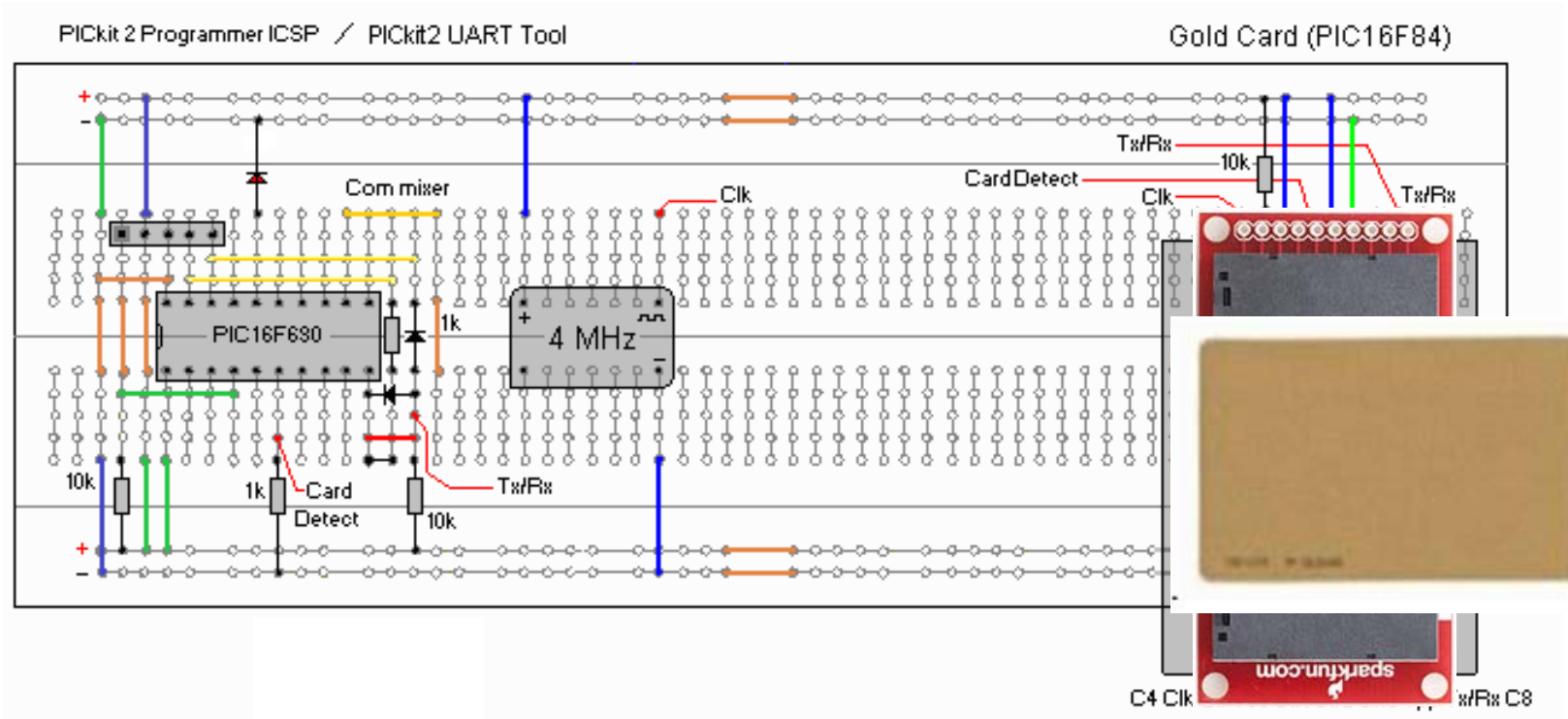
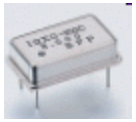
SmartCard laboration



William Sandqvist william@kth.se

Två processorer

SmartCardet innehåller en processor av typen **16F84A**. Den processorn saknar både inbyggd oscillator och seriekommunikationsenhet. Seriekommunikationen är därför programmerad med ”BitBanging”, och kortet använder en yttre oscillatorkrets.



På kopplingsdäcket sitter en processor av typen **16F690**. Den har inbyggd oscillator och inbyggd seriekommunikationsenhet.

William Sandqvist william@kth.se

Programmera SmartCardet

Programmera SmartCardet
med PICKit2-programmet

William Sandqvist william@kth.se

”Kommunikationscentral”

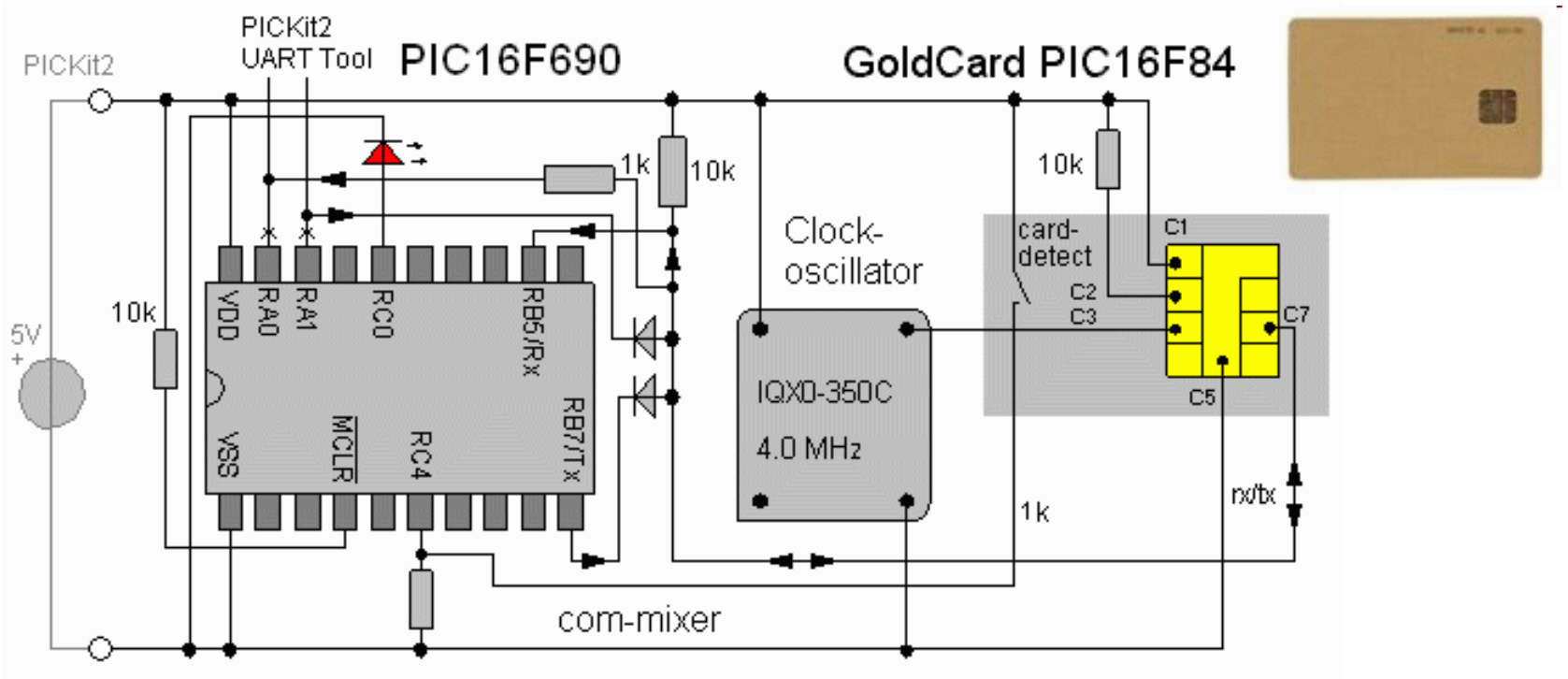
På kopplingsdäcket har vi byggt en ”**kommunikationscentral**” (De två dioderna bildar en diodgrind).

För att underlätta felsökning i programmen kan nu all kommunikation mellan PIC-processorn och SmartCardprocessorn övervakas med PICKit2 UART Tool. Om kortet inte säger något, kan Du fylla i det den skulle ha sagt från PC:ns tangentbord (”man in the middle”).

William Sandqvist william@kth.se

Kommunikationscentralen

”SmartCard” Lås och Nyckel



William Sandqvist william@kth.se

Att programmera två processorer

Du kommer att omväxlande använda PICKit2 för SmartCardet och Skolprocessorn 16F690.

Viktigt. Varje gång Du byter anslutningen till den andra processorn skall Du använda ”**Tools**” ”**Check Communication**” så att PICKit2 vet *vilken* processor som är ansluten.

- Det är *jobbigt* att omväxlande programmera två processorer!

- (Det är ändå jobbigare att programmera 64 processorer!)

William Sandqvist william@kth.se

”Lås” och ”nyckel”

Programmen: **`smrtlock.hex`** och **`smartkey.hex`**

När Du stoppar in SmartCardet i hållaren så frågar kopplingsdäcket:

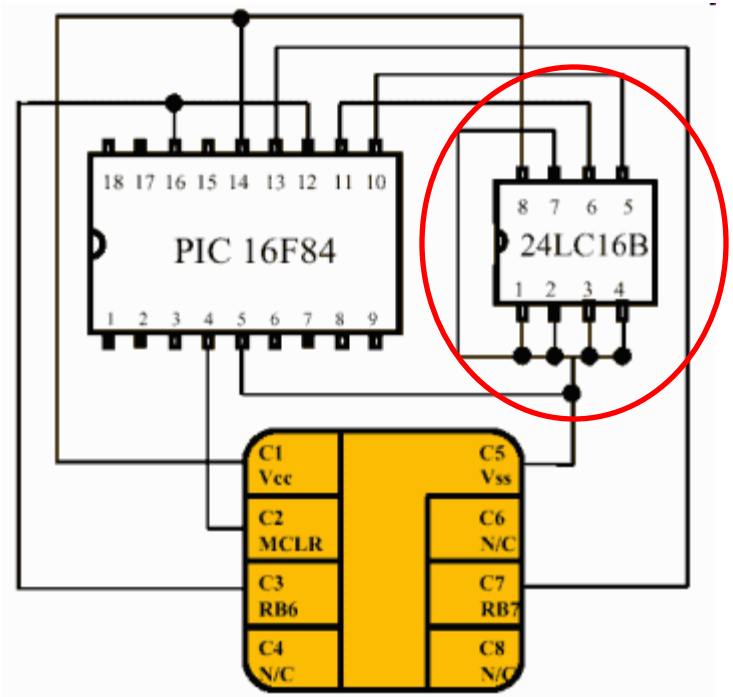
`Who is it?`

SmartCardet svarar:

`Me please open!`

Och eftersom detta är **rätt svar** så öppnar processorn på kopplingsdäcket låset (= lysdioden tänds). När SmartCardet dras ut, stängs låset.

I Banken behövs krypterad kommunikation

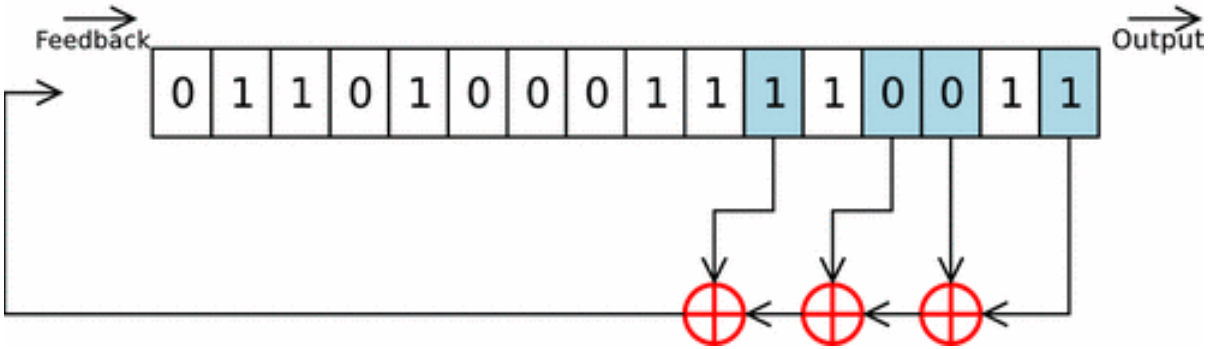


Kommunikationen mellan tex ett bankkort och en bankomat, är ”slumpmässigt” ***olika*** varje gång så att den inte bara kan avlyssnas och spelas in. Ett SmartCard innehåller ett extra minne för krypteringsnyckel och annan information. Det minnet kan bara nås via processorn, ej direkt från någon kontakt.

I Bankkortet är processorn ”Lässkyddad” så även programmet är hemligt.

William Sandqvist william@kth.se

Hur en PIC-processor kan ”beräkna” pseudoslumptal



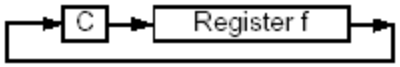
PIC-processorn är *dålig* på multiplikation och division. Ett sätt att beräkna “pseudoslumptal” utan mul/div är att använda rotations-instruktionen.
Tex. kan PIC-processorn rotera 16 bitar (2×8). I figuren sker "avtappning" från bit 0, 2, 3, och 5. De avtappade bitarna kombineras med EXOR operationer och roteras tillbaka genom Carry-biten. Just denna "avtappning" ger en *maximalt* lång talsekvens som upprepas först efter 65535 ggr.

(Om alla bitarna är “0” så stannar slumptalssekvensen, så det är denna kombination som måste undvikas!)

William Sandqvist william@kth.se

Ex. PIC-funktion

RRF Rotate Right f through Carry

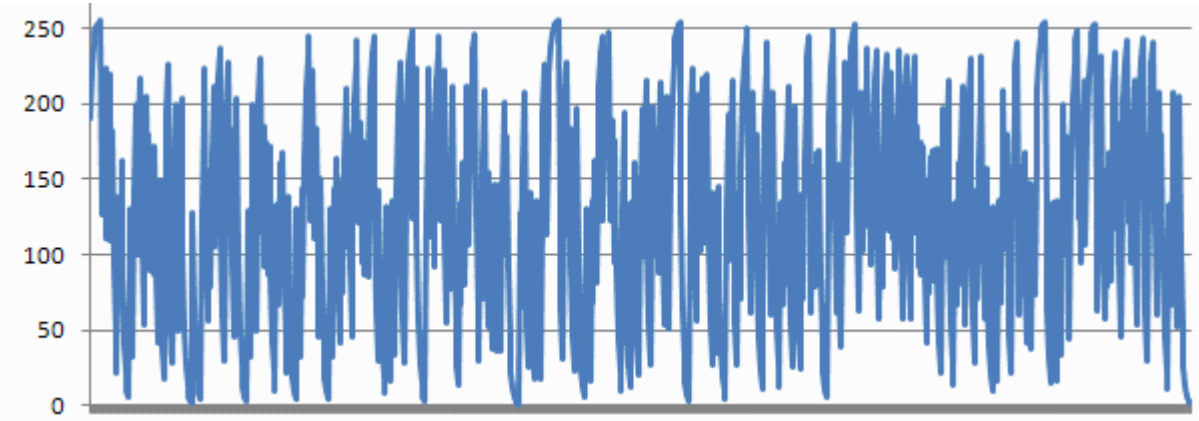



```
/* Random number function */
char rand( void )
{ /* 0x0000 won't run ... */
  bit EXOR_out;
  static char rand_hi, rand_lo;
  if( !rand_hi && !rand_lo ) rand_lo = 0x01;
  EXOR_out  = rand_lo.0;
  EXOR_out ^= rand_lo.2;
  EXOR_out ^= rand_lo.3;
  EXOR_out ^= rand_lo.5;
  Carry = EXOR_out;
  /* rotate right        */
  rand_hi = rr( rand_hi);
  rand_lo = rr( rand_lo);
  return rand_lo;
}
```

Linear feedback shift registers

Så här ser de första 700 8-bitstalen ut …

```
char rand( void );
```



100 190 223 239 247 251 253 254 255 127 191 223 111 183 219 109 **...**

William Sandqvist william@kth.se

Bankernas Chip and PIN -teknologi

Vid ”ansikte mot ansikte” – transaktioner:

- Chip – anger vilket/vems kort det är som används
  (*för att undvika förfalskade kort*)
- PIN – anger att det är kortägaren som använder kortet
  (*för att förhindra användning av stulna kort*)

Wikipedia SmartCard

William Sandqvist william@kth.se

Ett nyupptäckt säkerhetsproblem?

”Chip and PIN” is broken, 2010 IEEE Symposium on Security and Privacy.

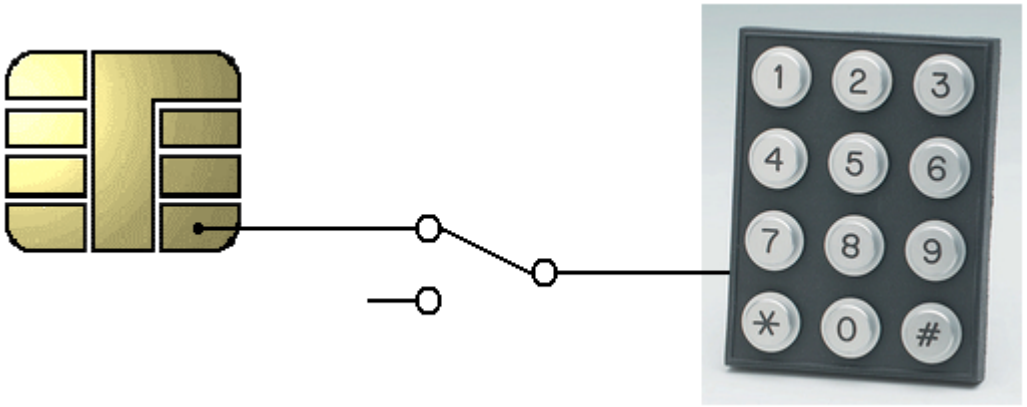
Steven Murdoch, Saar Drimer, Ross Anderson, Mike Bond

Stulet kort (med ”manipulerad” kortkontakt).
Ingen PIN-kod behövs!

Chip and PIN broken

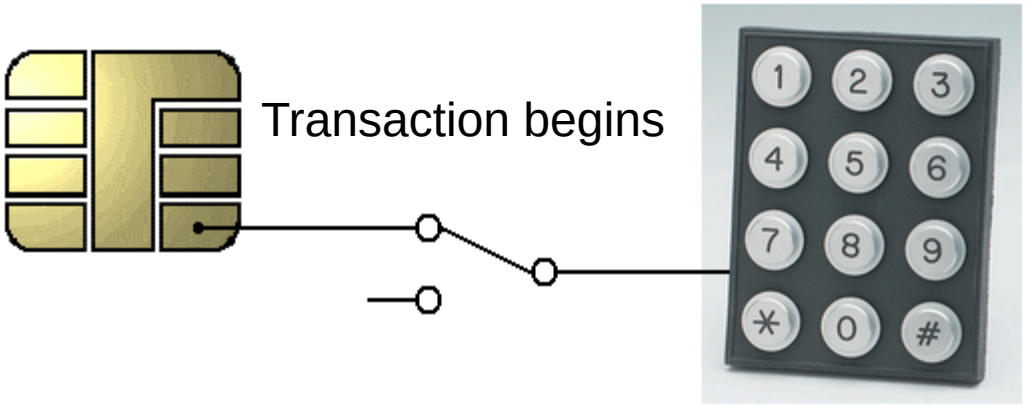
William Sandqvist william@kth.se

En ”Man in the middle” attack



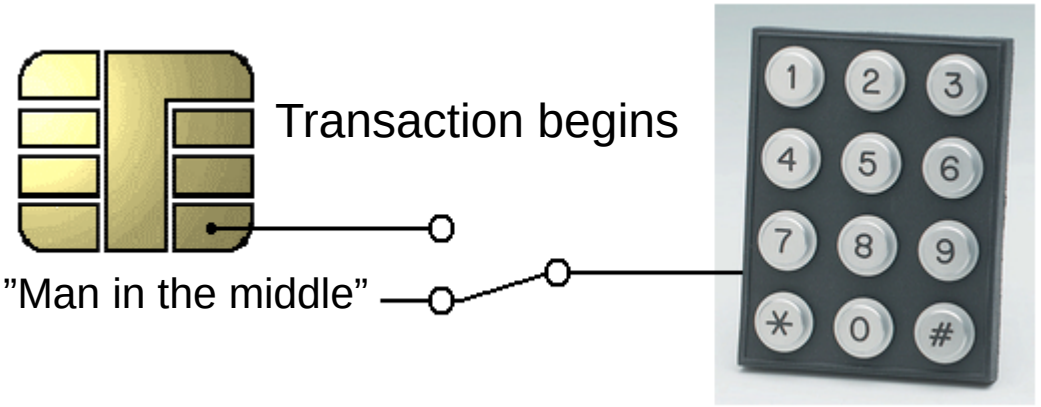
William Sandqvist william@kth.se

En ”Man in the middle” attack



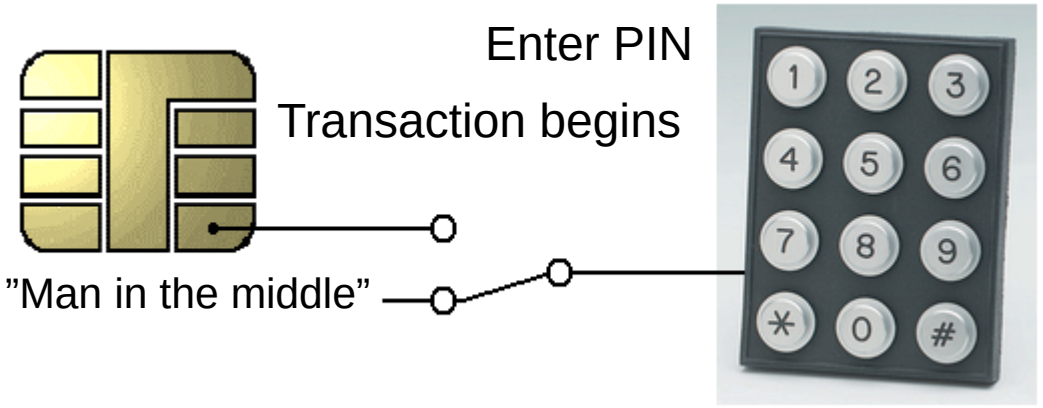
William Sandqvist william@kth.se

En ”Man in the middle” attack



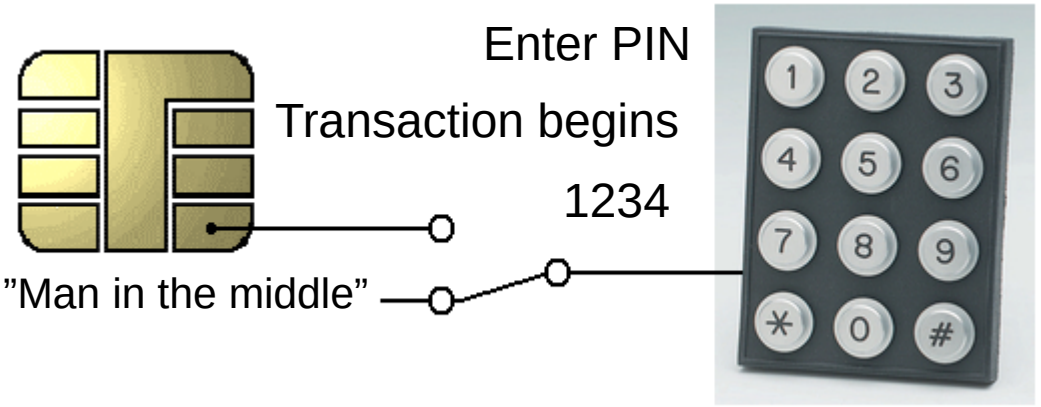
William Sandqvist william@kth.se

En ”Man in the middle” attack



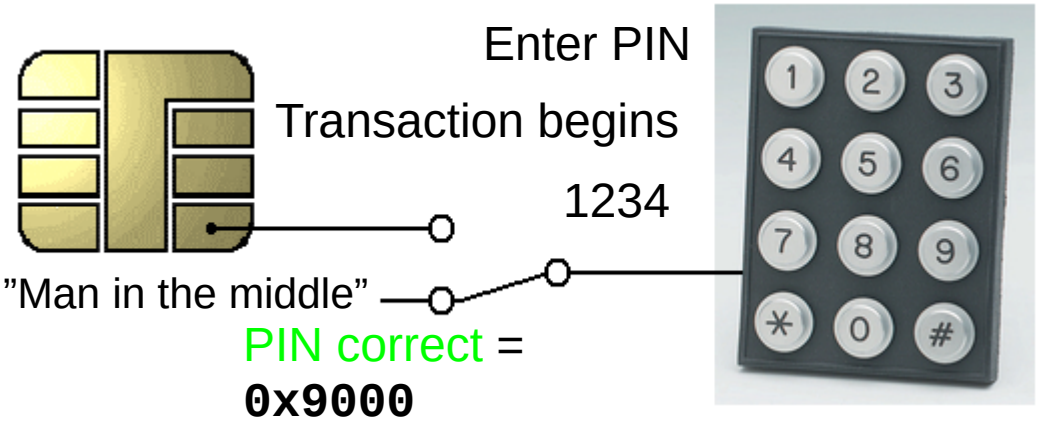
William Sandqvist william@kth.se

En ”Man in the middle” attack



William Sandqvist william@kth.se

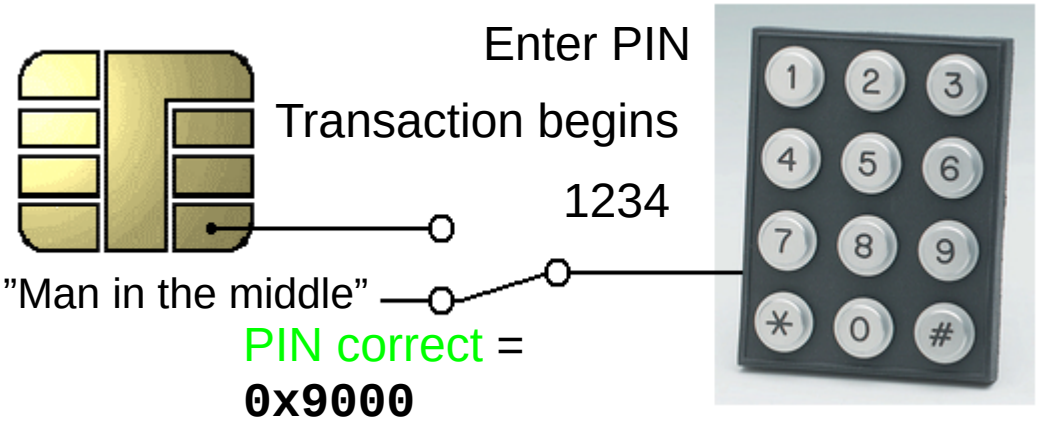
En ”Man in the middle” attack



William Sandqvist william@kth.se

En ”Man in the middle” attack

I got no numbers? So
”verifying without PIN”

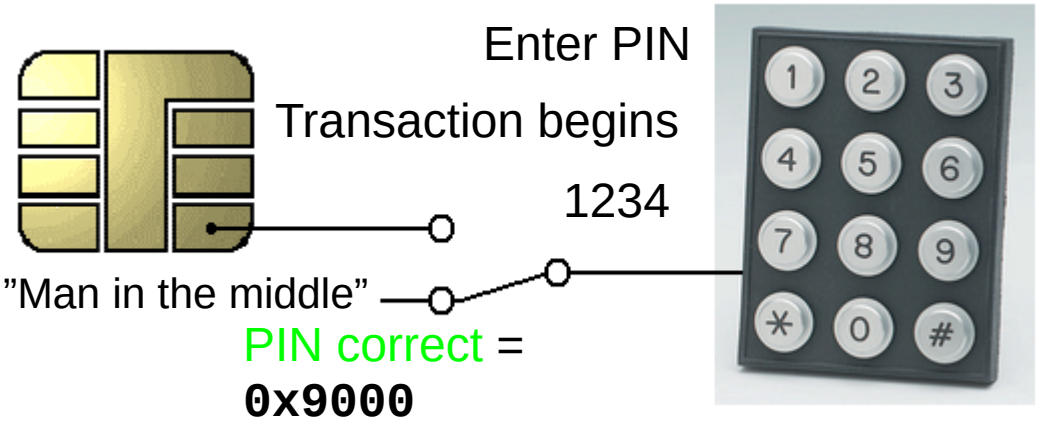


William Sandqvist william@kth.se

En ”Man in the middle” attack

I got no numbers? So
”verifying without PIN”

I had **”PIN confirmed”**
Complete the transaction

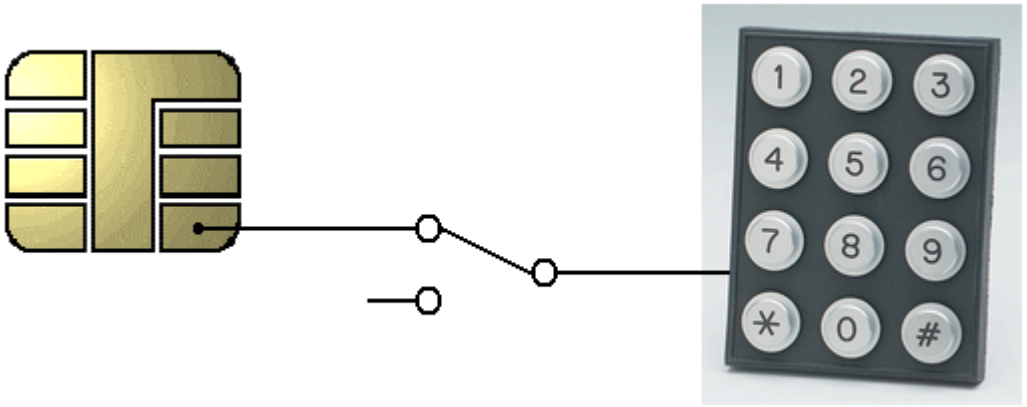


William Sandqvist william@kth.se

En ”Man in the middle” attack

I got no numbers? So
”verifying without PIN”

I had **”PIN confirmed”**
Complete the transaction

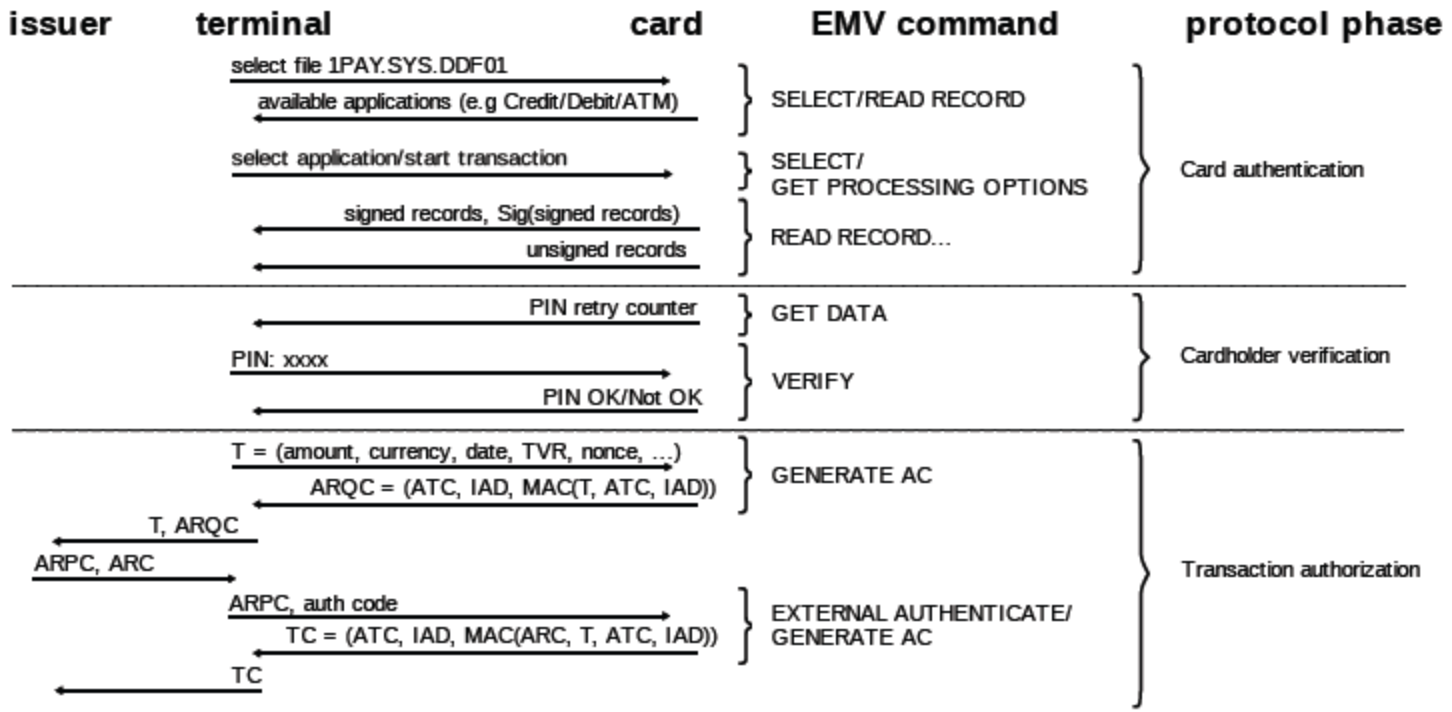


Protokollet är för komplicerat. Kortet och kortläsaren kan tro *olika* om vilken verifieringsmetod som använts! Det är detta som utnyttjas!

Standarden tillåter att verifieringen sker på annat sätt än med PIN – till exempel med legitimation och underskrift på kvittot eller utan PIN vid mindre belopp.
Det finns också kort utan PIN (tex för personer med handikappet att *inte* kunna komma ihåg ett PIN)

William Sandqvist william@kth.se

Transaktionsprotokoll



Card authentication och **Transaction authorization** sker genom utväxlande av kryptogram, men vad hjälper det när **Cardholder verification** består av ett enkelt klartextmeddelande som går att manipulera!

William Sandqvist william@kth.se

Hur stort är problemet?

Om ett köp signerats med en PIN-kod anser bankerna att Du är ansvarig för köpet. Dom anser att Du varit ”oaktsam” med koden om någon annan har utfört köpet.

- ***Detta resonemang håller inte längre!***

Kommer bankerna att behöva betala ersättning?

Problemet gäller butikernas handterminaler, ***inte*** bankomater – där är det banken som verifierar PIN-numret, ***inte*** kortet.

Men kanske är det tillräckligt allvarligt att det gäller upp till 730 miljoner kort när de används i affärernas betalningsterminaler?

Var köper man **SmartCard**?

Ett svenskt företag i Mölndal som säljer oprogrammerade SmartCard för tex. elektroniska dörrlås med SmartCard (till hotell, stugbyar mm) är:

Hansa-electronic

William Sandqvist william@kth.se