rubber Duckie usage



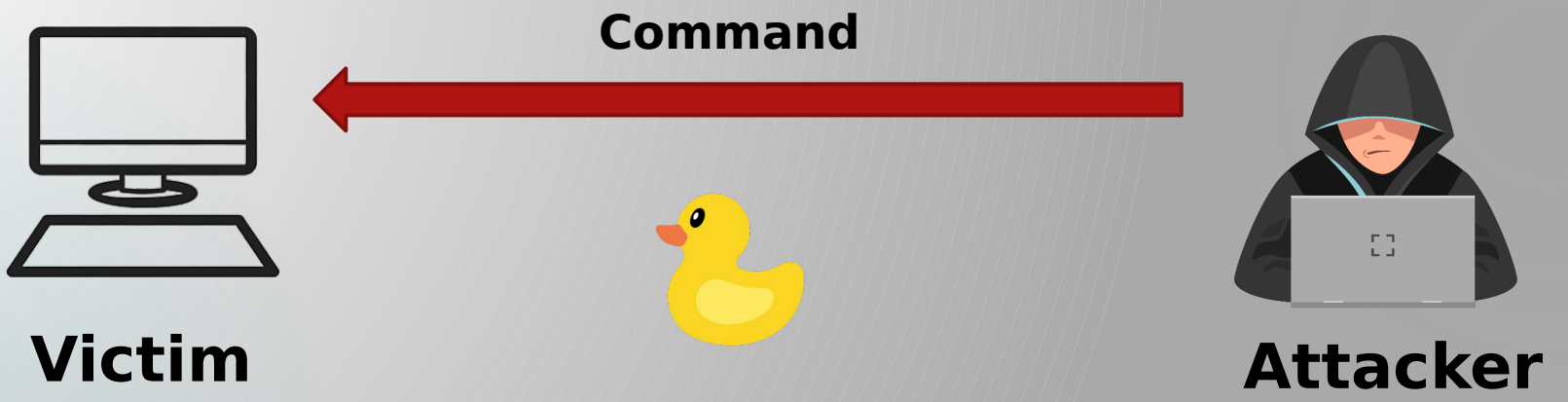
Victim

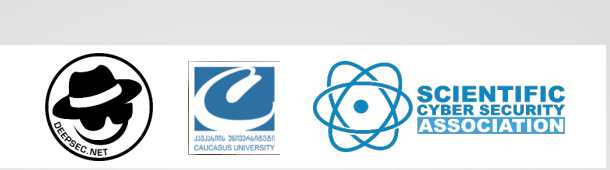
Attacker

Rubber Duckie usage



Remote Access Rubber Duckie

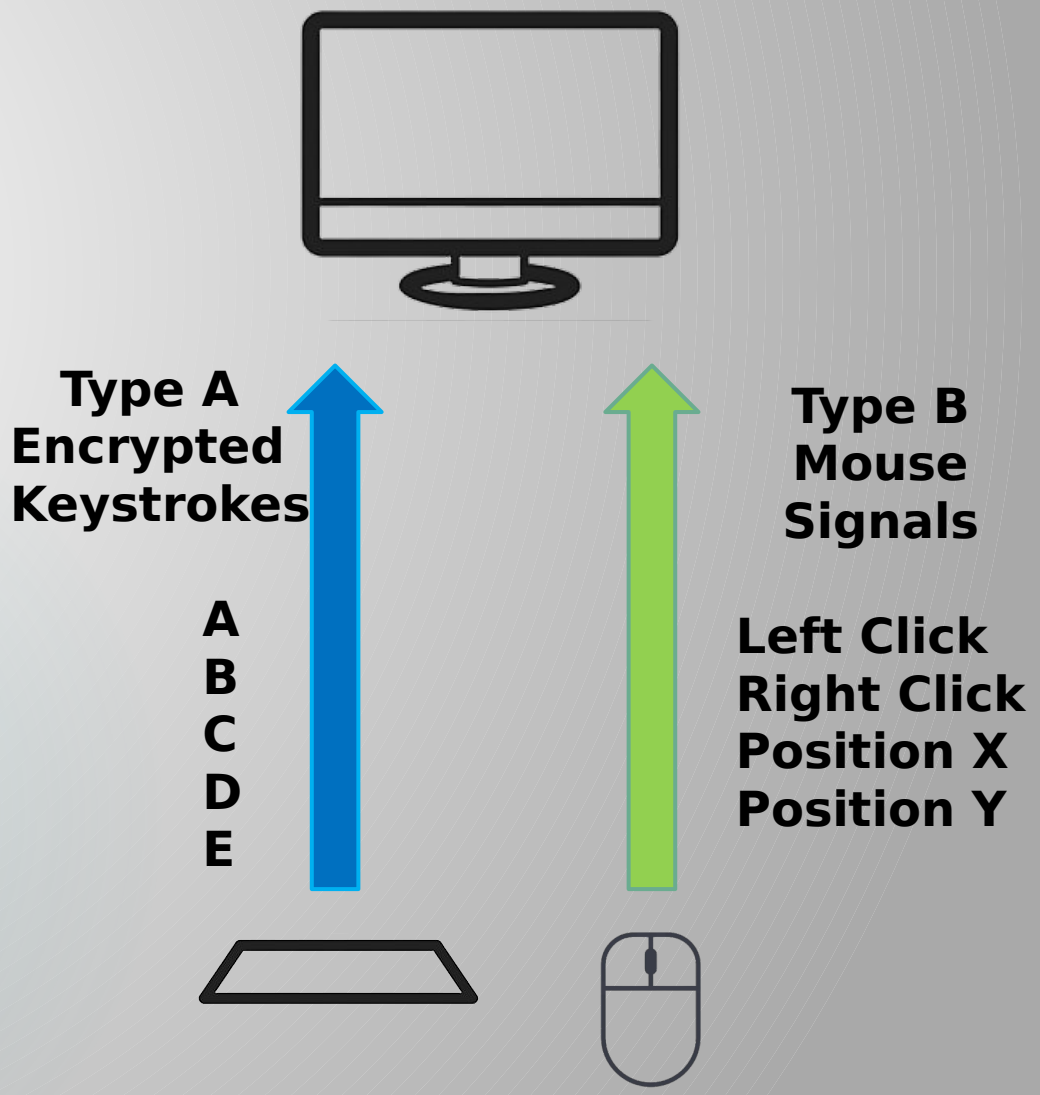




Keystroke Injection

CrazyRadio PA (Also the nRF24L)

nRF24L (2.4 GHz)


Type A
Encrypted
Keystrokes
A
B
C
D
E
Type B
Mouse
Signals
Left Click
Right Click
Position X
Position Y

Victim

Type B
Unencrypted
Keystrokes

Powershell.exe --------

Attacker

Type A
Encrypted
Keystrokes

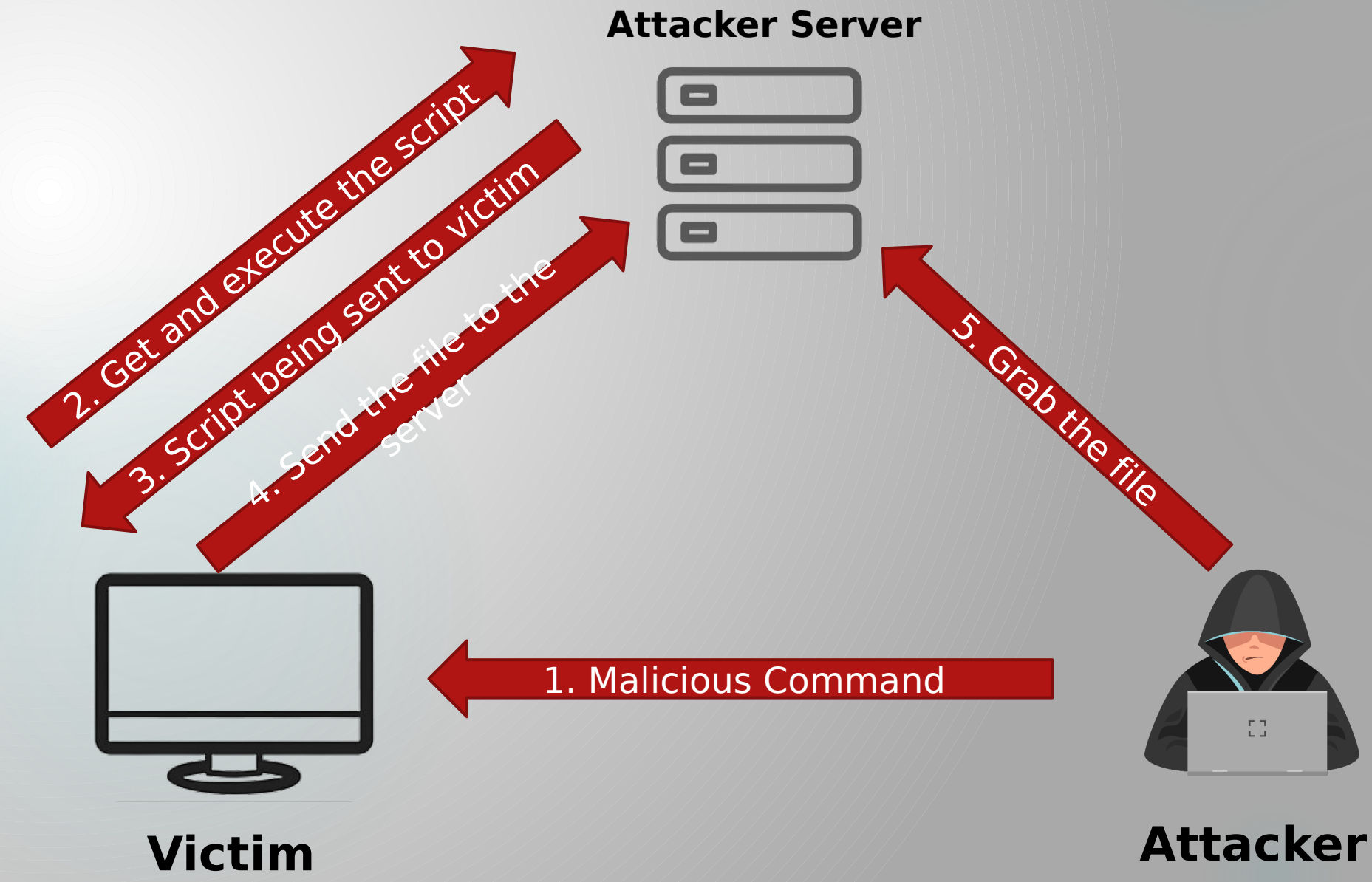
A
B
C
D
E

Type B
Mouse
Signals

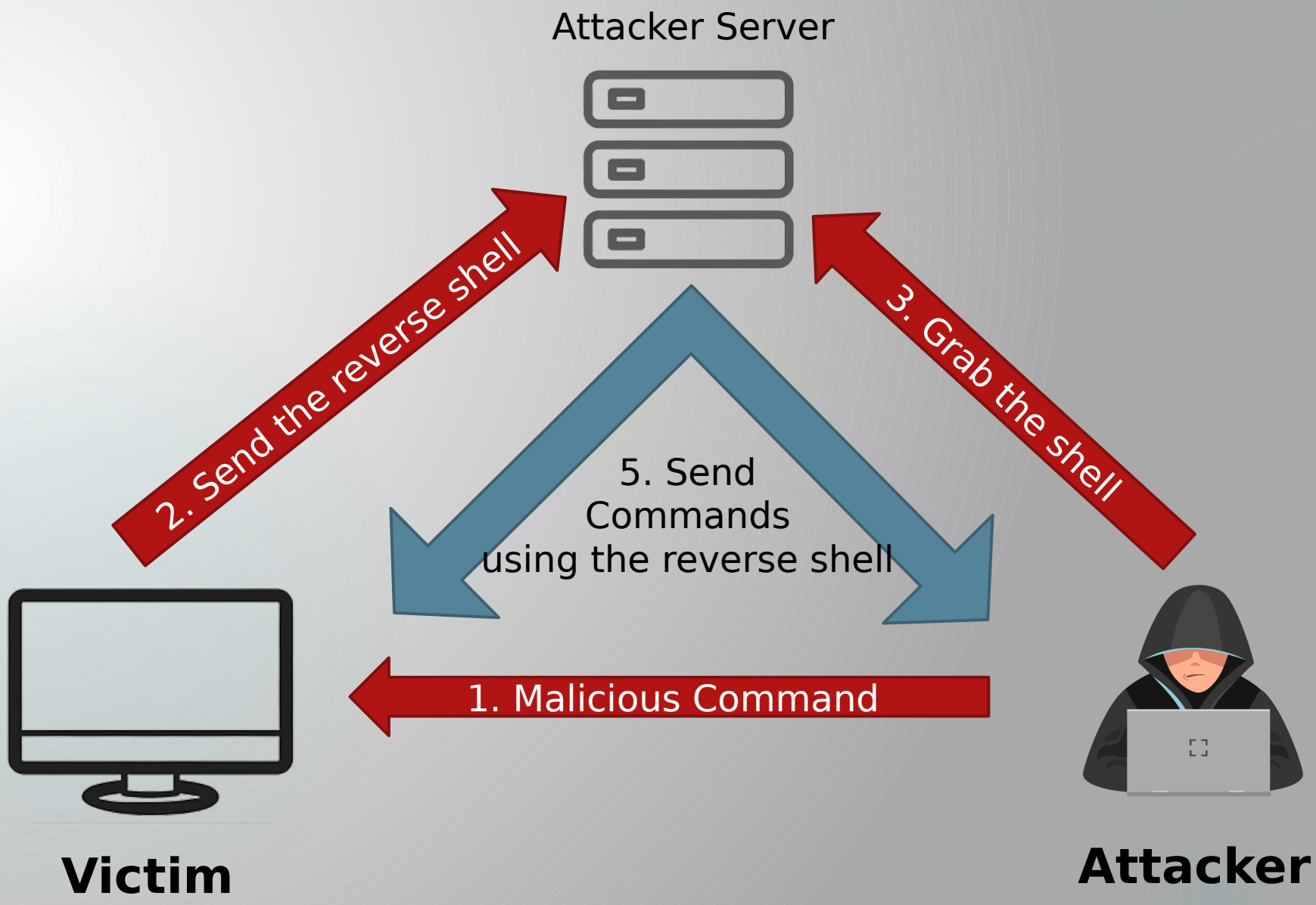
Left Click
Right Click
Position X
Position Y

SCIENTIFIC CYBER SECURITY ASSOCIATION

Wi-Fi credentials extraction



Reverse shell scenario



Any other attacks?

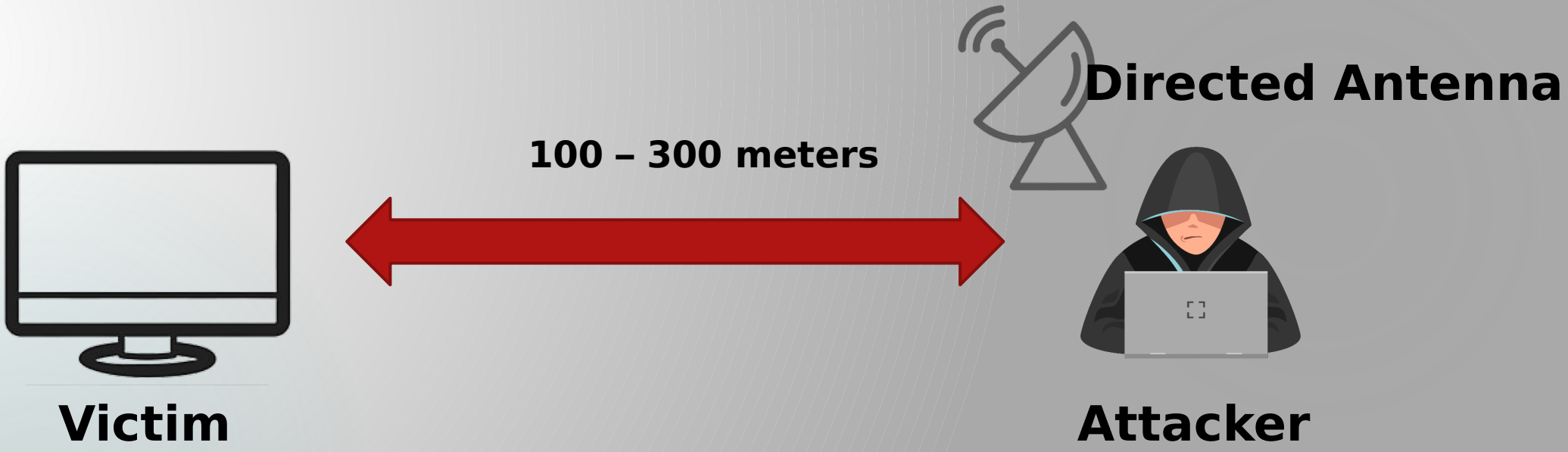
- Keylogger installation
- Backdoor/Trojan installation
- C2 Beacon installation
- NTLM Hashes extraction
- Website sessions extraction
- Add a new admin user
- Enable the RDP

And much more!

10 – 50 meters

Victim

Attacker


Directed Antenna
100 – 300 meters
Victim
Attacker

Relevance of keystroke injection

- More vendors to research
- Amount of already produced unpatched devices that are still in use

Advantages of keystroke injection

- Stealthy and quick. No antivirus shall detect it
- No need to be in the same local network
- Full control over the victim operating system

Disadvantages of keystroke injection

- Have to be lucky to guess the OS
- Physical proximity required

Conclusions

The widespread of wireless input devices and lack of security awareness makes it a perfect attack vector

- Efficient vector of attack but requires the victim to have vulnerable hardware
- Can be amplified using the directed antenna
- Instant “root” on the victim OS
- No antivirus shall spot the attack. The only way to stop the attacker is unplugging the dongle
- To make it even more efficient we may use the cloud hosted payload
- The vulnerability is only patched when all the vendors around the globe patch it

Thanks for your attention!

Q&A