VANDERBILT

ACTpro

Card Cloning and Hacking Prevention

ACTpro - Desfire and OSDP for High Security

At Vanderbilt, we believe ACT is one of the simplest access control systems to quote, ever! Just count up the doors and you're done. Sales are easier to make, quotations are more reliable, and complex part lists are a thing of the past.

ACTpro grows with your business

ACTpro secures your business by using the latest DESfire ™ EV1/EV2 cards and readers and Open Source Data Protection (OSDP) protocols to ensure that your cards cannot be cloned and your readers cannot be spoofed.

Sniffing devices

Sniffing devices are now available on eBay. These devices attach to the cable between the reader and the controller and store any valid card transactions. These can then be transmitted to by a smartphone app to replay the number sent to be checked by the controller. Therefore, no card or biometric is then even needed to access the door.
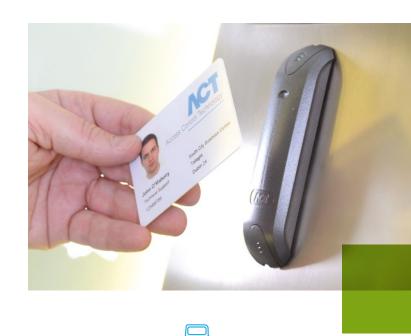
Websites

There are a multitude of websites that will make fake cards for you. The lowest cost and easiest way to quickly copy a simple keycard is to purchase an RFID card ID copier. These can be found on every day popular commercial websites.

Card and reader hacking and cloning examples

The keycard reader is the single most vulnerable point in your entire physical office security setup. 90% of all access control cards in the industry today are easily copied and cloned on the internet. This has created the growing realization that most access control ID systems are now totally open to being compromised and vulnerable to attack.

Card Cloning Devices

Devices are readily available online that will copy a wide range of access control cards from simple proximity to complex smart card formats.

Where ACTEnterprise wins

ACTpro solves these issues by using DESfire EV1/ EV2 cards which have never been able to be cloned or copied, using OSDP card readers which use encrypted communication so they cannot be spoofed.