

Explore with CEM

Physical Access Control

End to End Security : Card Cloning

Ian Schofield

Introduction

- About CEM
- Security components
- Issues & Concerns
- Card Cloning & Security
- Signal Cloning
- Solutions



KANTECH



SOFTWARE HOUSE



DSC



CONNECT24



Tyco International
Focus: Vital Products and Services
100K+ employees, 60 Countries



Tyco Security Solutions
Focus: Industry Leading Security Products, Services and Solutions
64K+ employees



SOFTWARE HOUSE



KANTECH



CONNECT 24



DSC

Unified Group of World-Leading Access Control, Video, and Intrusion Brands

Securing the people, places, things that are vital to us



Aviation



Gaming, Sports & Leisure



Healthcare



Industrial/Manufacturing



Oil & Gas



Ports/Maritime/Transportation



Education



Government



Financial/Banking



IT/Telecom/Professional Services



Retail



Residential

Access Control



KANTECH™

SOFTWARE HOUSE™

Video



Intrusion

DSC®

SUR-GARD®



Security components

- Policies, processes, and technology to manage identities and access to resources

Security Components

Control Environment

Risk assessment

Policies &
Procedures

Training &
Awareness

Compliance, Audit &
Effectiveness
Monitoring

Physical Security

Perimeter

Entry/Exit

Identification

Monitoring &
Response

Information Technology

Rights Administration

Network LAN, WAN,
WLAN

Anti-Virus &
Firewalls

Disaster Recovery

Control Environment



Risk assessment

- Document & regularly re-assess risks, severity & impact
- Avoid, Transfer, Mitigate, Accept, Escalate, Monitor
- Prioritise improvements, schedule and assign
- e.g. PACS trends monitoring & heat maps



Policies & Procedures

- Roles and responsibilities including checks & balances.
- PACS Credential Workflow, Incident Response, Monitoring
- IT : Change control, remote access, rights management, & passwords
- HR, : Screening, Training, T&Cs, Disciplinary process



Training & Awareness

- New hire and annual training, internal communication and toolbox talks
- Visitor management & Contractor conditions
- Use onsite, or even Online web based training



Compliance, Audit & Effectiveness Monitoring

- Build Workflow checkpoints into the process
- Security dashboards and reports
- Third party policy registrations. Monitor and control breaches (e.g. CEM BoC module)
- Log incidents, identify & validate control measures

Control Environment

Risk assessment



- Document & regularly re-assess risks, severity & impact
- Avoid, Transfer, Mitigate, Accept, Escalate, Monitor
- Prioritise improvements , schedule and assign
- e.g. PACS trends monitoring & heat maps

Policies & Procedures



- Roles and responsibilities including checks & balances.
- PACS Credential Workflow, Incident Response, Monitoring
- IT : Change control, remote access, rights management, & passwords
- HR, : Screening, Training, T&Cs, Disciplinary process

Control Environment

Training & Awareness



- New hire and annual training, internal communication and toolbox talks
- Visitor management & Contractor conditions
- Use onsite, or even Online web based training

Compliance, Audit & Effectiveness Monitoring



- Build Workflow checkpoints into the process
- Security dashboards and reports
- Third party policy registrations. Monitor and control breaches (e.g. CEM BoC module)
- Log incidents, identify & validate control measures

Physical Security



Perimeter

- Establish a buffer zone appropriate to the threat. e.g. 8ft+ fence with clear zones & additional measures such as barbed wire. Confirms intent and framework for monitoring.
- Integrate centrally security monitoring with CCTV & fence intrusion detection system
- Consider gates, future construction, safety evacuation and environmental requirements



Entry / Exit points

- Guards, man-traps, and turnstiles with anti-passback or interlocking at staff channels
- Daily, logged patrols to verify operation. Ideally using Integrated PACs guard-tour
- Time-zones to control access. Lockdown when not in use e.g. CEM Locked-Out feature
- On emergency exits, delayed/alarmed egress may be appropriate



Identification

- Visitor management process. Early application, ID policy, sponsors/escorts, logging, limited passes. e.g. one-time passes
- Visible ID with zone colour and eyes everywhere challenge protocol
- Clearly distinguish permanent staff, contractors and visitors

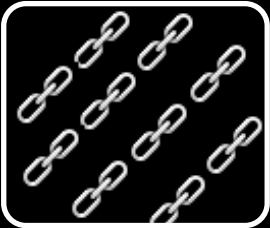


Monitoring and Response

- Route all relevant alarms to a central location
- Use sensors appropriate to the environment and CCTV to minimise false alarms
- Prioritize the Primary Security Line
- Develop, document and train for escalation & response

Physical Security

Perimeter



- Establish a buffer zone appropriate to the threat. e.g. 8ft+ fence with clear zones & additional measures such as barbed wire Y. Confirms intent and framework for monitoring.
- Integrate centrally security monitoring with CCTV & fence intrusion detection system
- Consider construction, evacuation and environment

Entry / Exit points



- Guards, man-traps, and turnstiles with anti-passback or interlocking at staff channels
- Logged patrols to verify operation.- Integrated PACs guard-tour
- Time-zones to control access. Lockdown when not in use e.g. CEM Locked-Out feature
- On emergency exits, delayed/alarmed egress may be appropriate

Physical Security

Identification



- Visitor management process. Early application, ID policy, sponsors/escorts, logging , limited passes. e.g. one-time passes
- Visible ID with zone colour and eyes everywhere
- challenge protocol
- Clearly distinguish permanent staff, contractors and visitors

Monitoring and Response



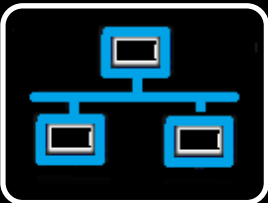
- Route all relevant alarms to a central location
- Use sensors appropriate to the environment and CCTV to minimise false alarms
- Prioritize the Primary Security Line
- Develop, document and train for escalation & response

Information Security



Rights Administration

- Establish workflow and full audit trail for access requests and use two-step authorisation
- Limit authorisations by time, location and duration
- Automatically “park” unnecessary credentials
- Implement 3s’ (something you have, ...know,are)



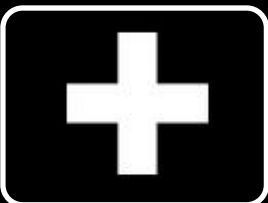
Network LAN/WAN/WLAN

- Segregate security LAN and physically secure end-points
- Consider Denial of service (syn/smurf...),, Interception, Social engineering
- Use subnets, firewalling, & switch security – don’t talk to strangers. Do you really need WLAN?
- Encrypt



Anti-Virus & Firewall

- Use automated mechanisms to make sure anti-virus is always up to date
- Restrict access to workstation USB ports’
- Use a server with rugged operating system



Disaster Recovery

- Identify the threats, locate each single point of failure and response actions incl. vendor support
- Deploy, maintain and test UPS
- Use appropriate server hardware with redundancy features, and failover to remote location
- Verify your backup, make multiple contemporary copies, and keep them safe !

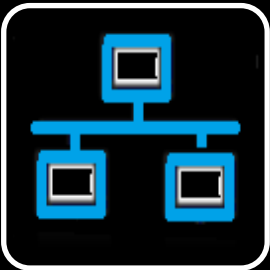
Information Security

Rights Administration



- Establish workflow and full audit trail for access requests and use two-step authorisation
- Limit authorisations by time, location and duration
- Automatically “park” unnecessary credentials
- Implement 3s’ (something you have, ...know,are)

Network LAN/WAN/WLAN



- Segregate security LAN and physically secure end-points
- Consider Denial of service (syn/smurf....),, Interception, Social engineering
- Use subnets, firewalling, & switch security – don’t talk to strangers. Do you really need WLAN?
- Encrypt

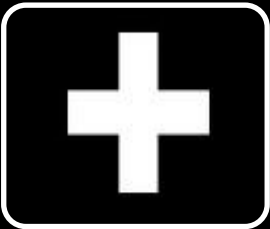
Information Security

Anti-Virus & Firewall



- Use automated mechanisms to make sure anti-virus is always up to date
- Restrict access to workstation USB ports'
- Use a server with rugged operating system

Disaster Recovery



- Identify the threats, locate each single point of failure and response actions incl. vendor support
- Deploy, maintain and test UPS
- Use appropriate server hardware with redundancy features, and failover to remote location
- Verify your backup, make multiple contemporary copies, and keep them safe !

Workstation Security

- House of Commons IT security compromised by a six year old schoolgirl from Winchester BBC Mar'07



Two years of storage
Automated emails over
wireless access point



System Security

- **Social**
 - “More than 70% of people would reveal their computer password .. for a bar of chocolate”
Infosecurity Europe Survery 2004
- **Network**
 - Open Sesame! Network Attack Literally Unlocks Doors Wired Aug 2009
 - RFID Hack Can Unlock Your Doors With Android Phones IBT Mar 2011
- **Signal : Cloning Wiegand**
 - “Open Sesame: Access Control Hack Unlocks Doors” Wired Aug 2007

Card Security

- “Proximity card spoofer” Hackaday Feb’06
- “MiFare RFID crack explained” Computerworld Mar’08
- “Legic Prime: Obscurity in Depth” CCC Dec’09
- Smartcard “Security demystified” OpenPCD Feb’11



Could you be
a victim of
card cloning?

Card Cloning

Card Cloning refers to the copying of an access control card or fob in order to compromise electronic door security on an access control system.

Sometimes referred to as 'card spoofing', a device is introduced to either duplicate a card or impersonate it.



Card Cloning Devices

- Palm sized devices can learn a Valid card number.
- They can then replay the card number at the reader or write to a blank card.
- Appears to system as a valid card number.
- Devices freely available on the internet.
 - From \$100-\$300.



Cloning Video

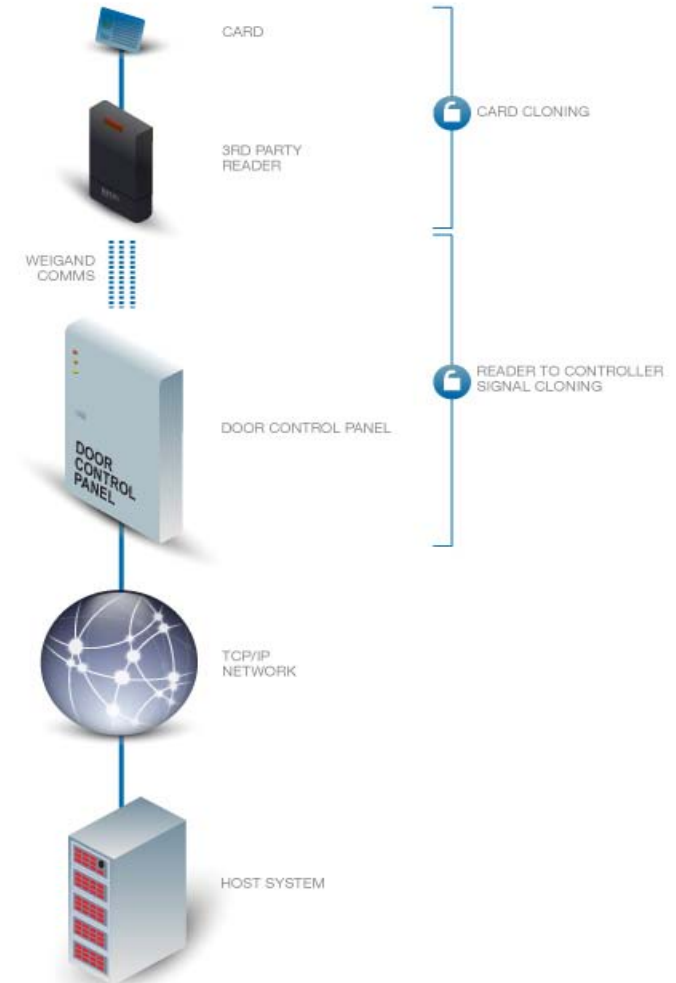


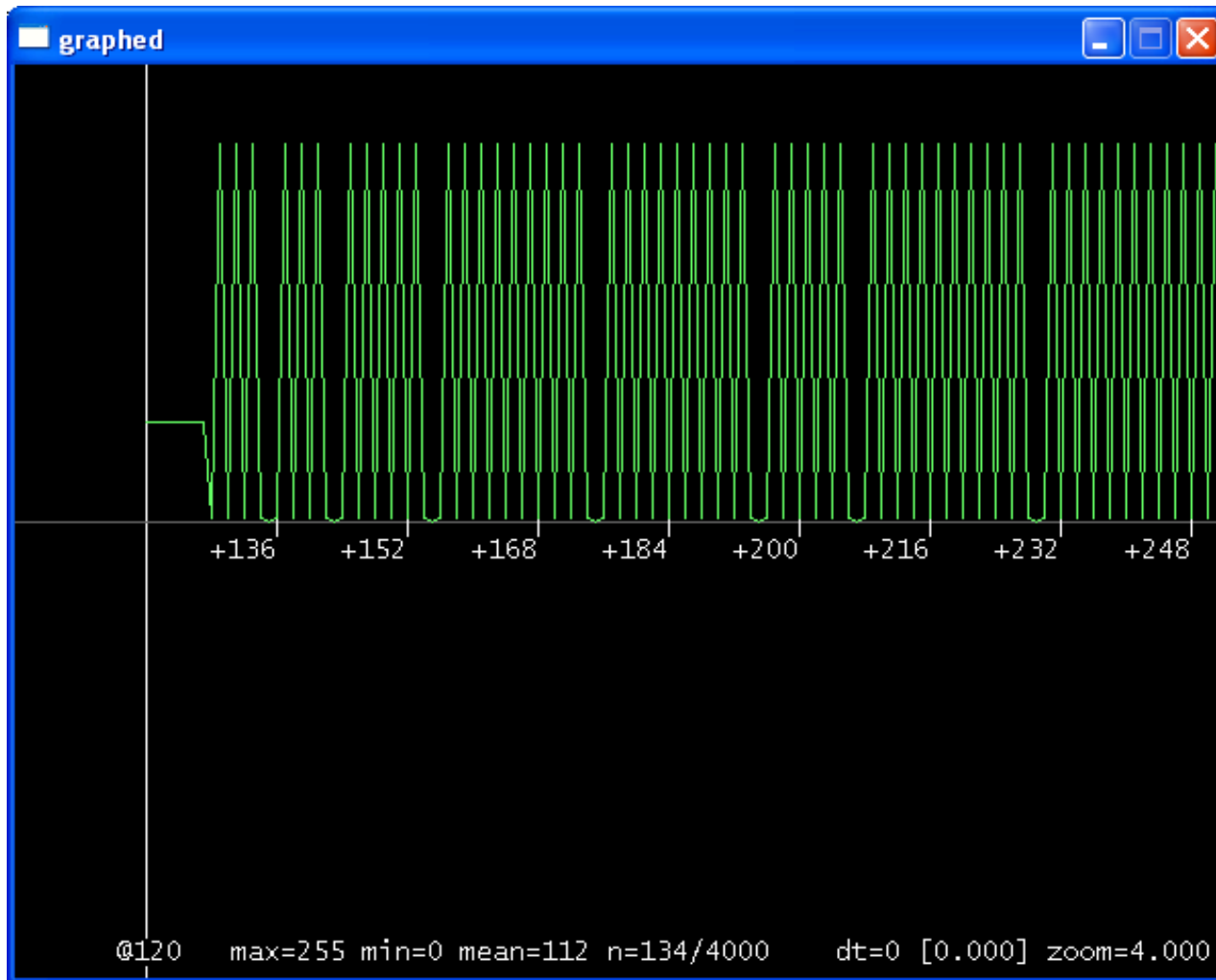
Truly portable, selectable frequencies and antennas.

Attack Sites

- Between the card and the read head.
- Between the reader and the panel.
- Between the panel and the host server.

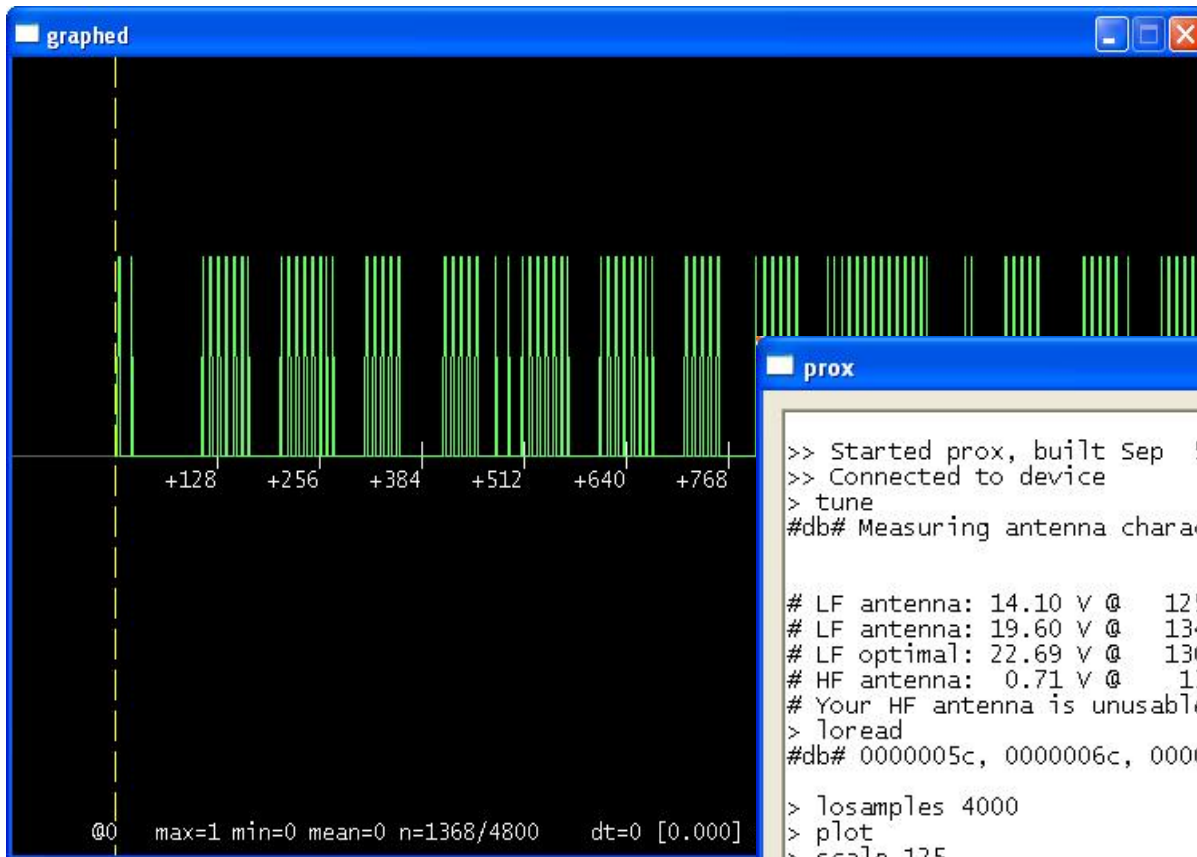
Typical Cloning Dangers





Captured MiFare
13.56Mhz CSN

How far ?
From 10metres



```
prox
>> Started prox, built Sep  5 2009 16:26:21
>> Connected to device
> tune
#db# Measuring antenna characteristics, please wait.

# LF antenna: 14.10 V @ 125.00 kHz
# LF antenna: 19.60 V @ 134.00 kHz
# LF optimal: 22.69 V @ 130.43 kHz
# HF antenna: 0.71 V @ 13.56 MHz
# Your HF antenna is unusable.
> lread
#db# 0000005c, 0000006c, 00000000

> losamples 4000
> plot
> scale 125
> hiddemod
```

125KHz capture (FSK)

Ready for playback

No Laptop required !

Smart card Security

- Authentication
- Channel Encryption
- Diversification
- Physical security



Card & Reader Authentication

- Mutual Three Pass Authentication

Reader and Card both know the **Key** = Trust

→ Send Key number

← Return Cipher (**random[B]**, **Key**)

Decipher with **Key** to get random[B] (reader knows card secret)

→ Send Cipher (**random[A]** + **random[B]**)

Decipher with Key to get random[A] (card knows reader secret)

← Return Cipher (**random[A]**, **Key**)

Trust established

Secret : Shared **Card** **Reader**

Channel Encryption

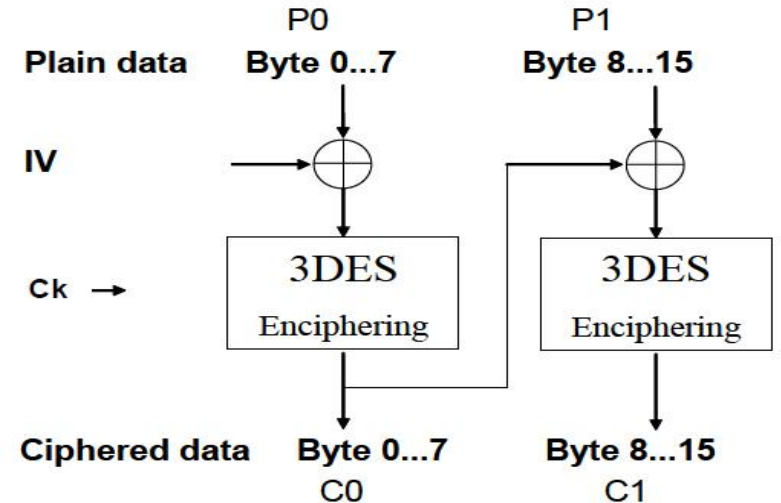
- Encrypted Session based Security
 - Session Key derived in Authentication phase
 - All data encrypted by Session Key
 - Secure pipe for all data between the card and reader
 - Prevents eaves-dropping

Privacy assured



Diversification

- Card specific keys
- Harder to hit moving target
- Reduce vulnerability
- Customer & Site specific



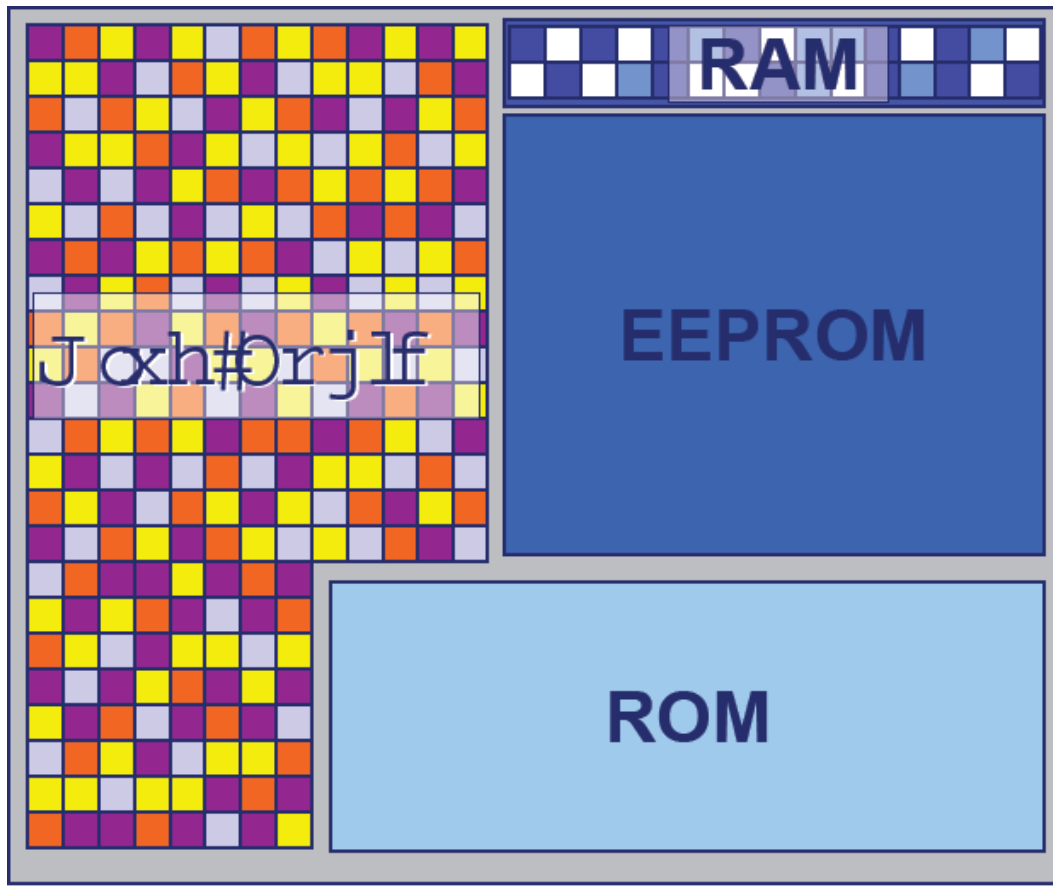
$m = (n+1)/8 - 1$; where m and n are integer

p = plain 8-byte block

C = ciphred 8-byte block

Unique

Physical Security On-Chip



- Functional blocks hidden
- RAM and CPU fully scrambled
- No System Bus to intercept
- Multi-layer design helps prevent reverse engineering
- Ideally CC EAL Proven

Signal Cloning

Reader to door controller signals can be copied by recording or 'sniffing' the pulses, (wired or wireless) between a card reader and its control panel.

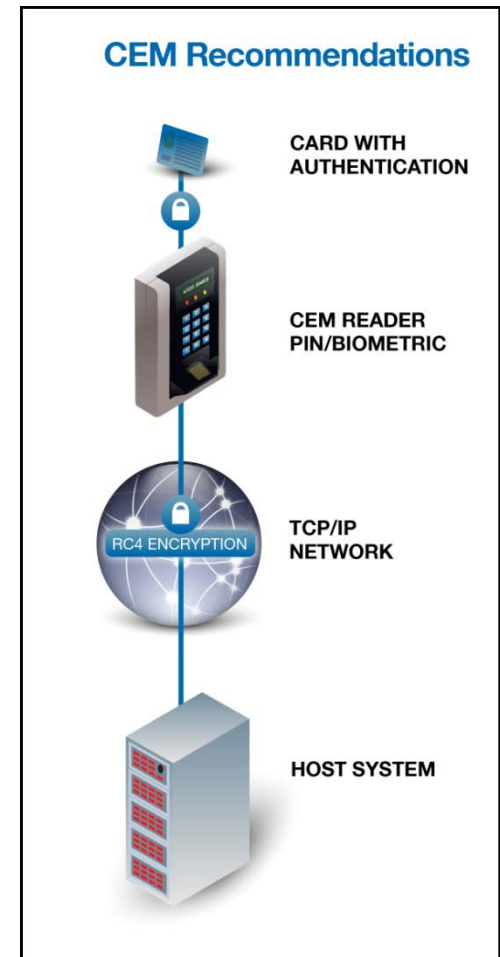
The recorded pulses are then played back to fool the system into thinking a valid card was presented, compromising door security on the access control system.

How does it work?

- The GSM based device is fitted across the 3 wiegand wires.
- A card is swiped and an SMS message is sent to a mobile phone.
- The device buffers a set of card numbers.
- The mobile phone sends the open command back along with a card number.
- If the door does not open, a different stored number is sent.
- Door opens.

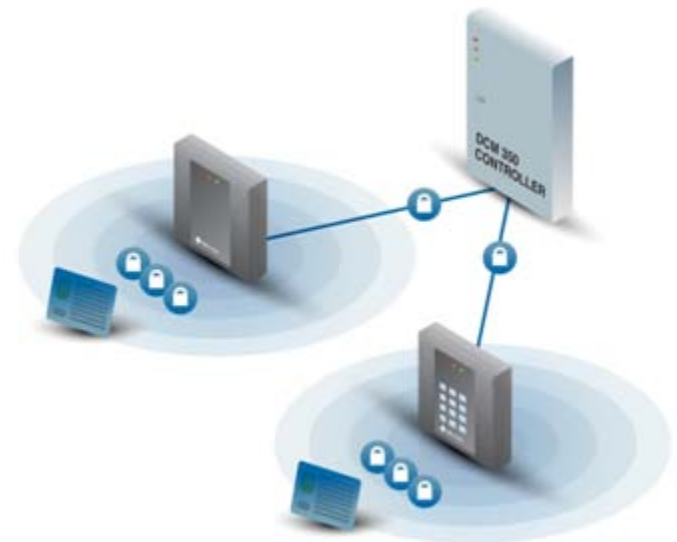
Advice & Solutions

- Use smart card cards with industry approved authentication and encryption such as DESfire, and PicoPass.
- Use readers capable of two or three factor authentication:-
 - Use Card and PIN verification or
 - Use Card and Biometric verification or
 - Use Card, PIN and Biometric Verification
- Use Video Verification.
- Use readers with Tamper Protection.
- Where a traditional panel approach is required, specify that the communications between the read head and the door controller unit must be secure.



Solutions : CEM DESfire Panel

- Encrypted 2 Door Controller – DCM350
- sPass DESfire Smartcard Reader
- CEM DESfire EV1 Pre-personalised Smartcard



Encrypted Door Controller - DCM350

- Encrypted LAN
- One or Two-door.
- RS485 connections for two **sPass** readers.
- Off Line Database.
- Board Only option.



Secure card reader - sPass



- Secure RS485 serial communications between reader & DCM 350 controller
- Low cost, DESFire smart card reader.
- 3DES (Triple DES) encryption.
- Option for keypad or no keypad.

CEM Smart card

- Contactless smart card.
- 3DES (Triple DES).
- Pre-personalised.
- 2-8K bytes EEPROM:-
 - 28 applications.
 - 16 or 32 files per application.
- 4cm Read Range (13.56MHz).
- Fully ISO / IEC 14443 A 1-4 compliant.
- For use with CEM S610 and sPass Reader range.

Mifare DESFire EV1



Example Uses



Advanced Public Transport



Access Control



Smart Card

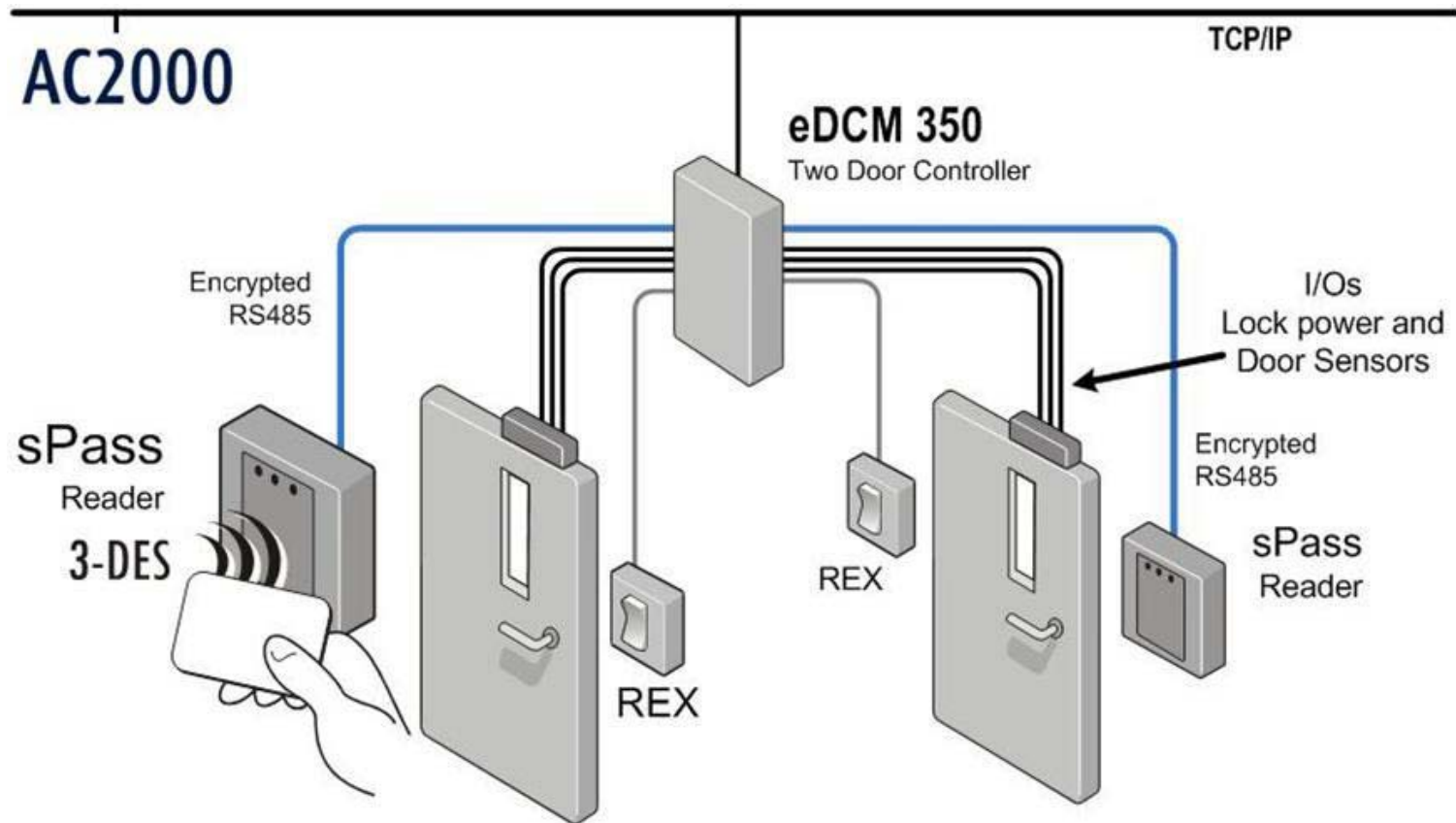


Cashing Vending



Loyalty Programmes

Example Topology



Explore with CEM
Physical Access Control
End to End Security

Ian Schofield

THANK YOU!



Could you be
a victim of
card cloning?