Breaking Access Controls with BLEKey
Most access controls suck.
so we made a thing!
Us

Eric Evenchick
Embedded Systems Architect
Faraday Future
@ericevenchick

Mark Baseggio
Managing Principal Consultant
Optiv
@markbaseggio
Why?
Wiegand

00 0 00
1 11
Card Reader

Upstream aka Door Controller

RF

Wiegand
HID iCLASS

Such enhanced security

So mutual authentication

Very encryption
iCLASS SE
Does anyone use one of these readers?
Wiegand, the man, the protocol, the legacy.
Visualizing Wiegand

DATA0

DATA1

0

1
Wiegand Protocol
Facility Code = 21
Facility Code = 21
Card Code = 29644
Facepalm
Physical Access = Winning
Oops...

Hi Eric,

We have update the firmware successful. But the BLE name is "BLEPenis"?
BLEKey in HID Prox Reader
The Attacks
Record Card Data

1. Alice taps card
2. BLEKey records data
3. Eve recovers data over Bluetooth
4. Eve creates cloned card
Replay Card Data

1. Alice taps card
2. BLEKey records data
3. Eve requests replay from BLEKey
4. Door opens
Reader DoS

1. Eve taps control card
2. BLEKey replays Alice’s card
3. BLEKey pulls both lines low to DoS
4. Nobody can use the reader until timeout occurs
1. Eve installs BLEKey in Maxi Prox reader
2. Eve hides reader in book bag or back pack
3. Eve skims cards.
OMG
REALLY!!!
Tamper Detection FTW
Logging
Video Surveillance
In closing.
So thanks, eh?

@ericevenchick
eric@evenchick.com

@markbaseggio
mark@basegg.io