Market Update | Access Control Vulnerabilities

The C.G. Systems, Inc. team is continually researching and training to stay abreast of changes to the technologies we offer our customers, as well as watching for new technologies that may provide good applications for our current and new customers. Our team is aware of the rise of cloning access control system key-fobs and cards and felt it important to inform our customers of the potential vulnerabilities for many of the legacy access control systems currently installed. For many of our HOA customers, this is not a vulnerability requiring an immediate action. However, it is wise for all our customers to consider a migration path for resolving these vulnerabilities in the future. Below are some links to further your own research:

- Most current Wiegand credentials can now be easily copied/cloned, see the attached websites for more information on cloneable cards and fobs:
  - https://www.key.me/ (you may find one of these kiosks in a store near you)
  - https://www.clonemykey.com/compatible-rfid-key-formats/
- Wiegand communications between card/fob readers and access control panels have become much more vulnerable to hacking, even with high end systems.
  - https://www.forbes.com/sites/thomasbrewster/2018/09/03/googles-doors-hacked-wide-open-by-own-employee/#741693503c7a
- Wiegand BLEKey $35 sniffing device can be permanently installed behind readers in 60 seconds: https://hackerwarehouse.com/product/blekey/

Potential Solutions - Short-term & Long-term:

Unless you are protecting significant secrets or other valuables, many HOA customers will not be extremely vulnerable. However, all customer should begin planning for an OSDP compliant system:

- Step One: Change out card/fob readers to encrypted readers and cards/fobs or Bluetooth smartphone credentials.
  - There are many companies now offering this step one solution, which still utilizes Wiegand communication to the access control panel and thus 'sniffing' the credential information from behind the reader is still possible.
  - **Note:** Step two requires the reader be registered with the actual access control panel for encrypted communications, which means most OSDP compliant systems will require the access control panel and the reader be from the same manufacturer.
- Step Two: Change out the access control panels to new panels that communicate via encrypted RS485 and preferably that are OSDP compliant. Currently only a few manufacturers have their high-level commercial panels developed for this standard.
  - We currently offer completely OSDP compliant systems via the manufacturers of **ICT** and **Kantech**.

If you have any further questions or concerns regarding OSDP compliant access control systems please feel free to contact California Gate at service@cgsystemsinc.com or by phone at **(714) 632 - 8882**. Thank you!