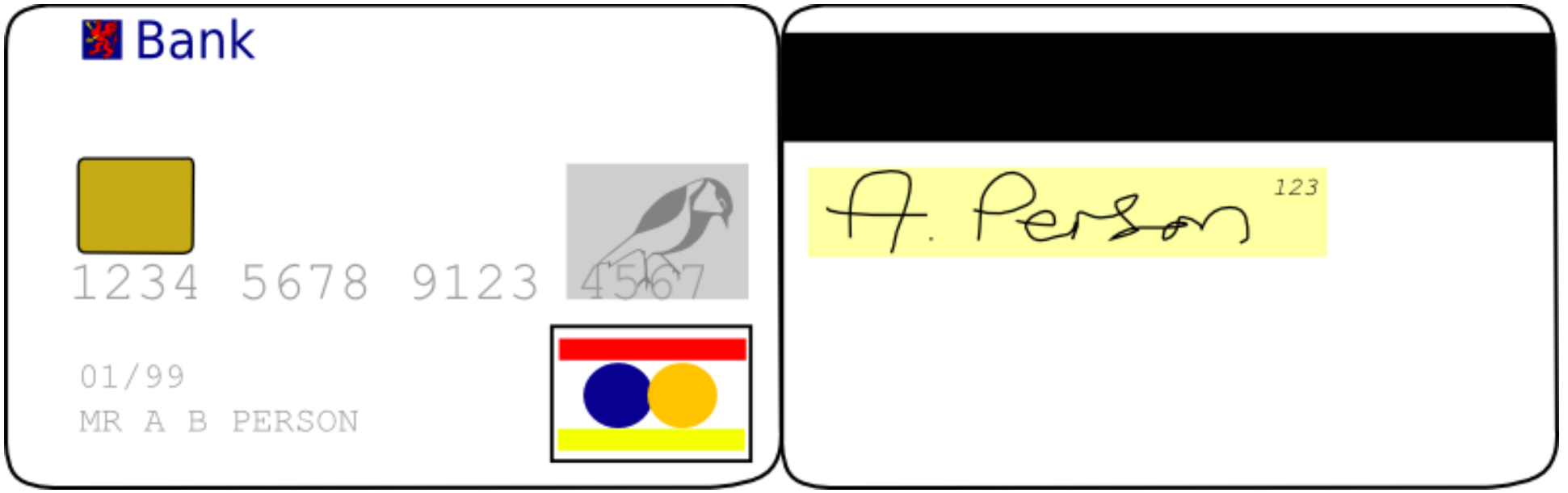
Prolomení EMV

Chip and pin is broken

Platební karty

- Magnetický proužek
- EMV
  - Pojmenován podle firem Europay, Master Card a Visa
  - Nasazen v Evropě, zavádí se v Kanadě a zvažovány USA
  - Převzat American Express a JCB
  - Počátkem roku 2008 přes 730 milionů uživatelů

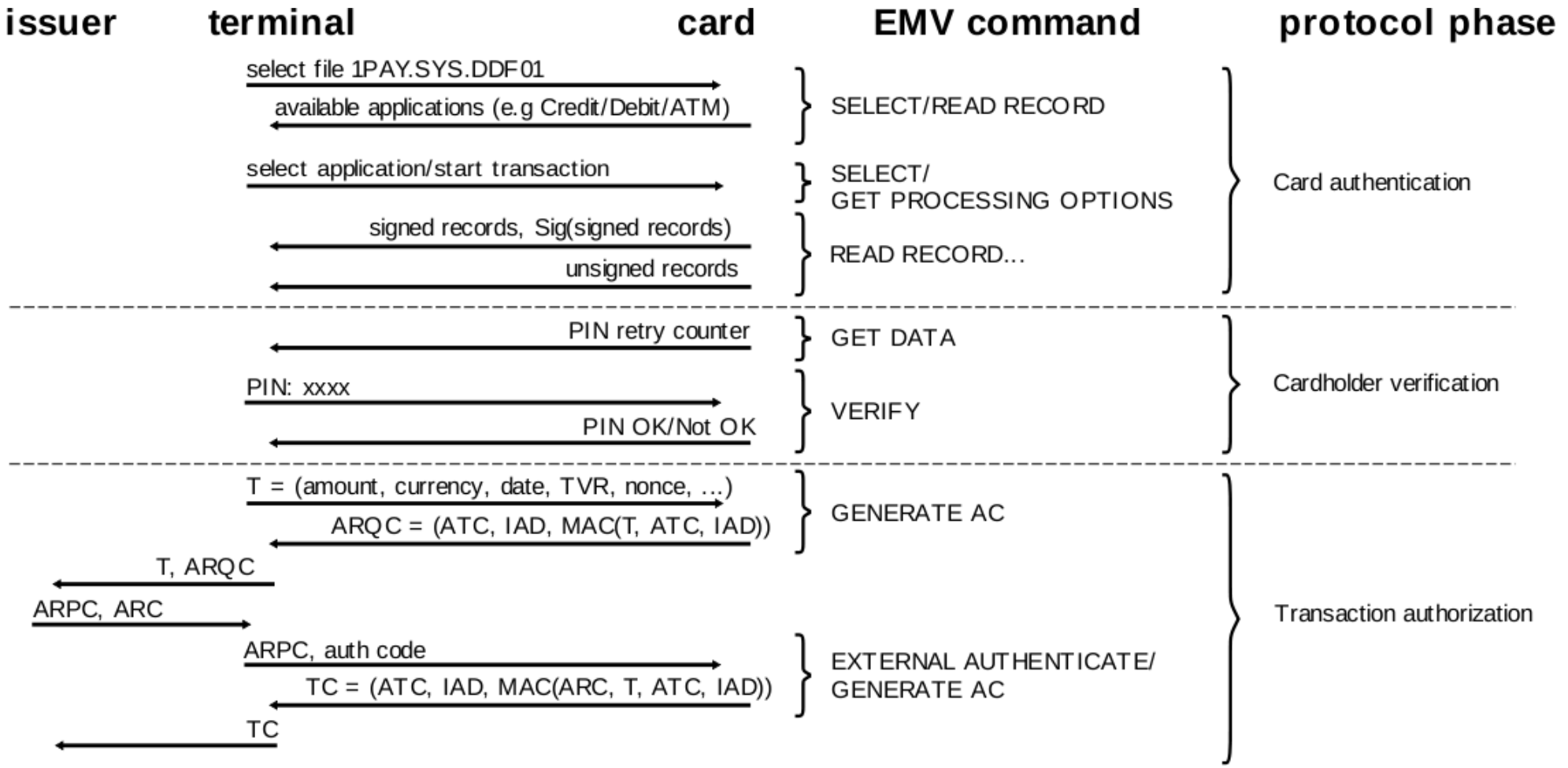
Platební karty - ilustrace



EMV – co nabízí?

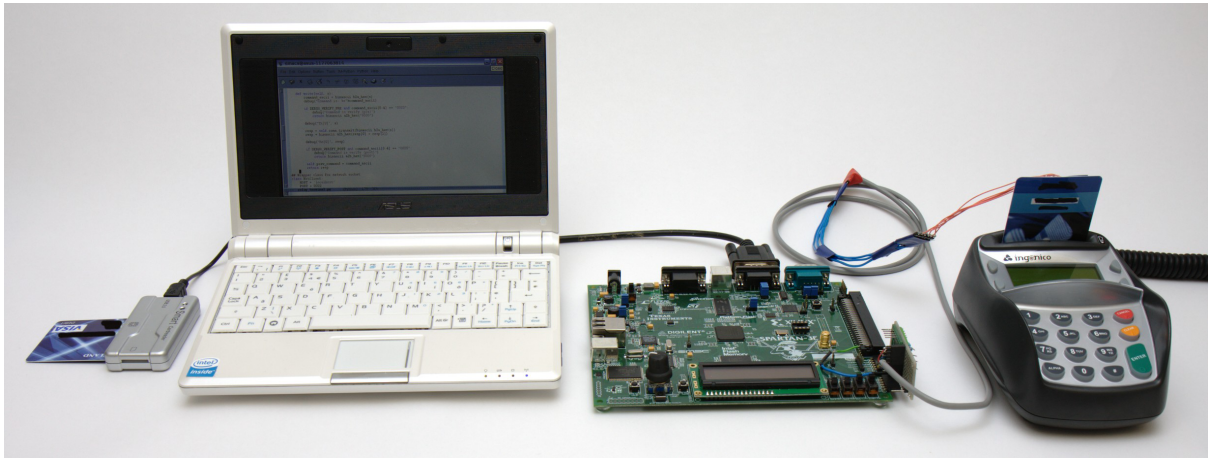
- Nejen označení pro protokol, ale také framework
- Založen na snaze o využití principu nulového rozšíření znalosti
- Vnejběžnějším kontextu používá funkci karta+pin
  - Offline a online pin autentizace
  - Offline a online platba
  - Komunikace mezi kartou a fin. institucí šifrovaná
  - Různé metody podpisu dat SDA/DDA

EMV – ilustrace



Demonstrace útoku

- Čtečka čipových karet (8$)
- Počítač – zde MITM skript (python)
- FPGA deska (189$)
- Plastová náhrada karty (2$)



Možné realizace útoku

- Možnost skrytí sestavy v batohu, kabeláž skryta
- Miniaturizace – místo FPGA a nb nějaká jednoúčelová hračka
- Karta rozstřižená tak, aby pasovala, pouzdro na ústřižek, vzhled karty

Příčiny

- Uzavřenost EMV
- Použití bitového pole namísto chybových zpráv
- Nepřehledná dokumentace
- Klíčové detaily roztroušeny napříč specifikacemi

Nabízená řešení

- Změna rozhraní u vydavatele karty
- Terminál bude číst IAD pole, pokud najde nekonzistenci ohlásí
- Přikládat výsledky autentizace nositele do komunikace probíhající s vydavatelem (1x se vyskytlo při testech)
- Zavést přerušení procesu při chybě
- Obalit existující komunikaci např. TLS protokolem