ESPKey Demo

View a New & Installed ESPKey
TTP: On-Path Attack or Adversary-In-The-Middle (AiTM)

The ESPKey is an AiTM attack for Wiegand Access control systems. How will you know a system is Weigand? When you pull the badge reader off the wall, you will find small wires of various colors, either immediately or further up the line. The secure alternative is OSDP, with less wires - however this is expensive to install. You will find Weigand more often than OSDP in the wild.

Above: Reader with ESPKey installed (left), and ESPKey on static-proof bag (right)

Step 1: View Installed ESPKey

In the Lab: Use a screwdriver to take the screw out of the reader, and gently remove the cover

Step 2: View the ESPKey

Please do not install the loose ESPKey on the wires.

In the Lab: The ESPKey will be installed inside on the Weigand wires, with LEDs lit up indicating that it's receiving power. The ESPKey reads the cleartext binary data as it passes from the reader to the door controller, captures and stores the data, and creates a Wifi hotspot for you to connect to it and interact with it.

Hold the uninstalled ESPKey up to the wires and see how easy it would be to install. There are tiny letters on the ESPKey indicating which wires should be installed into each channel. You can see how easy it would be to place the wires in the channel and use a punchdown tool to allow the vampire clamps to pierce the plastic and tap the data/power going through the wires.

Please **DO NOT** install the extra ESPKey. They are very difficult to remove and damage our demo hardware.

Step 3: Connect to the ESPKey

In the Lab: We named the Wifi hotspot "ESPKey-88110b" - you can rename them to something less conspicuous if you're in the field. The password is "accessgranted" all lowercase

Once connected, navigate to 192.168.4.1 in your browser (or or http://ESPKey.local)

Try swiping any badge on the reader (it supports both high and low frequency). It should show up on the ESPKey's homepage. If it doesn't, refresh the page. You can click that badge, view the badge data, and most importantly - hit "Transmit" which injects the badge data into the wires.

Please **DO NOT** change the ESPKey configuration or enable DOS mode (it's buggy with the current build - we're working on it).

In the Field: If you install an ESPKey on an exterior reader at a building, you can then:
1) Select "Transmit" from your phone anytime to unlock the door
2) Use the badge data to clone/write a badge using a Flipper Zero or Proxmark
3) Optional: Enabled DOS mode, taking the reader offline. Then you show up as an access control tech and magically fix it. Be careful - it's inconvenient and often unnecessary to take badge readers offline to gain entry. We recommend less disruptive techniques.