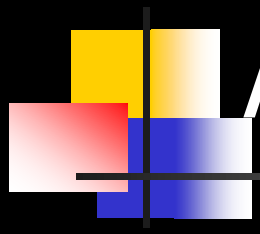
晶片卡弱點分析
MIFARE, ATM Card & 花博門票

Anderson Ni 倪萬昇

2010/07/01

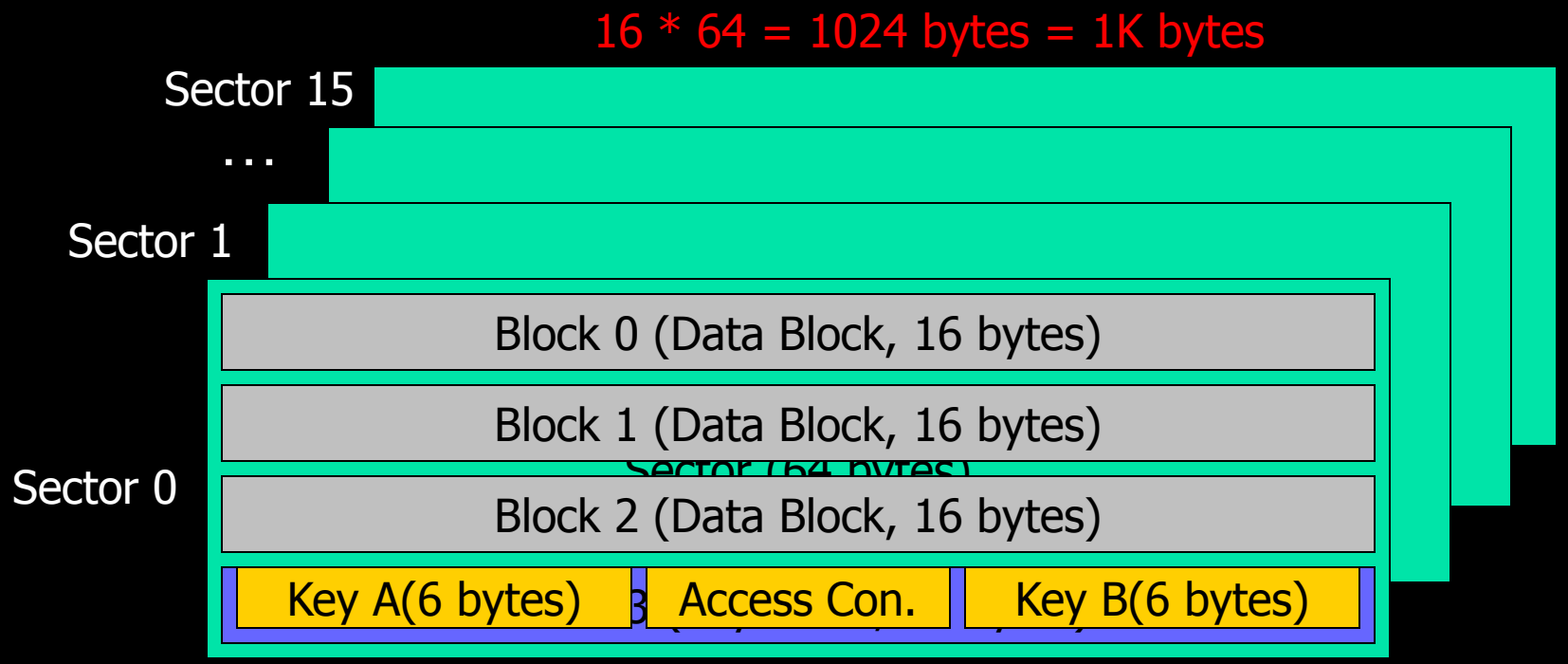


Agenda

- MIFARE 安全漏洞探討
- ATM Card與網路ATM安全漏洞探討
- 台北國際花博覽會門票安全漏洞探討

Introduction of MIFARE

- RF ID (ISO 14443-3 Type A with MIFARE,13.56 MHz, Distance 10 cm)
- Memory Card (S50 1K bytes, S70 4K bytes)



Weakness I of MIFARE Key Length

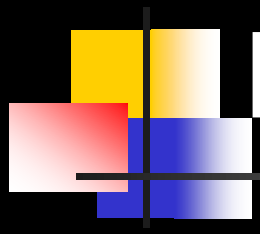
- Key Length of MIFARE Key A/B is 48 bits
  - Key length of Triple DES is 112 or 168 bits and key length of AES is 128 , 192 or 256 bits
  - Key won't lock even if key authentication failed too many times!

Brute Force Attack!!!!!

(圖片來自於網路)

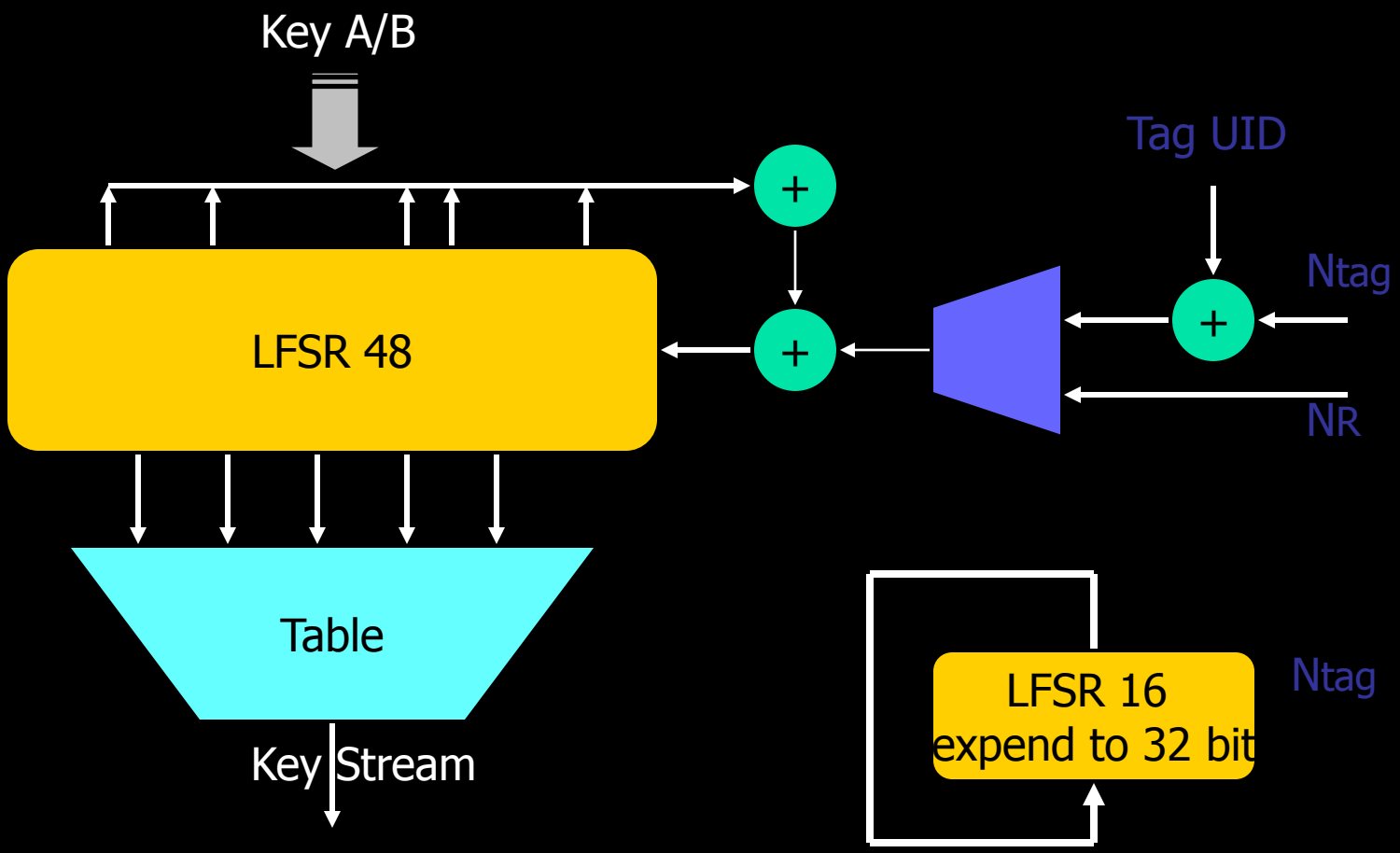
=> By the thesis, we can use 100 reader at the same time to get 1 key in 2 weeks…

Weakness II of MIFARE Random Number Generator

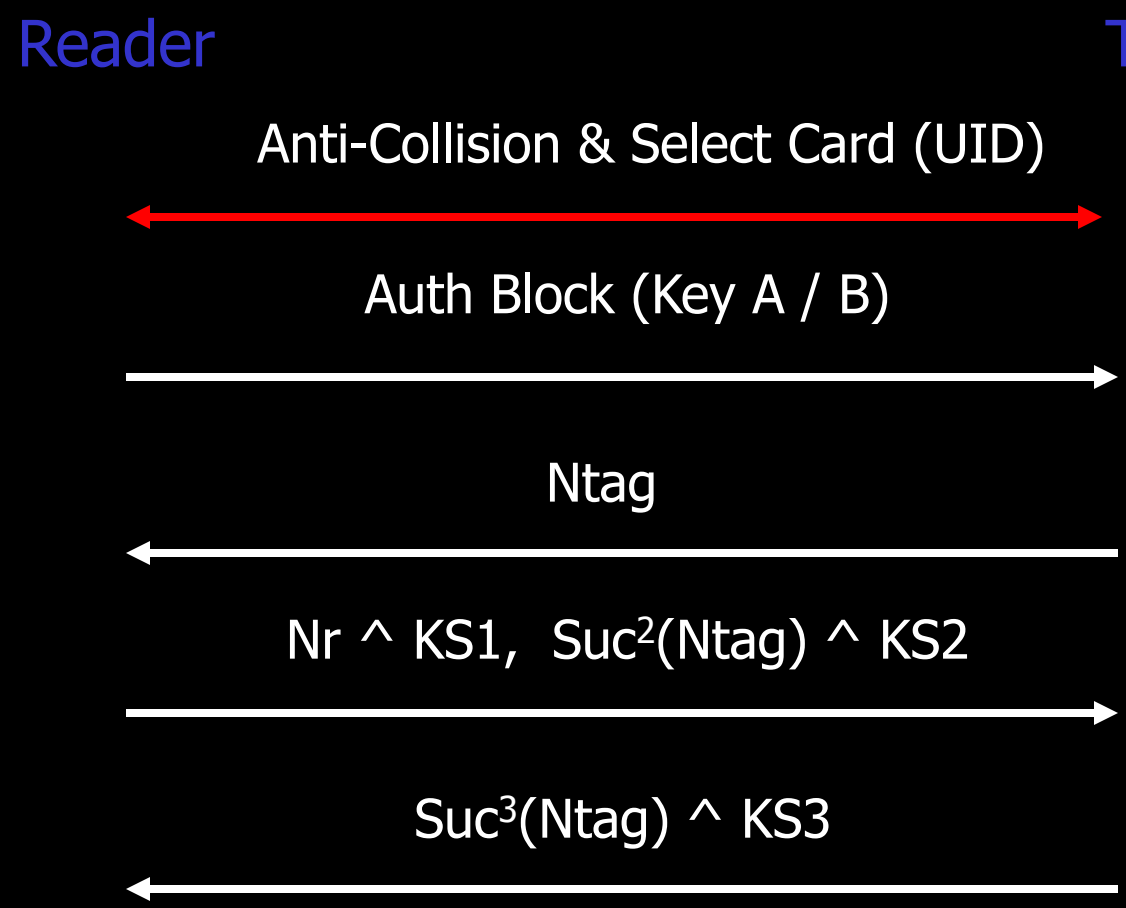


- The Random Number Generator is designed by LFSR-32 bits…
  - But… the seed is decided by the value of timer… and the timer will start to count from power on…
  - If We can control the timing… we can control the random number!

Weakness III of MIFARE Crypto 1 Algorithm

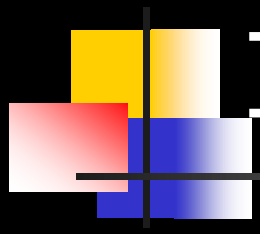


Three Pass Authentication



MIFARE Against from Weakness

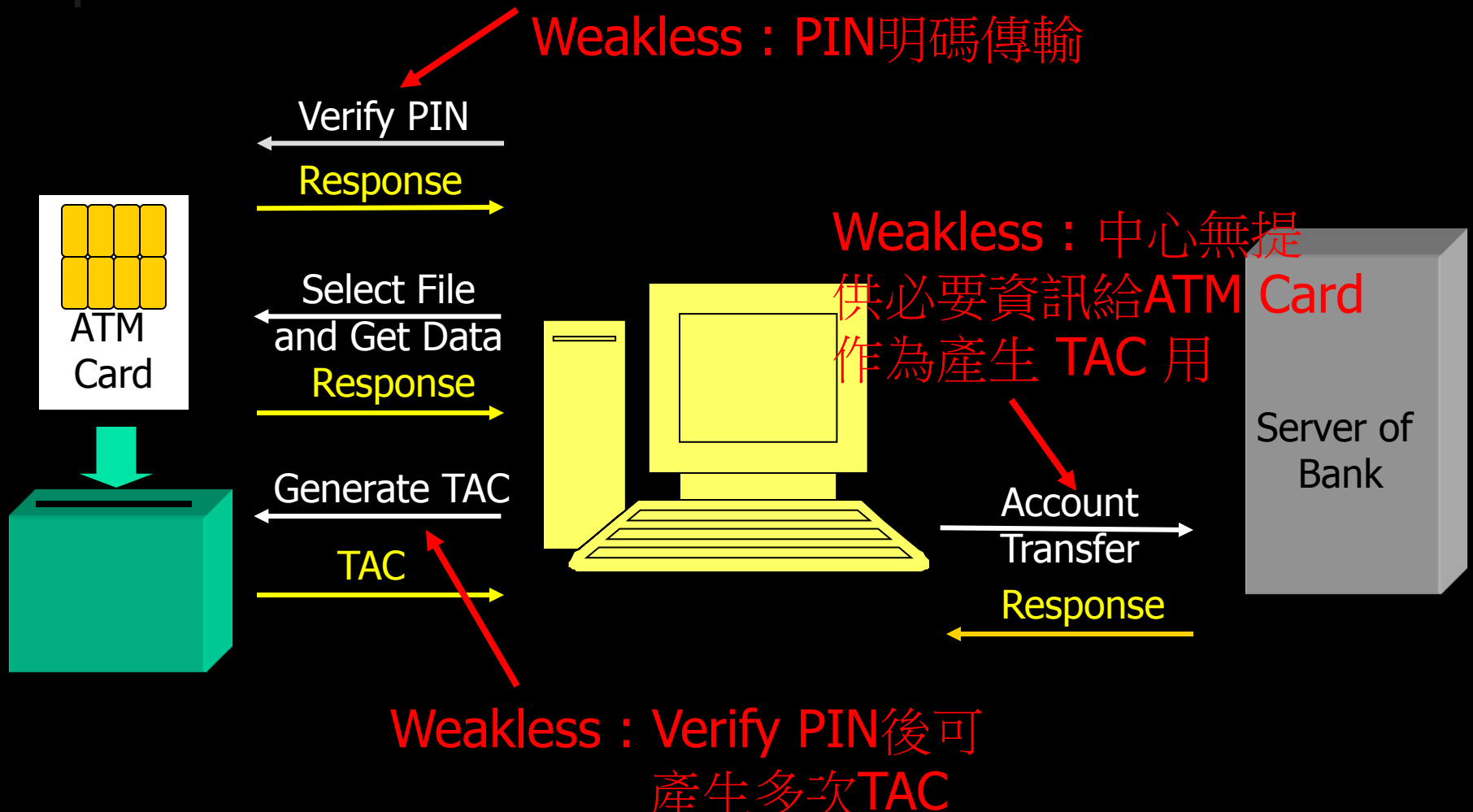
- 防偽驗證碼 (by DES or Triple-DES)
- 黑名單機制與卡片鎖卡旗標
- 除特定消費方式,大部分交通應用或小額消費均有攝影機…



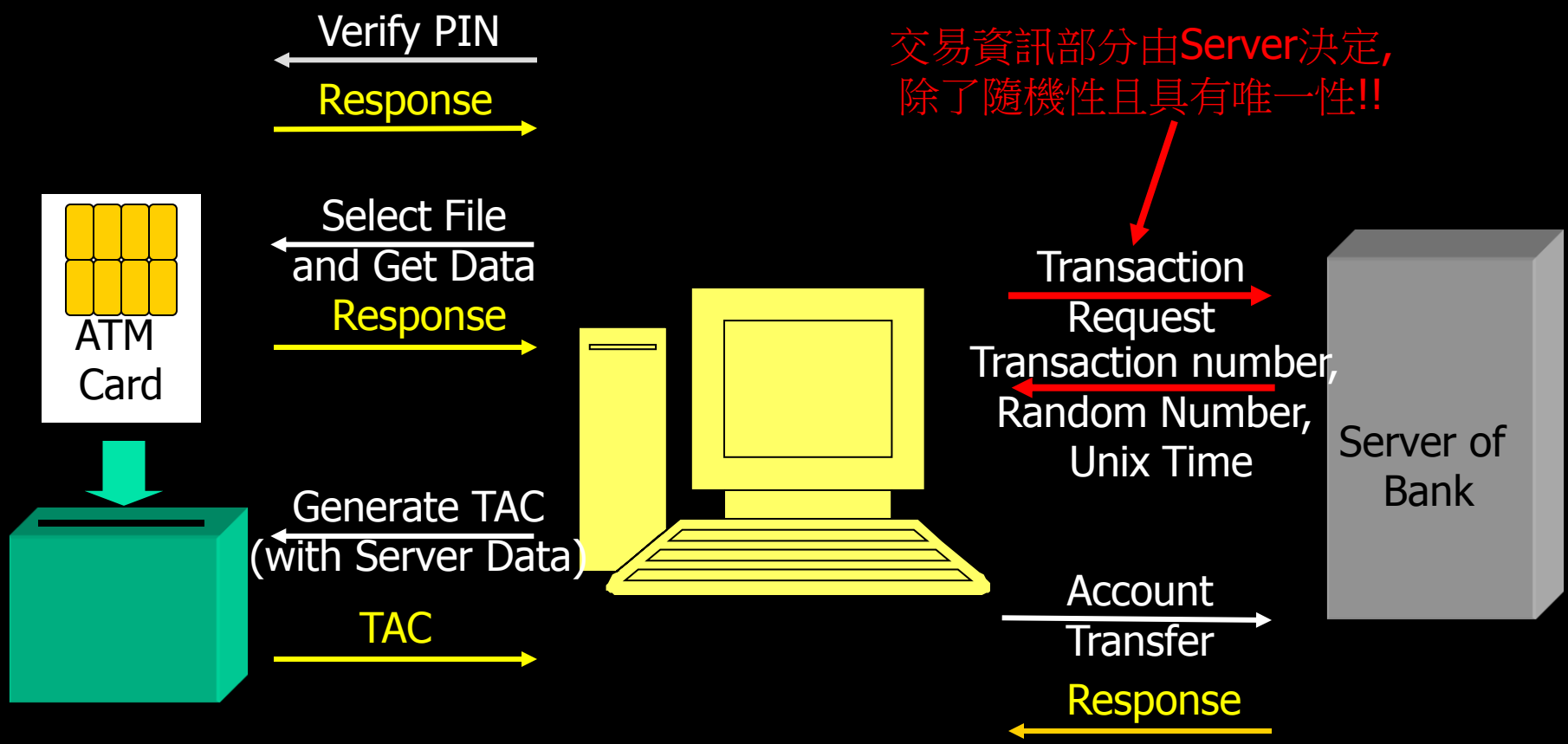
Introduction of ATM Card

- Personal Data (Account, Bank ID.. etc)
- User PIN
- Authentication Keys between Bank and Card
- Supporting DES, Triple-DES and TAC algorithm
- Secured Hardware with EAL 4^{+}

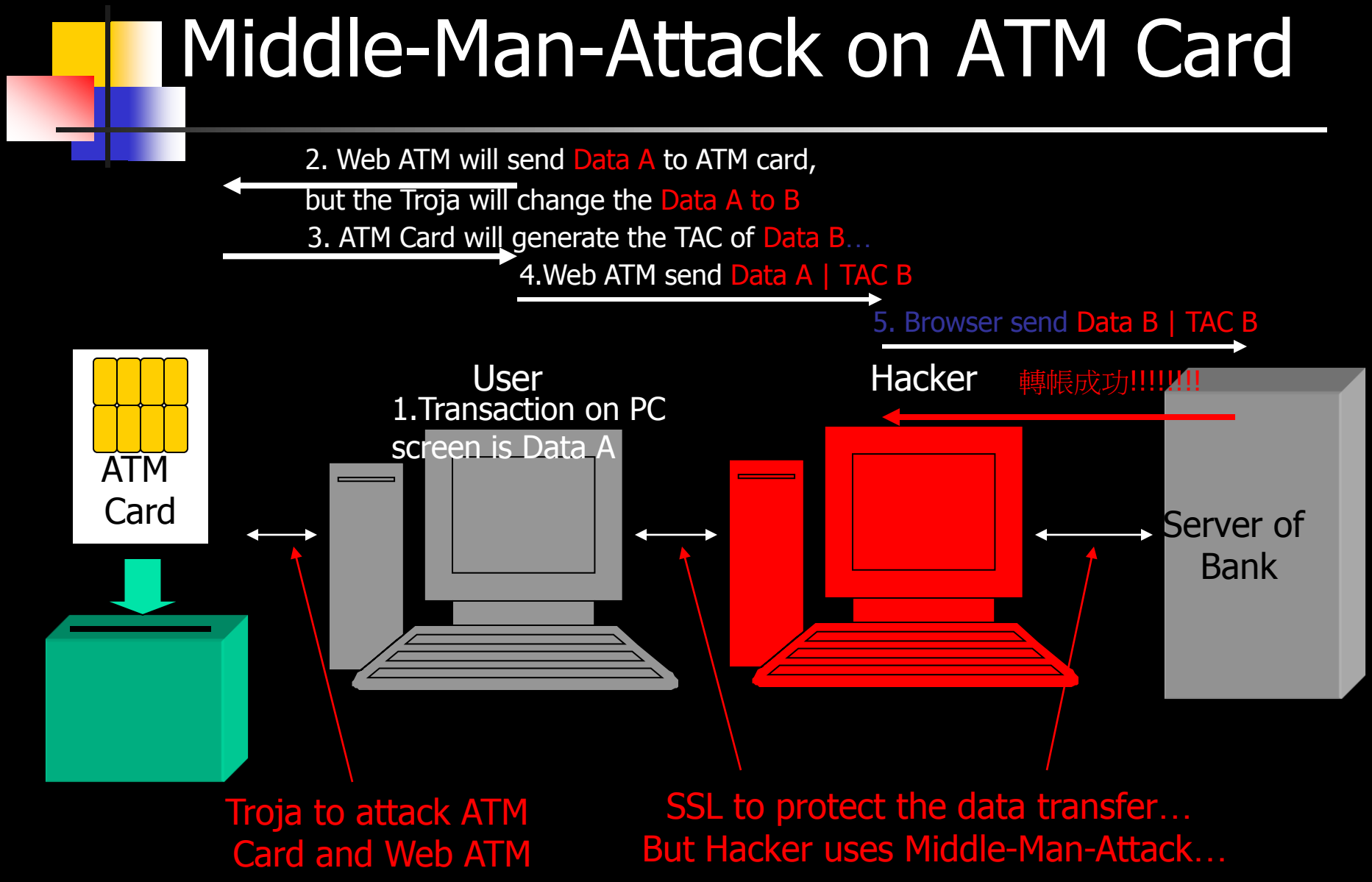
Transaction of ATM Card



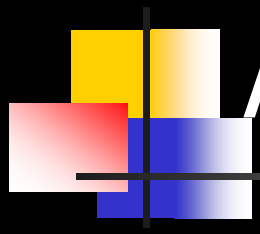
Transaction of ATM Card



Middle-Man-Attack on ATM Card



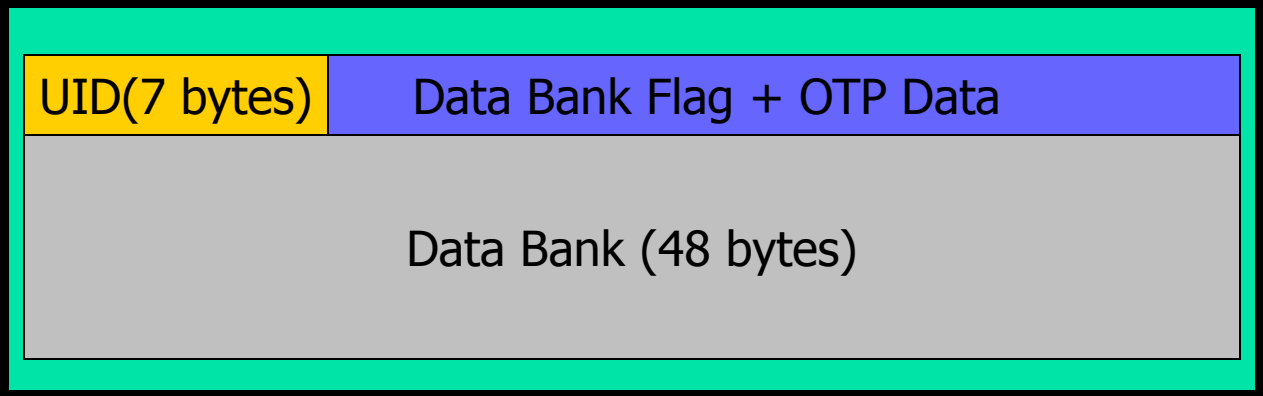
Conclusion of Web ATM and ATM Card



- 不要使用網路ATM...

2010台北國際花博門票介紹

- 一日票, 三日票, Easy Card and CHT NFC
- 一日,三日票使用MIFARE Ultra Light
- Memory Card (64 bytes only)
- 無金鑰區塊



Example 1 of 花博門票

UID	OTP Flag	OTP Data
1474B85B02CB1B8052	480000	6C72DBD0

578EC887000000000000C080000F303

00000000000010208011000000000001

FD3A0000000000000000000F181B21A

Example 2 of 花博門票

UID	OTP Flag	OTP Data
04845481E2AD1B80D4	480000	490ECB35

934492FB0000000000000C080000F303

00000000000010208011000000000001

FD3A0000000000000000000F1CE2D3A

Attacking of 花博門票 - Clone

- Clone Card – 事先購買團體票後,進行卡片所有資料之Clone… 並且偽造相同資料之卡片,即可有兩張同資料之卡片可供使用
(若無黑名單機制,Clone之卡可無限進行重置繼續使用)

Attacking of 花博門票- Change

- 修改卡片內容 – 將卡片內註記為一日或三日卡的部份修改為3日
- 若進場後,註記進場時間,但未註記出場時間或未將OTP flag關閉,可將本資料清除或將原始卡片資料寫入,又是一張未使用的卡
- 其他

Thank You!!

Q & A