Your Smartcard is Dumb

A Brief History of Hacking Access Control Systems

Shortman
chad@allthenticate.com

Founder and CEO of Allthenticate

Outline

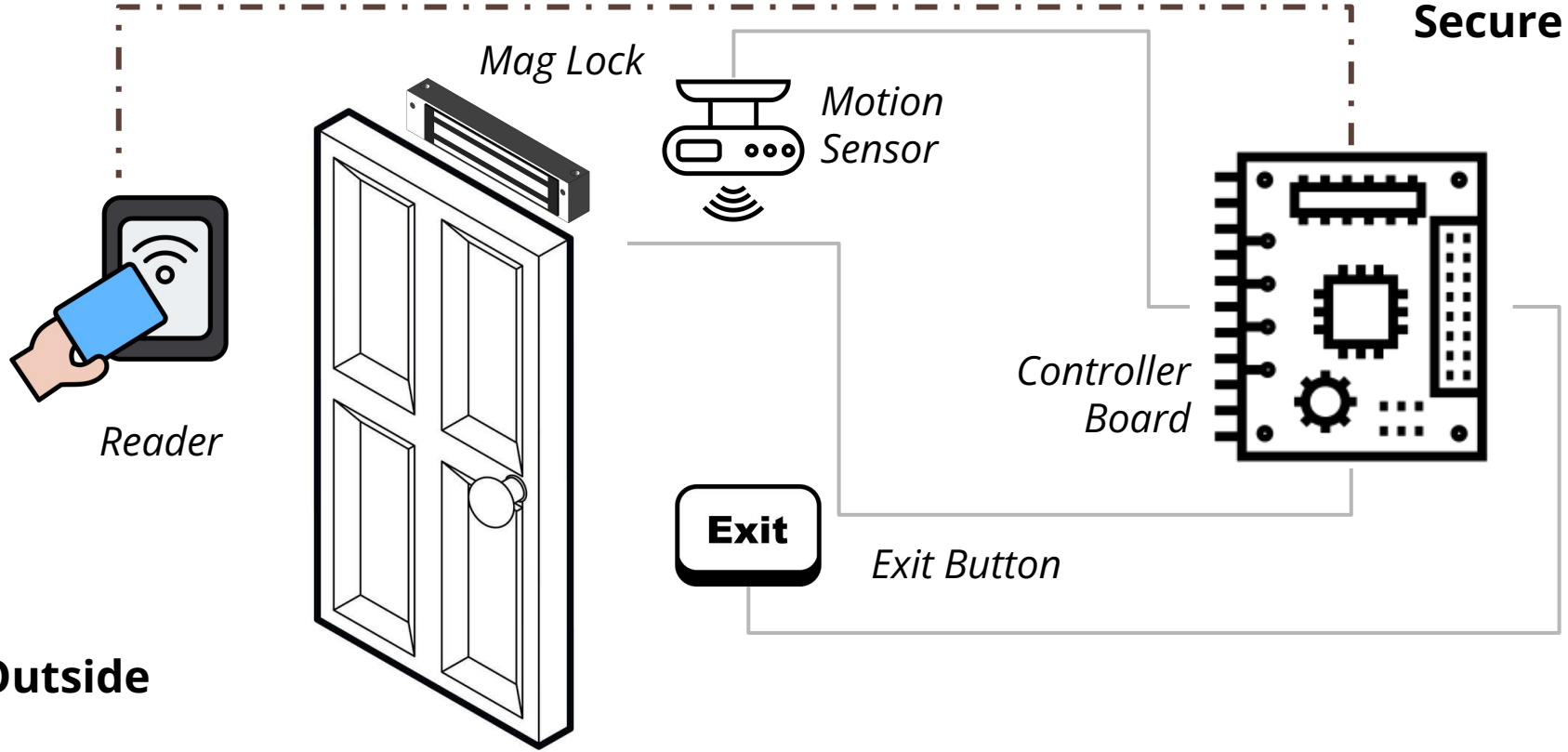
Allthenticate

- Access Control 101
- What is a “smartcard?”
- Ok, got it. How do we break it?
- Can we do better?

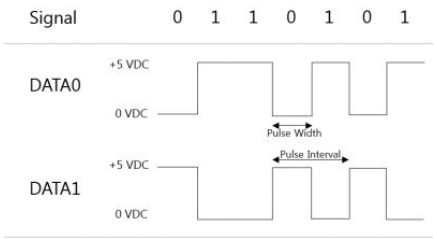


Access Control 101

Allthenticate



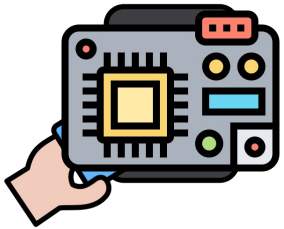
Access Control 101

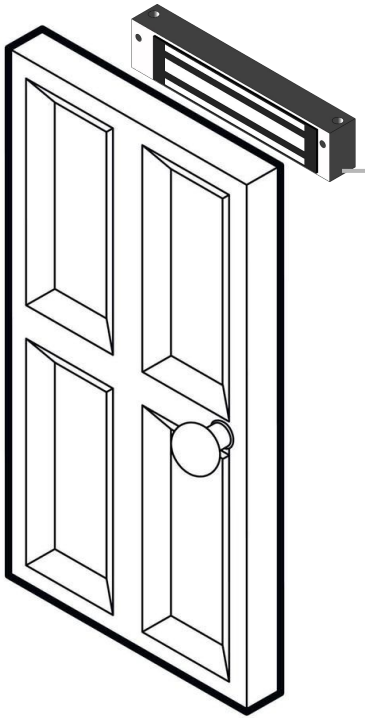


Allthenticate

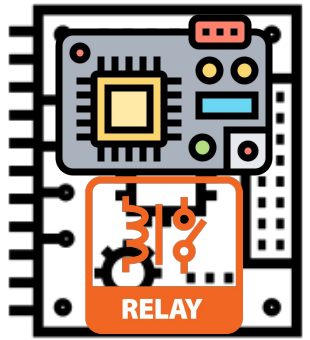
Secure Side

Wiegand (Unencrypted)









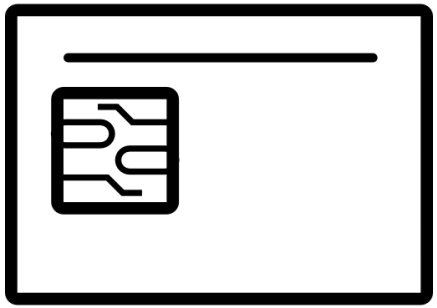


Outside

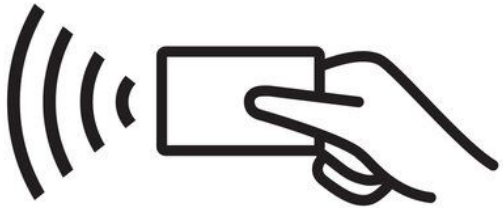
What is a smartcard?

Allthenticate

It looks something like this:



or

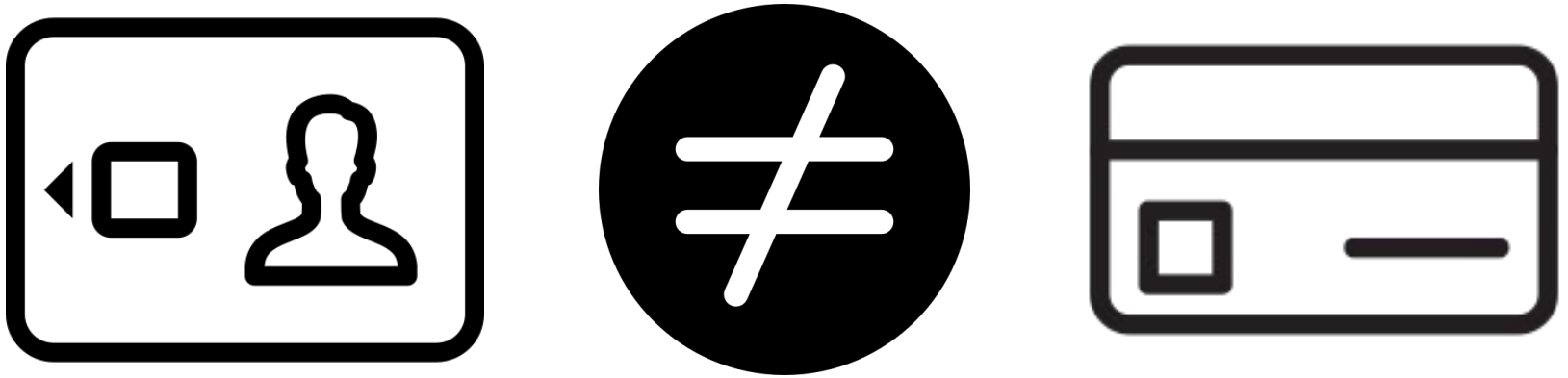


or



Not all smartcards are created equal

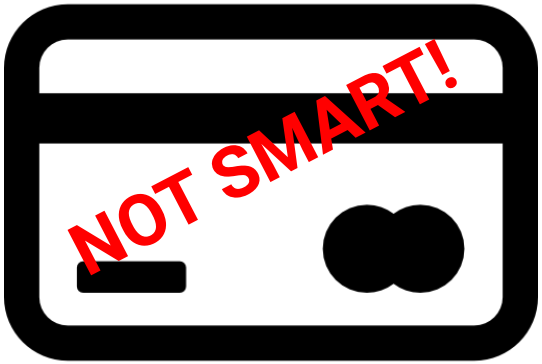
Allthenticate



Credit Cards (magstripe)

Allthenticate

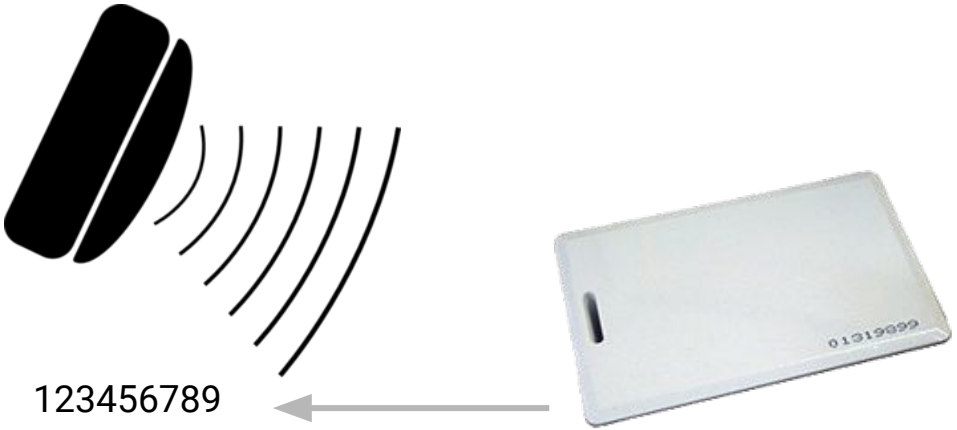
Simply store the information that is on the card



Simple Proximity Card (125 kHz)

Allthenticate

Anyone can read the data



Data has always been transferred in an **unencrypted** form with the prox card credentials. Card readers were designed to communicate small sets of data typically in **8-16 digit card numbers**.

https://willelectronics.com/why-125-khz-prox-cards-are-unsecured/

Proximity Cards (memory cards)

Allthenticate

Used to store a receive data, typically using **symmetric encryption**





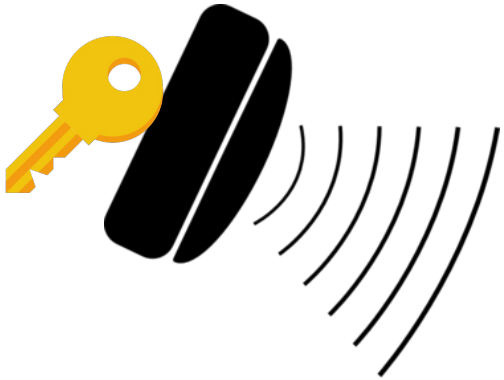




Encrypted Proximity Card (13.56 MHz)

Allthenticate

Shared key must be used to read data



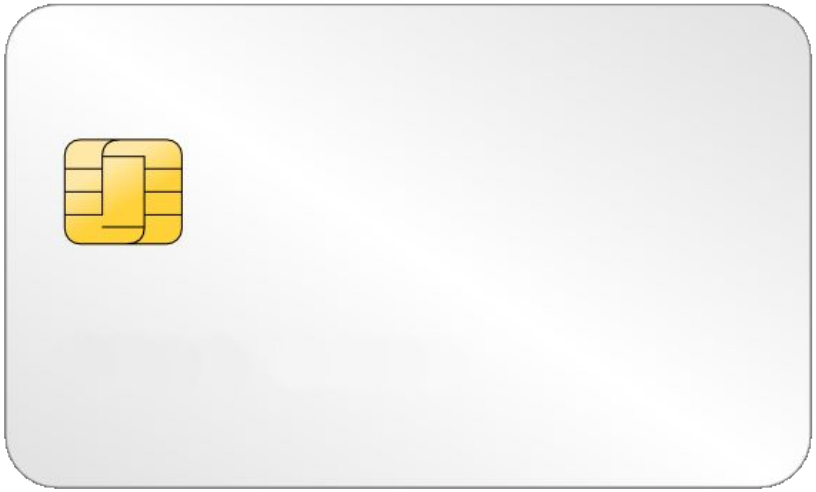
123456789



Smartcards

Allthenticate

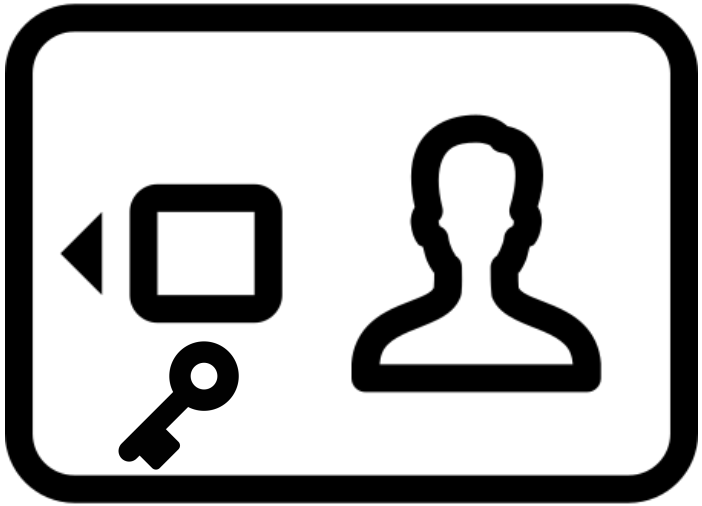
Contain a computer: *CPU, Memory, Operating System (Java)*



Smartcards (asymmetric encryption)

Allthenticate

The private key never leaves the card and is used to *sign* messages



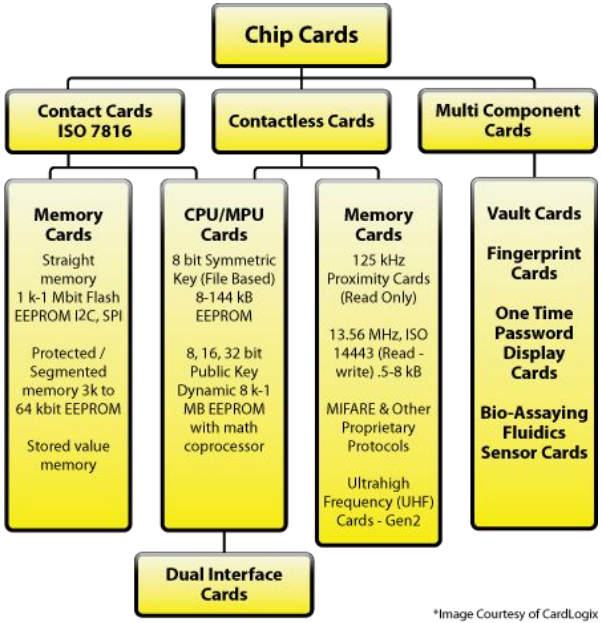




What's in a smartcard chip?

Allthenticate

A little computer embedded in plastic



How do smartcards work?

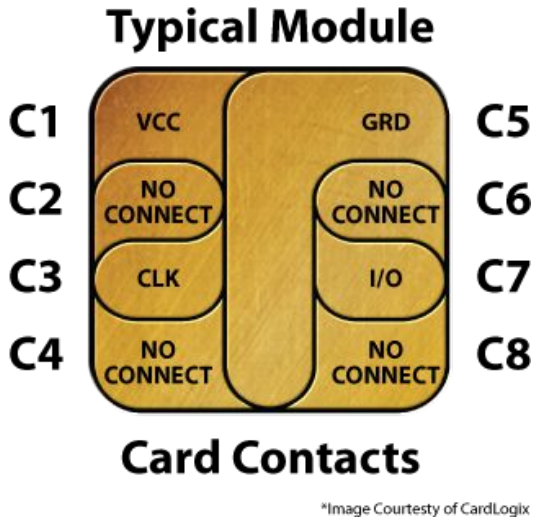
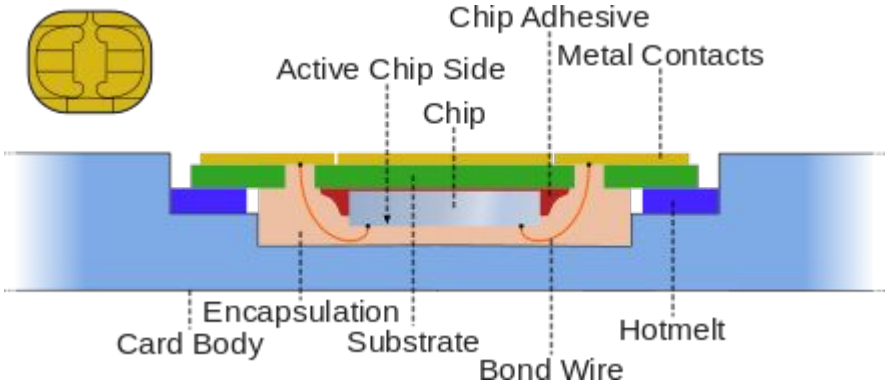


*Image Courtesty of CardLogix



Why do we have smartcards?

Allthenticate

Passwords aren’t great

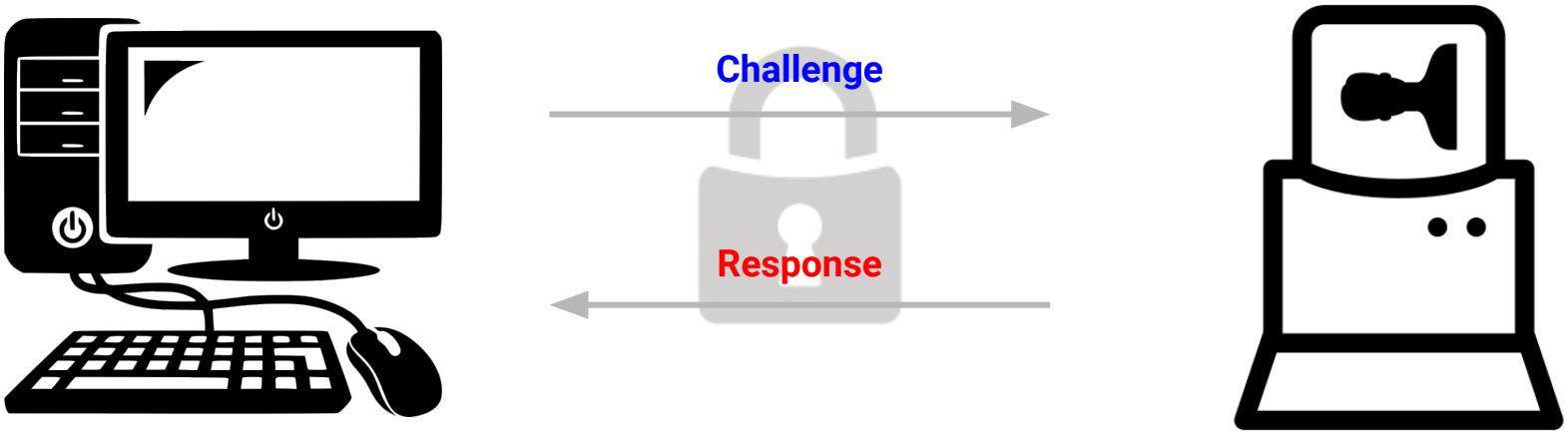
Carrying a full computer is complicated (or used to be)

They can be “something you have”

> *Users can be authenticated by something they **have, are**, or **know***

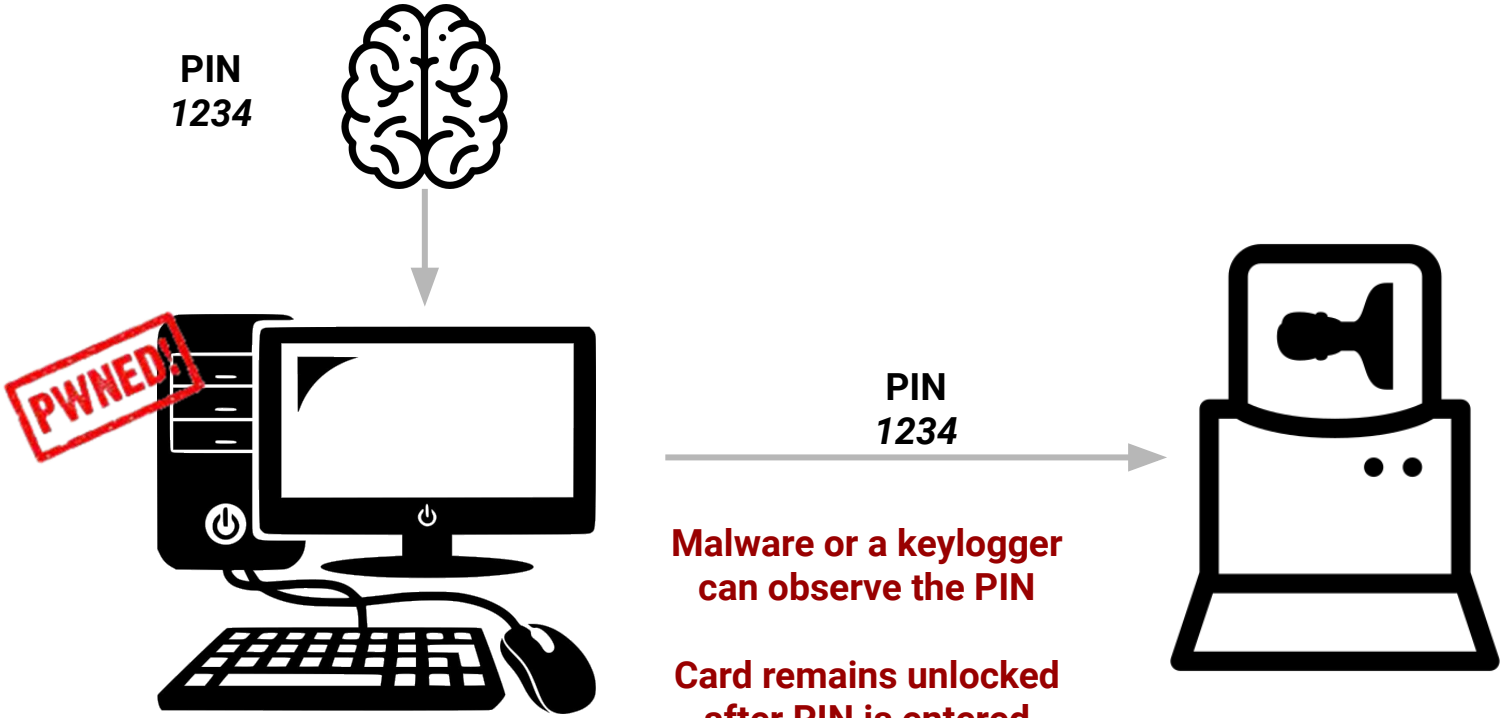
Are they actually better?

Allthenticate



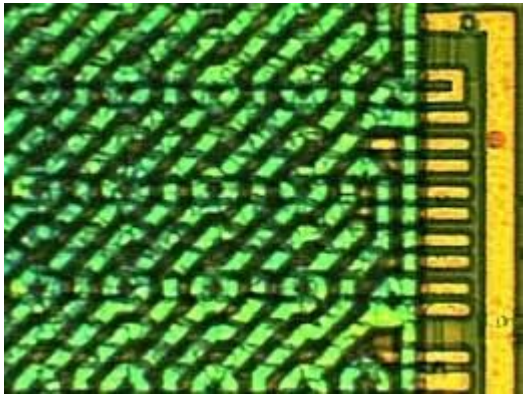
Are they actually better?

Allthenticate

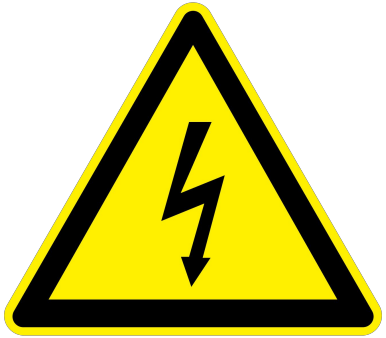


Physical tamper resistance

Allthenticate



Mesh of contacts that will “destroy” the chip if breached



Brownout detection for voltage glitching

```
if PIN == STORED_PIN:
    unlock();
else:
    failed_attempts++;
```

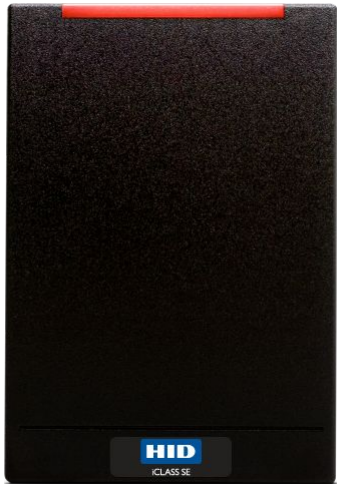
NOT SMART!

```
pin_attempts++;
if PIN == STORED_PIN:
    unlock();
```

Fault-resistant software

Who uses smartcards?

Allthenticate



Physical Access Control



Digital Authentication



Device Identification

What’s the worse that can happen?

Allthenticate

Using the card without the user’s permission

Cloning the smartcard

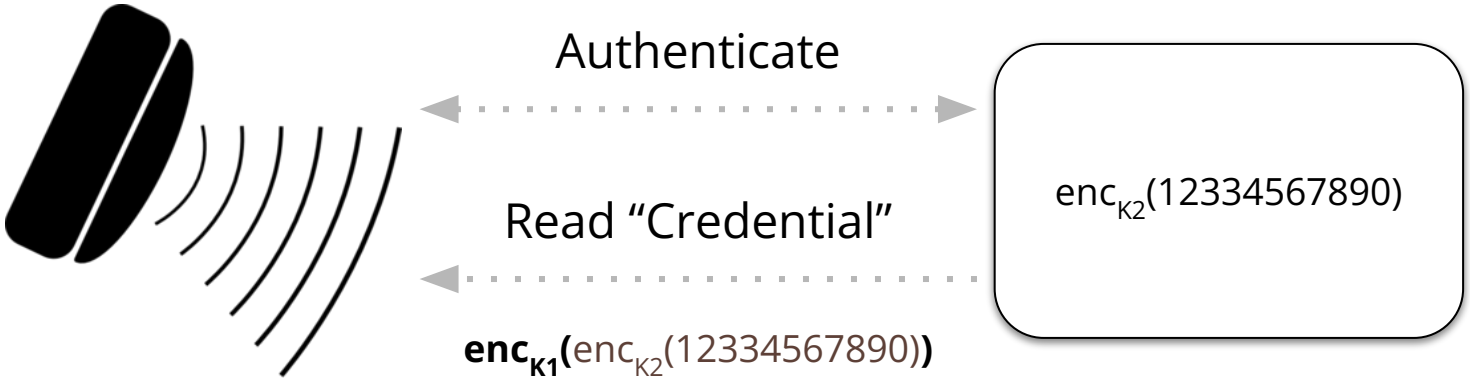
Subverting the need for a card all together

Allthenticate

Ok, let's break it down

K1: In-transit Key

K2: At-rest Key



How do we break it?

Find that dang key!



Smartcard Attacks: Mifare

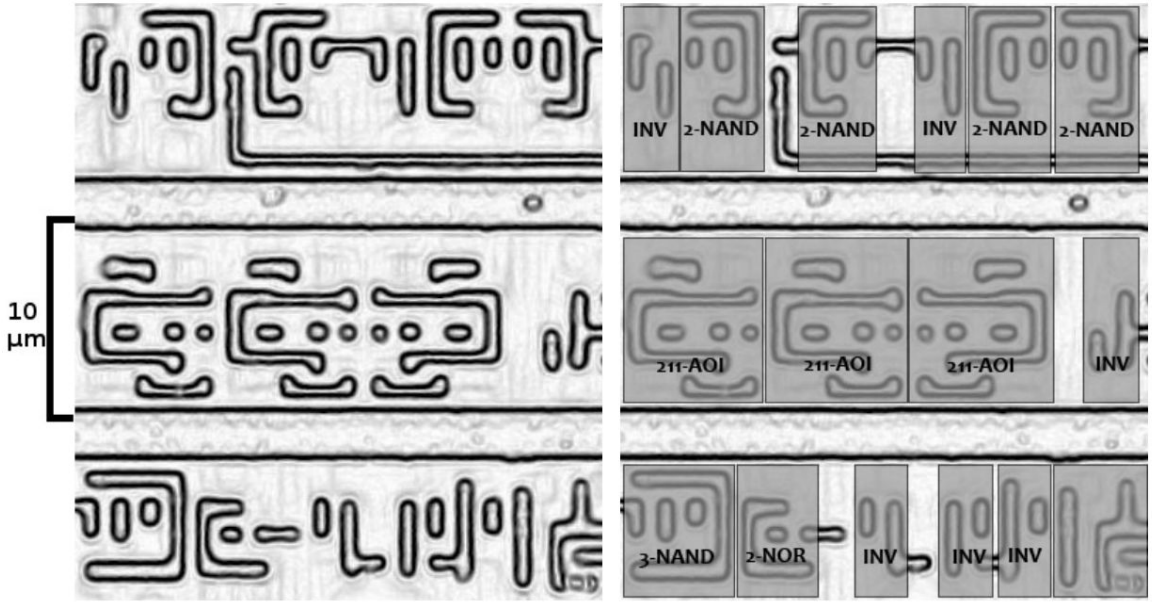
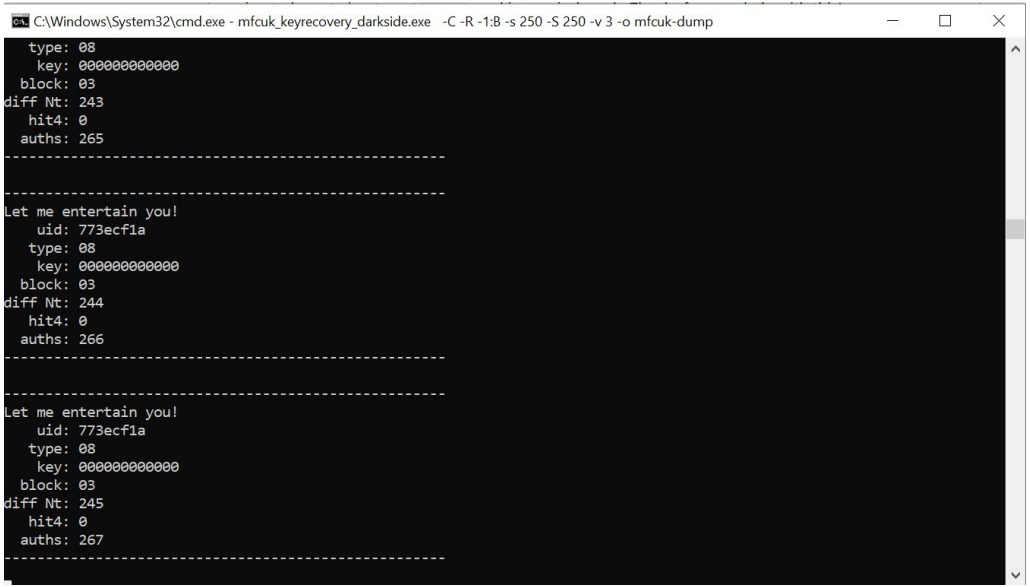


Figure 1: (a) Source image of layer 2 after edge detection; (b) after automated template detection.

Smartcard Attacks: Mifare

Allthenticate

Result: Mifare cards can be trivially cloned with a tool: *mfcuk*



Smartcard Attacks: HID (Normal)



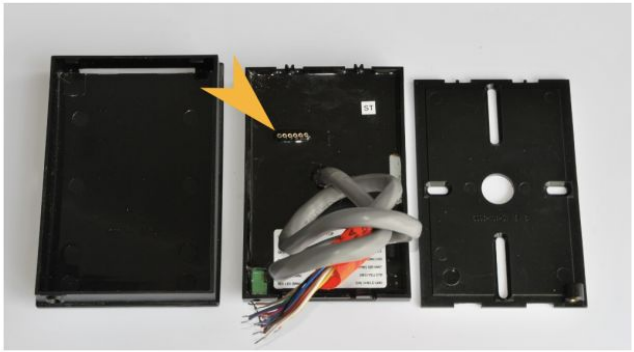
What if this key were leaked?

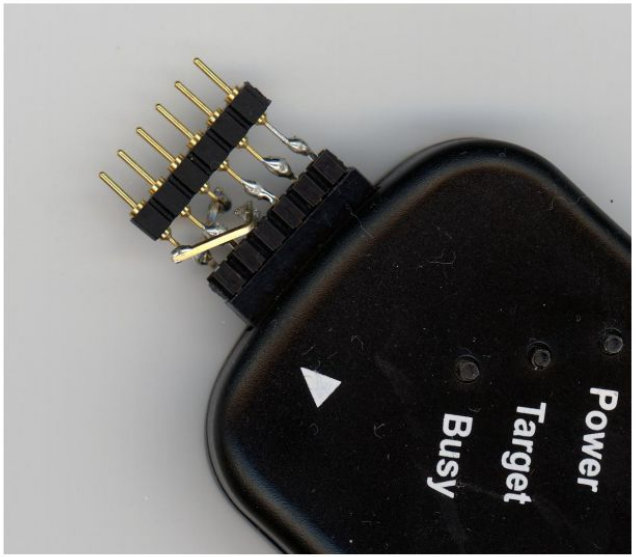


Allthenticate

Smartcard Attacks: HID (Normal)

Heart of Darkness: exploring the uncharted backwaters of HID iCLASS





Smartcard Attacks: HID (Elite)

Elite mode enables *customer-specific* keys

See: *Dismantling iClass and iClass Elite*

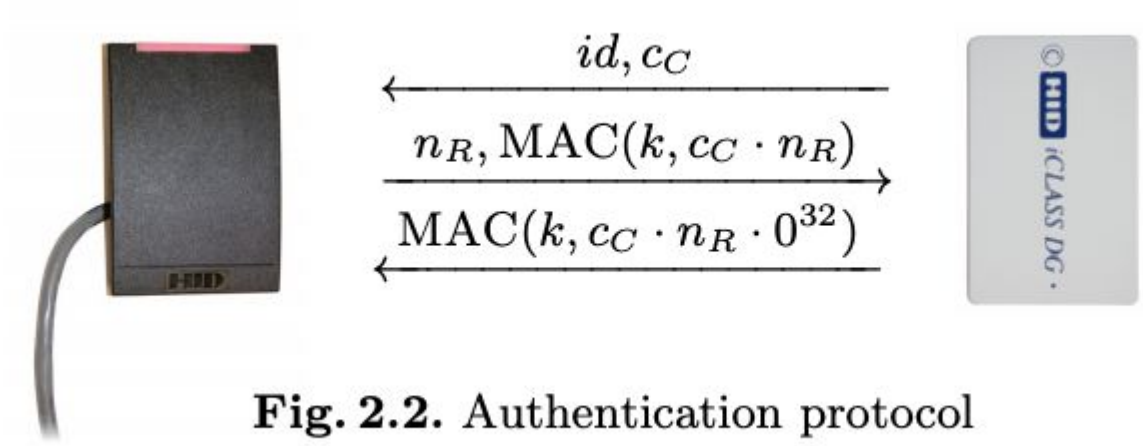


Fig. 2.2. Authentication protocol

Allthenticate

People are “Flipping” out



What do these attacks have in common?

Allthenticate

Bad implementation

Otherwise, smartcards have been one of the most secure mechanisms that we have



Why don’t we use smartcards more then?

Allthenticate

They do not scale well: one smartcard for every service

They require extra hardware: you need a smartcard reader

They lack a user interface: they can only be “something you have”

Can we do better?

Allthenticate



Imagine, a super smartcard

Allthenticate



Secure Elements

Allthenticate

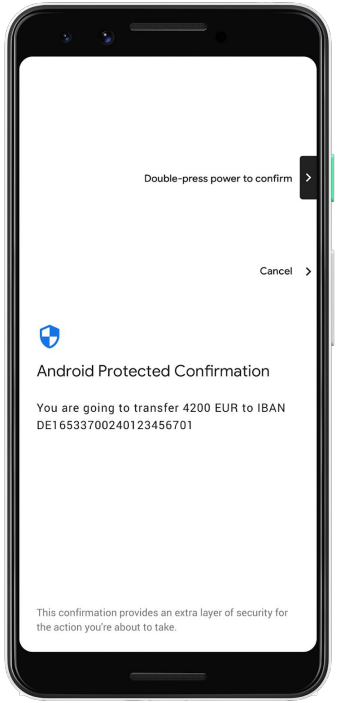
Smartphones already have smartcards onboard



Trusted Execution Environment

Allthenticate

They can even provide a secure, trusted interface



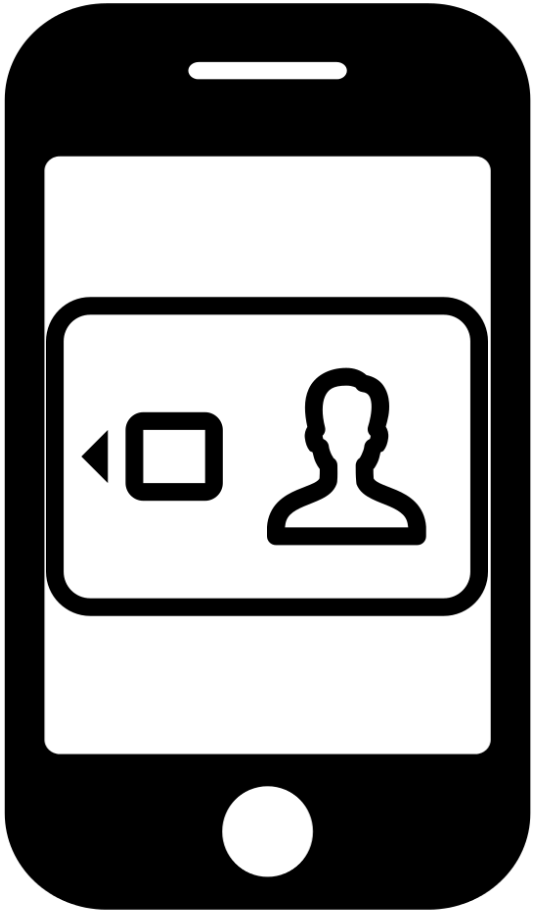
The Future

Allthenticate

Trusted interaction with humans

Capable of interacting with anything

Can replace everything in your wallet



ALL-IN-ONE ACCESS CONTROL AND AUTHENTICATION SOLUTION.



Use a secure credential on your smartphone for *everything*.

www.allthenticate.com

JOIN THE ALLTHENTICATION REVOLUTION



