Enhancing the Conditional Access Module Security in Light of Smart Card Sharing Attacks

Konstantinos Markantonakis, Michael Tunstall, Keith Mayes

Dr Konstantinos Markantonakis
(BSc, MSc, MBA, PhD)

K.Markantonakis@rhul.ac.uk
http://www.markantonakis.eu
Tel: +44(0)1784-414409

Information Security Group Smart Card Centre
http://www.scc.rhul.ac.uk

Agenda

- Introducing the ISG and SCC
- What is all about?
- Content provision in the Sat TV Industry
- A Changing World
- Open Receivers and Threats
- Assumptions
- Notation
- Enhanced CW Transfer Between CAM and Card
- Security Analysis
- Conclusions

Smart Card Centre
Royal Holloway

The ISG Smart Card Centre

- Information Security Group
  - Royal Holloway, University of London, Egham, Surrey, UK
  - 14 full-time staff, 40 Phds, 200 Msc/Year
  - Taught by experts from industry and academia

- Smart Card Centre
  - Founded in October 2002
    - RHUL, Vodafone and G&D
    - Considerable connections to industry

Smart Card Centre
Royal Holloway

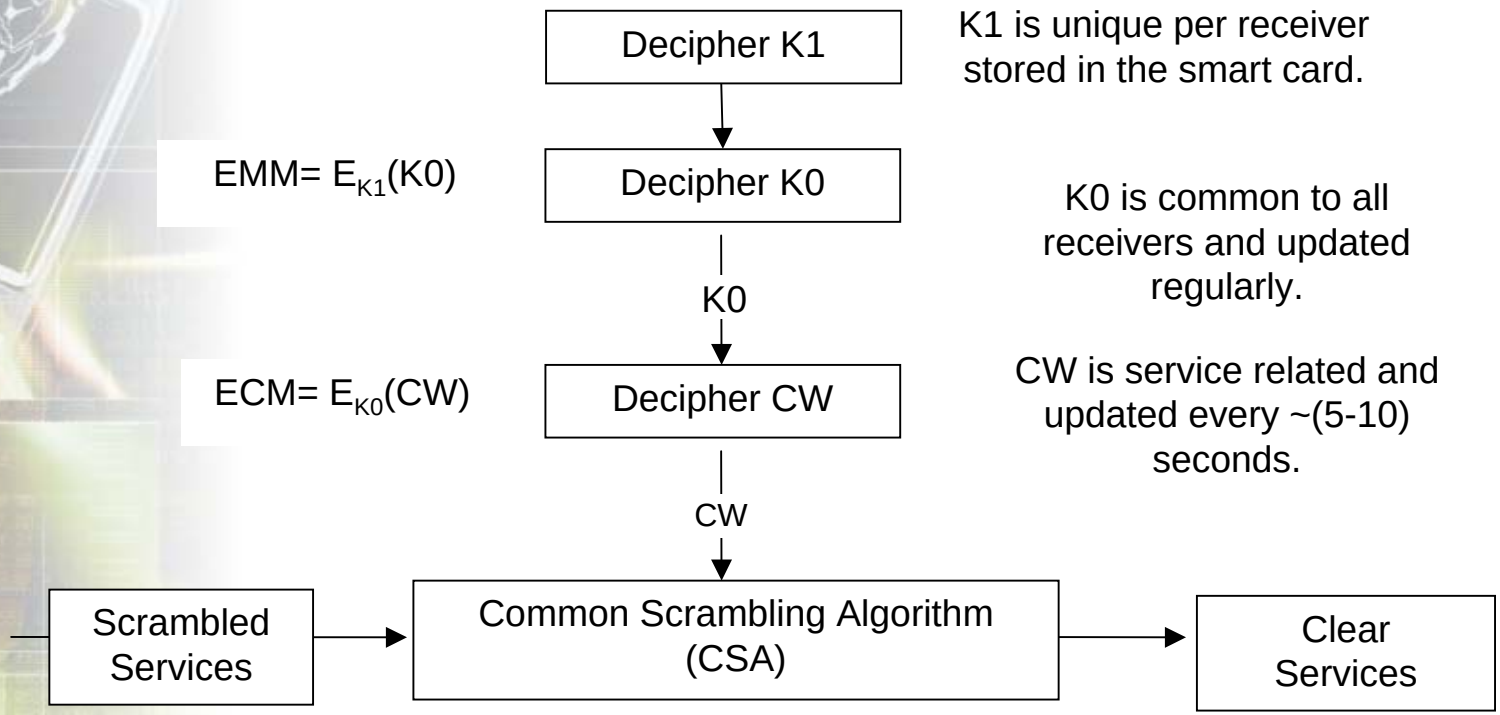
What is all about?

- Satellite (Sat) TV consumers are looking of ways to enhance their viewing experience.
  - “Open” Satellite receivers were introduced.
  - New threats were therefore introduced/realised.
- The world of code-makers and code-breakers is well illustrated in satellite TV security.

- **Scope**:
  - To briefly introduce the recent technological advances,
  - Propose relevant countermeasures for a specific type of attack, called *the card sharing attack*.

Smart Card Centre
Royal Holloway

Content Provision in the Sat TV Industry



Smart Card Centre
Royal Holloway

A Changing World…

- **Intro**
  - Often 1 STB = 1 Service Provider
  - Need for Open Receivers.
    - One box = several services
    - Reconfigurable = more tools.

- **Threats**
  - Highly configurable environments.
  - Effective Internet community surrounding these devices, providing
    - Tools, Knowledge, and Assistance
  - Relatively cheap (£400).

THESE ARE COMPUTERS!

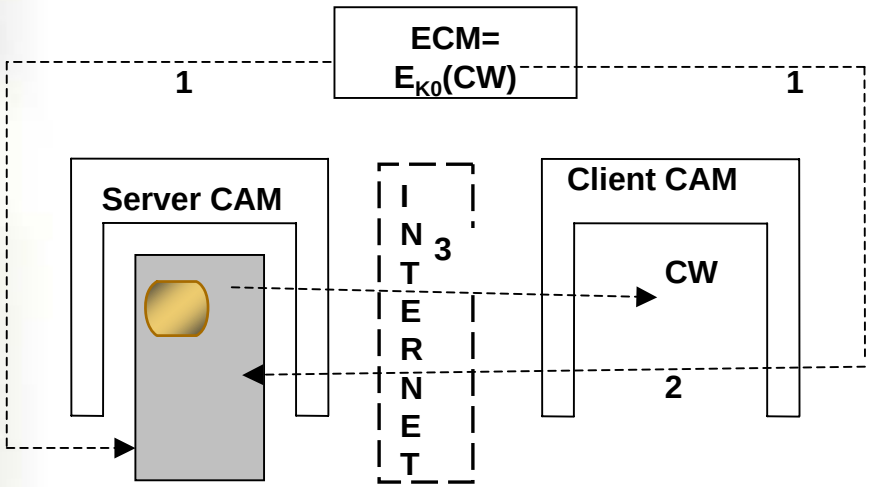
Not like a CD/DVD Player but a fully functional desktop computer

Smart Card Centre
Royal Holloway

Open Receiver Threats

Security Measure	Open Receiver Attack Method	Effectiveness
Non-CAS protected STB	Downloadable software emulator	Simple and endures but limited ☆ ☆ ☆
CAS protected STB	Cloned smart card or CAM	Simple but limited lifespan ☆ ☆ ☆
"Emerging" Card Sharing	**Downloadable software and constant Internet Connectivity**	**Average complexity but enduring hack** ☆ ☆ ☆ ☆ ☆

- The card sharing attack is central to our work…



Smart Card Centre
Royal Holloway

Assumptions

- (A1) The proposed countermeasure may be software and/or hardware based.
- (A2) Card and CAM applications are installed in advance.
- (A3) Devices adhere to standards and technologies.
- (A4) Legitimate devices (CAM and SC) are “tamper resistant”.
- (A5) CAM ←→ Card communication may be eavesdropped.
- (A6) → The security functionality can be spread between the SC and CAM.
- (A7) → No communication link from the STB to the satellite TV operator.
- (A8)→ The CAM and the card have access to common cryptographic algorithms.

Smart Card Centre
Royal Holloway

Notation

Notation	Description
Y||Z	Represents the concatenation of data items Y, Z in that order.
X→Y: Z	Implies that entity X sends entity Y a message with contents Z.
{X, Y, Z}	Implies that items within curly brackets are optional.
$E_K(Z)$	Is the result of enciphering data Z with a symmetric key cryptographic algorithm (e.g. AES or triple-DES) using key K.
$PK_X(R)$	Is the result of enciphering of data string R using a public key cryptographic algorithm (e.g. RSA) with key X.
CSN	Represents the Card's Serial Number.
X_SK	Represents a session key, generated by entity X, to be used for the subsequent cryptographic protection of a secure channel.
Rand_X(i)	Is a random number, with incremental number (i), and generated by entity X (e.g. a Host or a Card).
Cert(X)	Represents a certificate on key X.
PE_X	Represents entity X's Public Encryption Key, e.g. an RSA public key.
SE_X	Represents entity X's Secret Encryption Key, e.g. an RSA privatekey.
CW	Represents the key used to encrypt the satellite TV broadcast. This key is transmitted from the card to the CAM for the subsequent signal decryption.
PS_X	Represents entity's X Public Signature Key, e.g. an RSA public key.
SS_X	Represents entity's X Secret Signature Key, e.g. an RSA private key.
$SIGN_X(R)$	Is the result of a digital signature of data string R using a public key algorithm (e.g. RSA) with key X.
X_ID	Represents entity's X identity.

Enhanced CW Transfer Between CAM and CARD (i)

1) ENCAM → SC: Rand_ENCAM || Cert(PE_ENCAM) || ENCAM_ID || Request_Cert(PE_SC) || Request_Cert(PS_SC) || { optional parameters }

2) SC → ENCAM: $SIGN_{SS\_SC}$ (E_{PE_ENCAM}(Rand_SC || Rand_ENCAM1 || {SC_SK} || {Cam_Generate_Session_Keys})) || { Cert(PS_SC) || CSN) || Cert(PE_SC)}

Smart Card Centre
Royal Holloway

Enhanced CW Transfer Between CAM and CARD (ii)

(3i) ENCAM → SC: E_{SC_SK}(Rand_SC || CK || Rand_ENCAM2 || optional parameters)

OR

(3ii) ENCAM → SC: E_{PE_SC}(ENCAM_SK || Rand_SC || Rand_ENCAM2 || optional parameters) || E_{ENCAM_SK}(CK || Rand_ENCAM2)

4) SC → ENCAM EKEY(Rand_ENCAM2 || CW || {optional parameters})

Smart Card Centre
Royal Holloway

Security Analysis

- If the cards secret keys are compromised
  - The Issuer will have to decide whether:
    - to terminate or block the card, or simply update the card's functionality by using certain management keys as described in GlobalPlatform.
- In case the an off-card entity (e.g. the Issuer or Certification Authority) RSA encryption key pair is compromised.
  - The off-card entity has to generate a new certification key pair, which will replace the one used to certify the compromised key.
  - The off-card entity has to generate a new RSA encryption/signature key pair
    - and certify the public key of this key pair using the new private certification key.
  - All the cards carrying the old public certification key have to be updated with the new public key.

Smart Card Centre
Royal Holloway

Security Analysis

- Replacement of certification key pairs is also deemed necessary when RSA public encryption key certificates are due to expire to ensure that a key is not used beyond its expiry date.
- If a TCM private signature or encryption key is compromised a similar procedure to when the card keys are compromised needs to be followed.

Smart Card Centre
Royal Holloway

Conclusions

- Open Receiver technology will continue to improve with consumer demand.
- The attacking communities will also continue to grow, aided by:
  - Anonymity of the Internet
  - Facility of information dissemination
- The proposed protocols and underlying platform achieves the secure delivery of the CK key (obtained from the on card decryption of the CW) at the ENCAM by using the session keys.
- The card is the only trusted element at user site and therefore the solution is likely to be found there.
- The need for more powerful cards with enhanced communication bandwidth capabilities is paramount.

Smart Card Centre
Royal Holloway

Thank you for your attention…

Any Questions?

Smart Card Centre
Royal Holloway