Smart Cards

By: Andrew Egly

Brief History

- 1970 – Dr. Kunitaka Arimura of Japan filed the first and only patent on the smart card concept.
- 1974 – Roland Moreno of France filed the original patent for the IC card, later dubbed the “smart card”.
- 1982 – Field testing of serial memory phone cards took place in France – the world’s first major IC card test.
- 1987 – First large-scale smart card application implemented in the United States with the U.S. Department of Agriculture’s nationwide Peanut Marketing Card.
- 1994 – Europay, MasterCard, and Visa (EMV) published joint specifications for global microchip-based bank cards (smart cards).
- 1995-96 The first of 40,000 multi-functional, multi-technology MARC cards with chips were issued to U.S. Marines in Hawaii.
- 1996-98 MasterCard and Visa began sponsorship of competing consortia to work on solving the problems of smart card interoperability.
    - Two different card solutions were developed: the JavaCard backed by Visa, and the Multi-application Operating System (MULTOS) backed by MasterCard.

History cont.

- 1999 – Smart Access Common ID Project. Federal agencies to acquire a standard, interoperable employee identification card. The U.S. Government (General Services Administration) starts true multi-application Java card pilot in the Washington, D.C. metropolitan area.

- 2001 – Global Platform Specification 2.1 designated baseline specifications for smart cards, including Cryptographic support and card lifecycle

- 2002 – Estonia citizen smart card

- 2005 – EMV compliant cards introduced in Malaysia

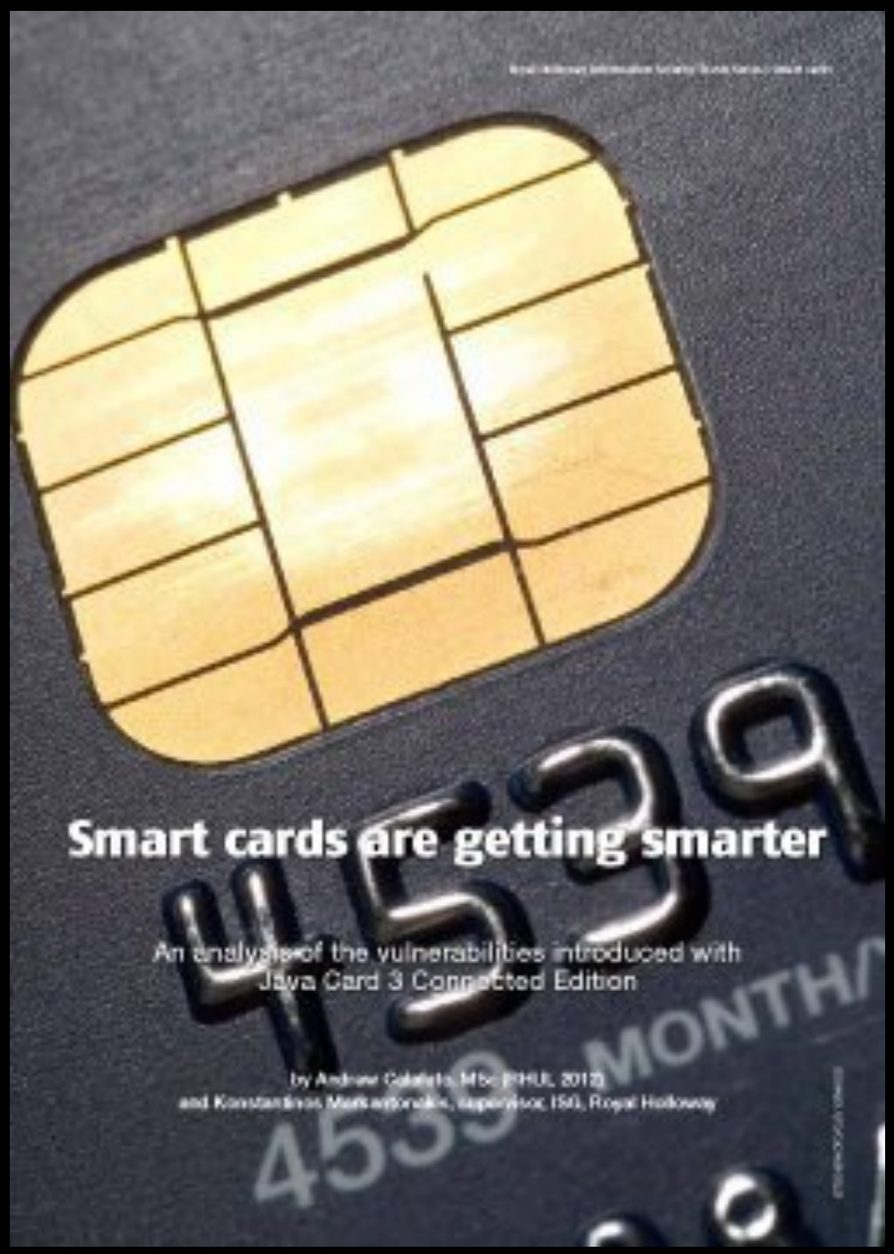
- 2009 – Belgium and Spain eID identification cards

- 2012 – Millions of PIV and CAC cards deployed in the U.S.

- 2014 – 3.4 billion EMV cards in circulation worldwide; U.S. introduces EMV cards

Rise in popularity

- Declining cost of production of smart cards
- Growing concern that magnetic strips cannot provide adequate security
- increased protection against fraud and security breaches compared to magnetic strips



Breaches and Hacks

- May 2006, Shell suspended EMV (Europay, Mastercard, Visa) payments in 600 UK gas stations, which was attributed to the EMV terminal being tempered with

- Researchers from the NCR Corporation demonstrated multiple ways of hacking “payment points of interaction”, like PIN pads, to get past chip-and-pin protections. They successfully implemented both passive and man-in-the-middle attacks to compromise key libraries and files on PIN pad devices, allowing them to capture card data including cardholder names, account numbers, card verification values (CVVs), and even PINs.

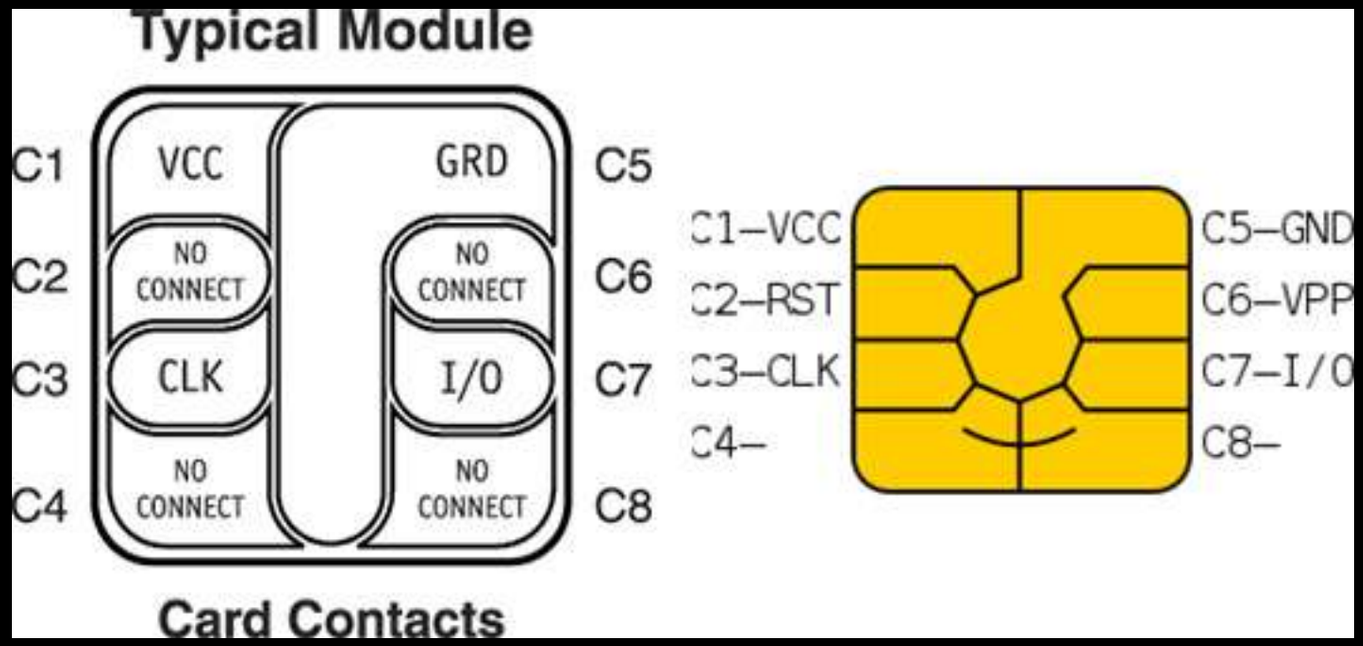
- Sep 2017 750,000 ID cards found to have a security risk that would allow identity theft days before hosting a cyber security conference

- A few mentions of the ability to get information from the card reader before encryption happens during a transaction

How they work

- contains an embedded microprocessor
- Smarts cards may have up to 8 kilobytes of RAM, 346 kilobytes of ROM, 256 kilobytes of programmable ROM, and a 16-bit microprocessor.
- The smart card uses a serial interface and receives its power from external sources like a card reader.
- The processor uses a limited instruction set for applications such as cryptography.

How they work cont.



- VCC: Power supply input
- RST: Used itself or in combination with an internal reset control circuit.
- CLK: Clocking or timing signal
- GND : Ground
- VPP : Programming voltage input
- I/O : Input or Output for serial data to the integrated circuit inside the card.

Main uses

- **Stored Value** – The primary use of smart cards is stored value, particularly loyalty programs that track and incentivize repeat customers. Stored value is more convenient and safer than cash.

- **Securing Information** – In addition to information security, smart cards achieve greater physical security of services and equipment, because the card restricts access to all but the authorized user.

- **E-Commerce**– Smart cards make it easy for consumers to securely store information and cash for purchasing. The card can carry personal account, credit and buying preference information that can be accessed with a mouse click instead of filling out forms.

- **Personal Finance** – Customers can use secure smart cards for fast, 24-hour electronic funds transfers over the internet

- **Health Care** – Rapid identification of patients; improved treatment. A convenient way to carry data between systems or to sites without systems. Reduction of records maintenance costs

Types of cards

- Contact Smart Card: communication medium between card and host (computer, ATM, etc). Chips same as SIM cards

- Contactless Smart Card: the chip communicates with the card reader through RFID induction technology. These cards require only close proximity to an antenna to complete transaction.

- Cryptographic Smart Cards: often used for single sign-on. Most advanced smart cards include specialized cryptographic hardware that uses algorithms such as RSA and DSA

References

- http://cardwerk.com/smart-card-history/
- http://www.win.tue.nl/pinpasjc/docs/Card%20Spec%20v2.1.1%20v0303.pdf
- http://cardwerk.com/smart-card-technology-overview/
- https://www.securetechalliance.org/smart-cards-faq/
- http://info.rippleshot.com/blog/the-brief-history-of-chip-card-hacking
- https://www.ft.com/content/874359dc-925b-11e7-a9e6-11d2f0ebb7f0
- https://computer.howstuffworks.com/question332.htm
- https://www.electroschematics.com/5074/smartcards-how-it-works/