Head of Security

Colin Whittaker

Presented by

Industry Perspective

EMV Security - A UK Payment
- Conclusions
- The Terminal & Key Management
- Card Authentication Methods (CAM)
- Cardholder Verification Methods (CVM)
- Understanding the Language
Understanding our Language

APACS

Branding, Image, Hologram

Dynamic Data Authentication

Static Data Authentication

Is this a valid and authentic card that has been presented?

Card Authentication Methods (CAM)

PIN

Biometric

Forensic Signature

Is presenting the card to pay?

How do we verify at point of sale that the owner of the card

Cardholder Verification Methods (CVV)
Off the card in distant back and CWM databases?

Off the card locally?

On the card?

How do we verify the CWM data?

How do we protect the CWM data?

Fallback and priority

What happens if the CWM fails or does not work?

Which method should we choose?
How safe and secure is static data?

Where are the risks in using SDA in an off-line environment?

Are we authorizing transactions predominately on-line or off-line?

Card Authentication Methods (CAM)
Java cards are now readily available and easy to use.
- There is a large body of technical knowledge.
- But SIM card and satellite chip cards have all been attacked.
- Integrity and Authenticity can in principle be preserved.

Can smartcards protect static data?

- Magnetic Stripe data
- Identity Credentials
- Music, video and Film and Luxury Products
- Is any static data safe from counterfeiting?

The Protection of Static Data
But in Nov 2001 cards to a longer key length,

By 1 Jan 2002 Carte Bancaria had successfully migrated all

Pin scheme private key; including the ability to say "yes" to any

This led to the production of fraudulent cards with valid data,

Internet.

Key was successfully factored and openly exposed on the

In April 2001 the Carte Bancaria Scheme 320 bit Private

Learning from the experience of others
Smart Card Copying Tool

راه حل برای کپی کردن کارت هوشمند

Conecte o Fio ao PC

Conectar o fio ao PC

Charge device Atech 300 Series USB

充電装置 ATC300 Series USB
How do you update or revoke them?

Which public key should be used for what smartcard?

Scheme Public Key distribution

Applications

UK PIN Entry Device Protection Profile for Point-of-Sale

The terminal must be secure and not subject to compromise

Terminal and terminal

The CAM and CVV require an interaction between Card

Smartcards require a terminal

Terminal Requirements
Right as are overall security needs
Reputation and credibility are as important reasons to get it
perception is critical
These cards and terminals are in the public domain. Their

Online vs off-line; SDA vs DDA; key length
Surviving and evolving over time to new threats
Solutions must be tailored to need and be capable of

It is not just about a public key cryptography and smartcards
terminal and user lifecycle
end process and the entirety of the scheme, card, key,
Risk management requires an understanding of the end-to-

Conclusions