Attacking Factories via USB Devices

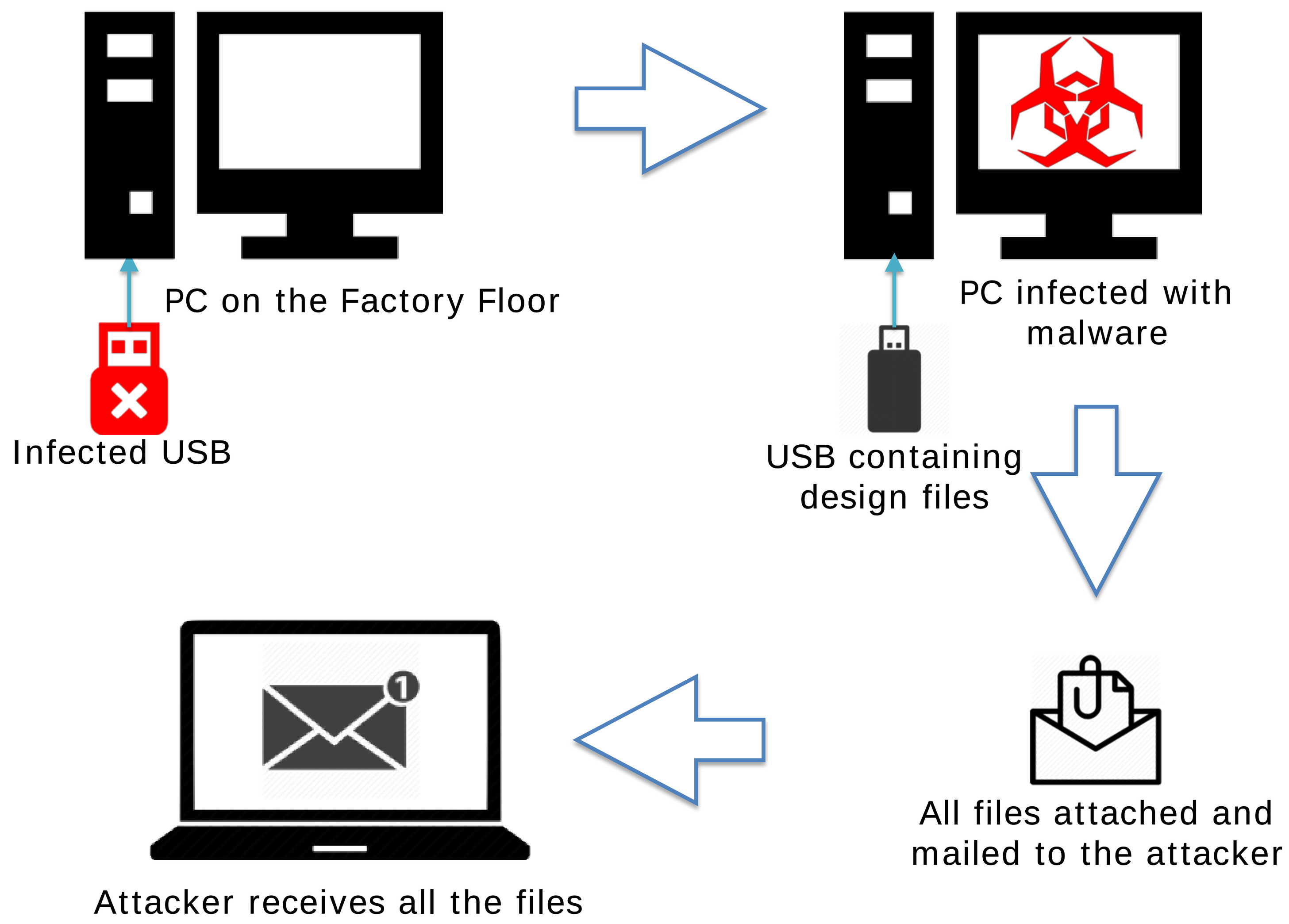
Kushagra Madan, Marianne Winslett, William P. King

ENGINEERING AT ILLINOIS
INFORMATIONTRUST INSTITUTE
CRITICAL INFRASTRUCTURE RESILIENCE INSTITUTE
U.S. DEPARTMENT OF HOMELAND SECURITY

What an attacker can do

➢ **Steal designs and data**

- PC malware is installed as soon as an infected USB is inserted in the PC.
- All data from any USB subsequently inserted in the PC is secretly sent to the attacker.

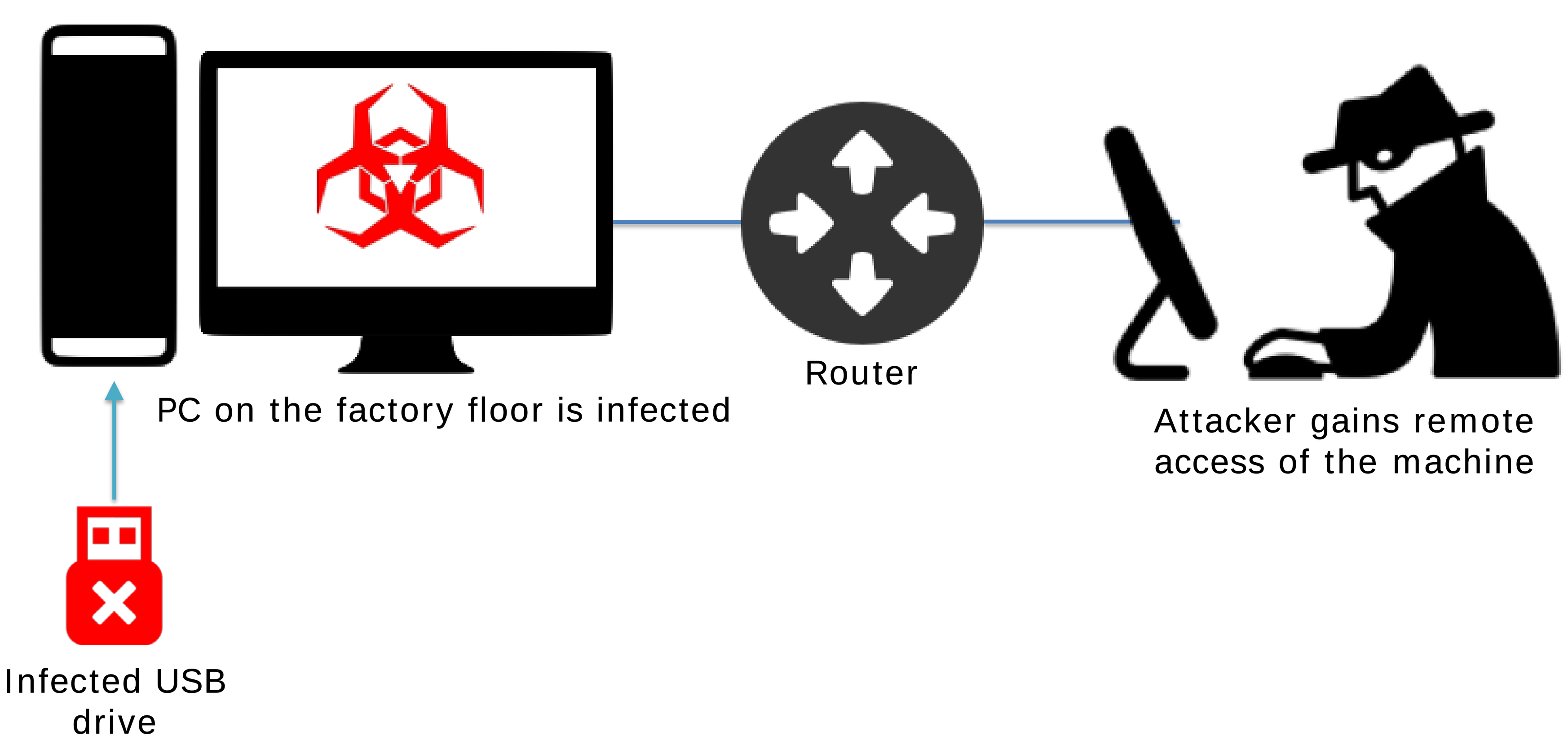


➢ **Alter designs and data**

- USB malware searches for designs, G-code and data as soon as the USB is inserted in the PC.
- After finding a file of interest, the malware corrupts the file as defined by the attacker.

➢ **Control a PC remotely**

- USB malware gives remote access to an attacker on the same network as the infected PC.
- The attacker has complete control over the infected PC from their local machine and can carry out a variety of attacks.



➢ **Alter machinery firmware**

- USB malware provides a new firmware file and forces its installation.
- The new firmware may cause damage to the machinery, introduce defects into products, or make good products look defective.
- Example: Machinery-destroying Stuxnet, which spread in part by exploiting a vulnerability in the handling of Windows shortcut icons. Malware was executed when an infected shortcut icon on a USB was displayed.

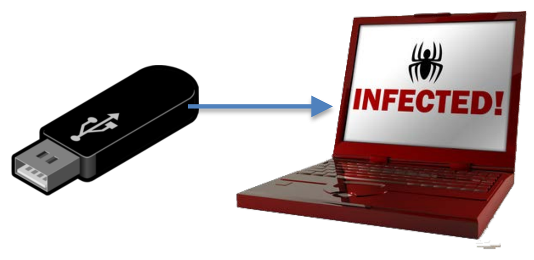
Why it Works

➢ **Factory employees and vendors use USBs to transfer design files to PCs on the factory floor,** because internet transfers are seen as too risky.

➢ **It's easy for them to get an infected USB.**


Get it as a freebie in an event


Pick it up in a parking lot or corridor

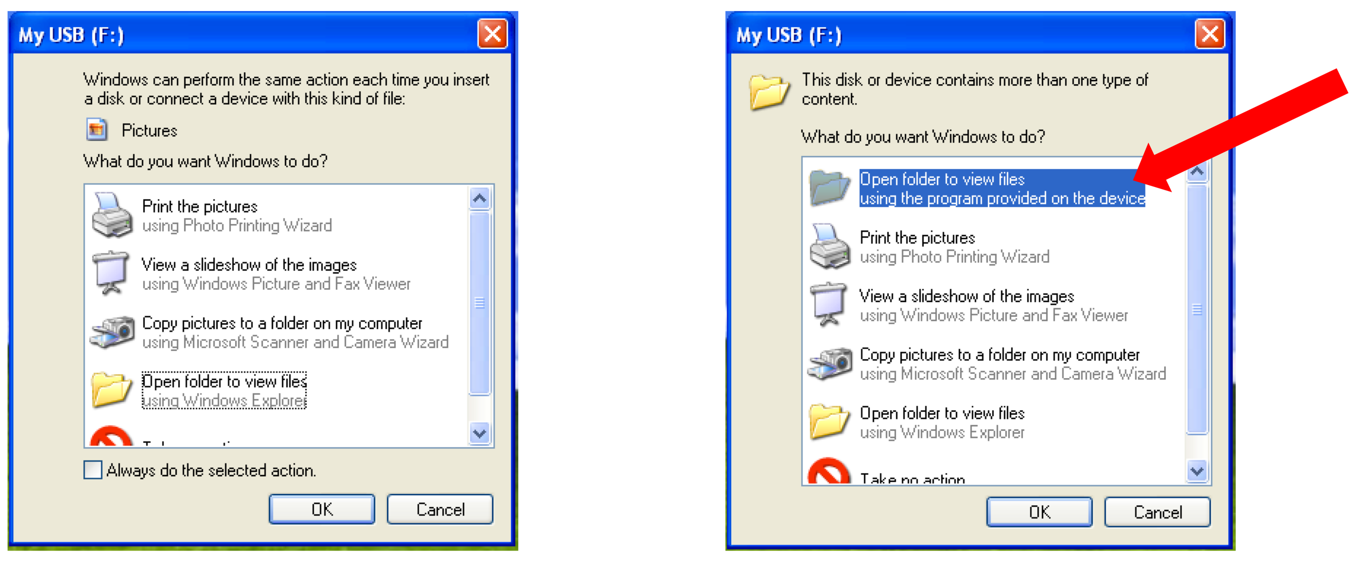


Use a healthy USB in an infected PC

➢ **Factory PCs run old, unpatched, vulnerable versions of Windows,** because machinery is long-lived and software updates can cause cascading failures.

How it works

➢ **Exploit Windows' Autorun**



Attacker's Autorun script on a USB uses social engineering to dupe the user.

'U3 Smart Drives' can execute a payload as soon as they're plugged in.

➢ **Inject malware into reverse-engineered USB firmware**

Reverse engineering the firmware to make the USB behave differently.

E.g., micro-controller reprogrammed to behave as a keyboard that types in commands from a script.

➢ **Exploit other vulnerabilities**

Patches are released whenever a vulnerability is discovered, but patches are not normally installed on PCs on the factory floor.