**🔓 Wireless Hacking of Keyboards, Mice & Drones**

🎯 *Understand how insecure wireless protocols can be exploited in real-world attacks.*

**🧠 Why Study This?**

Many **wireless input devices (keyboards, mice, drones)** don’t use strong encryption, or **don’t authenticate** the device they’re communicating with.  
That makes them vulnerable to **injection**, **sniffing**, or even **full control**.

**🎯 Challenge Lab 1: MouseJack Attack**

**🔍 What is MouseJack?**

MouseJack is a **vulnerability in wireless mice and keyboards** that allows attackers to:

* Inject **keystrokes**
* Bypass lock screens
* Gain access without needing Bluetooth pairing

🧠 Affects: Devices using **non-Bluetooth 2.4 GHz** wireless dongles (like Logitech Unifying Receivers)

**🛠 Tools Needed:**

* **Crazyradio PA dongle** (cheap 2.4 GHz USB dongle)
* **MouseJack toolset** (https://github.com/BastilleResearch/mousejack)
* Compatible target device (Logitech, Dell, HP, etc.)

**🧪 Steps to Simulate MouseJack:**

1. Plug in **Crazyradio PA**
2. Install MouseJack tools:
3. git clone https://github.com/BastilleResearch/mousejack
4. cd mousejack
5. pip install -r requirements.txt
6. Scan for devices:
7. sudo ./scan\_interface.py
8. Inject keystrokes (simulate attack):
9. sudo ./inject\_command.py <device> "start powershell"

💡 *You can open PowerShell, run commands, or even download malware.*

**🔍 Who Created MouseJack?**

* **Bastille Research** – a security research company specializing in radio and wireless attacks.

**🎯 Challenge Lab 2: Bastille Tools & Awareness**

**📡 Bastille Overview:**

* Scans the **entire radio spectrum** for vulnerabilities
* Detects:
  + Unauthorized devices (rogue mice, keyboards)
  + Wireless injection attempts
  + Bad security protocols

🛠 Bastille supports devices like:

* Logitech
* Microsoft
* HP
* Lenovo
* And others using **2.4 GHz dongles**

**🎯 Challenge Lab 3: Drone Hacking**

**🔍 How Are Drones Hacked?**

**1. Wi-Fi Controlled Drones**

* Use default Wi-Fi credentials
* Unencrypted control channels

🛠 Tools:

* aircrack-ng (capture Wi-Fi)
* Wireshark (sniff drone packets)
* SkyJack (hijack drones via Wi-Fi)
  + By Samy Kamkar

**2. Radio Controlled Drones (2.4 GHz)**

* Some use no encryption
* Can be hijacked using **HackRF**, **SDR**, or **RollJam**

**3. GPS Spoofing**

* Trick drone into flying to a fake location
* Using GPS simulator or SDR

**⚙️ Example Tools:**

| **Tool** | **Purpose** |
| --- | --- |
| Crazyradio PA | MouseJack wireless attack |
| Bastille | Radio frequency threat detection |
| SkyJack | Drone hijacking over Wi-Fi |
| HackRF | SDR to jam/snoop/control drones |
| Wireshark | Analyze control packets |
| SDR# | Visual radio spectrum |

**🚨 Preventive Controls**

**For Keyboard/Mouse:**

* Use **Bluetooth** or **wired** input devices
* Disable unused USB receivers
* Keep firmware updated

**For Drones:**

* Use encrypted communication
* Avoid flying in **GPS-spoofable** zones
* Monitor via RF tools like Bastille

**🧠 Final Notes**

* Wireless input hacks are **quiet**, fast, and require **no physical access**.
* Drones are vulnerable due to **lax security + wireless openness**.
* Tools like **Bastille** are emerging to help organizations monitor the **RF spectrum**, which was previously ignored.