# Smart Card Platform Fingerprinting

## Securing Cyberspace Workshop IV (SCWS4)
## Special purpose hardware for cryptography: Attacks and Applications


Dr Keith Mayes

Keith.mayes@rhul.ac.uk

Director of the ISG Smart Card Centre

Royal Holloway University of London


Royal Holloway
University of London

vodafone

Royal Holloway University of London

Giesecke & Devrient

# *The Smart Card Centre of the Royal Holloway University of London.*

- The ISG-Smart Card Centre was founded in October 2002 by Royal Holloway University of London, Vodafone and Giesecke & Devrient
- The primary objective was to create a World-Wide centre of Excellence for training and research in the field of Smart Cards, tokens, applications and related technologies
- We have expanded the involvement of other industry partners to broaden the scope of expertise and influence
- An MSC course module and seminar programme exists for advanced topics in Smart Cards, Tokens, Security and Applications
- An active PhD programme exist

www.scc.rhul.ac.uk

# *The Information Security Group*

- The ISG is one of the largest and most respected academic security groups in the world (Queen's award)
  - 17 Full-time Academics, 1 Part-time Academic, 1 Senior Visiting Fellow, 7 Visiting Professors, 4 Consultants, 6 Postdoc RAs
- It brings together in a single institution, expertise in education, research and practice in the field of information security and each year trains 150+ MSc, 70+ PhD students
- Topics Covered
  - Cryptography
  - Mobile security
  - Smartcard/token security
  - Critical infrastructures
  - Security architectures/frameworks
  - Trusted computing
  - Access control
  - System security

*www.isg.rhul.ac.uk*

# *The Discussion Topic..*

- The mobile communication industry is critically dependent on security solutions for authentication confidentiality and integrity
- The technical measures to ensure security have evolved but still depend on “keeping secrets” - so the spectre of widespread cloning remains
- Smart card platforms that could host “clones” are now readily available
- Are there means to detect and reject clone card platforms when all your secrets are known?
- Are there practical smart card “platform fingerprints”?

# Contents

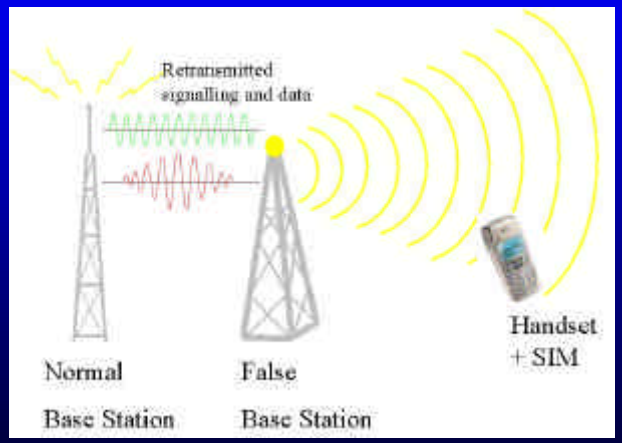
- Overview of Mobile Communication Security
- Overview of SIM/USIM attacks
- Secrets used in SIM/USIM
- The impact of Clones
- Biometric Analogy
- Leakage fingerprint as possible solution
- Detection
- Practical problems
- Concluding remarks

# Overview of Mobile Communication Security (1G)

- Total Access Communication System (TACS)
  - Analogue system used in UK based on AMPS system
- Relied on the Subscriber Number (SNB = Phone number) and Electronic Serial number (ESN) that were transmitted in clear
- Attacker used radio scanner to capture SNB/ESN pairs or simply eavesdrop calls
- Phones were meant to prevent unauthorised reprogramming of SNB/ESN – they did not!
- RESULT = major cloning problem
  - Expensive and time consuming to police
- Lessons learned
  - Phone was not tamper resistant – specialist hardware needed
  - Call confidentiality required – cryptography needed
  - Caller anonymity needed – new identities needed

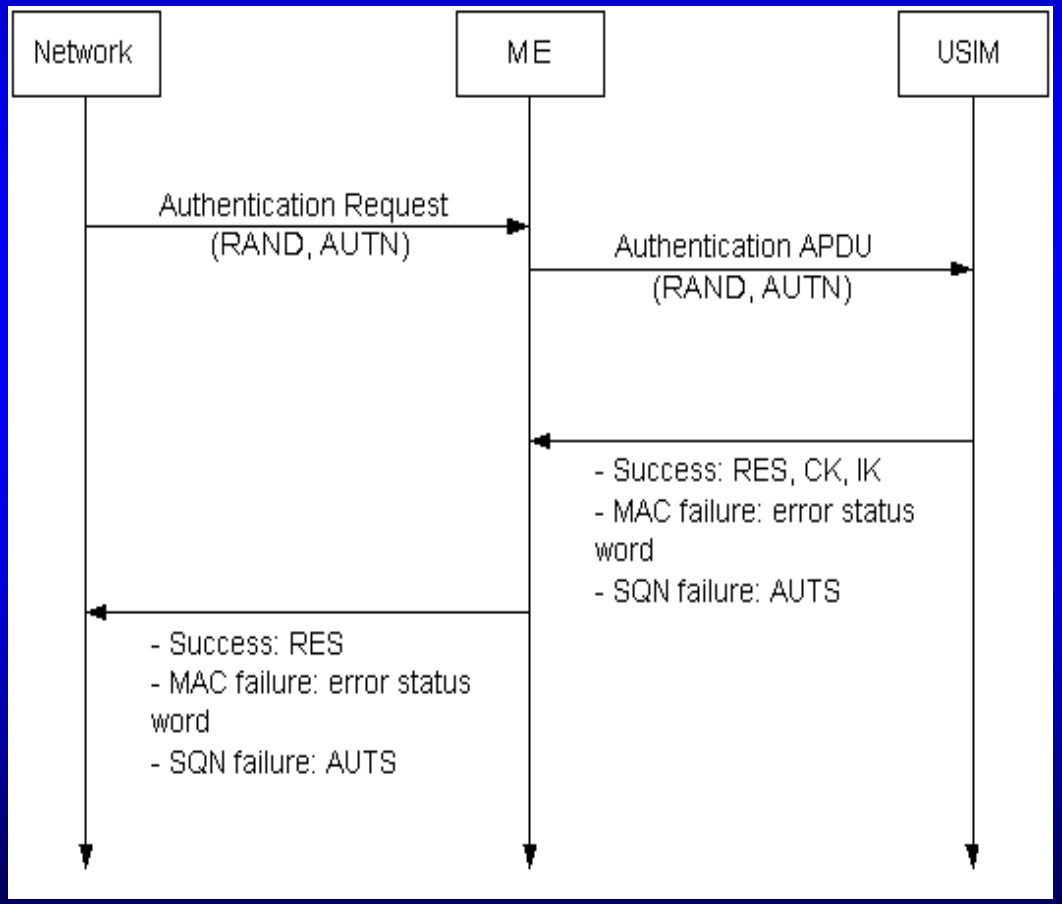
# Overview of Mobile Communication Security (2G)

- Global System for Mobile Communications (GSM)
  - Digital system including a Subscriber Identity module (SIM)
- Positives
  - Used a secret (Ki) plus an operator defined algorithm, implemented in the card (& network) – only session key and authentication result left the card
  - IMSI/TIMSI used instead of phone number to help caller anonymity
  - Radio interface confidentiality for caller via session key encryption
- Negatives
  - The example algorithm (Comp128-1) which was meant to be kept secret was leaked & found to be weak and then attacked
  - Because the Base station was not authenticated by the user it was possible to have false base station attacks
- RESULT some cloning & false BTS problems
  - Better algorithms exist
  - – but some networks still persist with Comp128-1
- Lessons learned
  - You can't rely on an algorithm remaining secret
  - The algorithm should be well designed
  - (and no weaker when published)
  - Mutual authentication needed



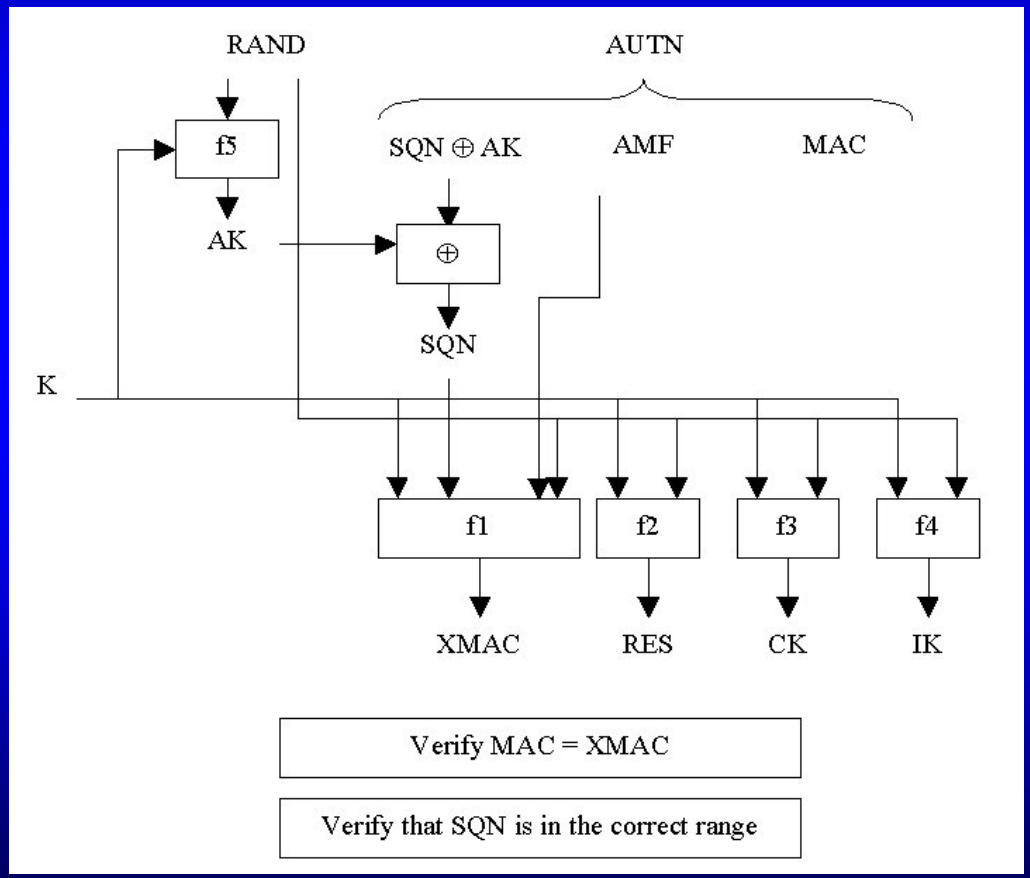
# Overview of Mobile Communication Security (3G)

- Universal Telecommunication System (UMTS)
  - Digital system including a Subscriber Identity module (USIM)
- Positives
  - Added mutual authentication
  - Integrity key, anonymity key
  - Replay attack protection
  - Stronger example algorithm (milenage), designed openly and published by SAGE
  - Core algorithm may be customised to a network operator



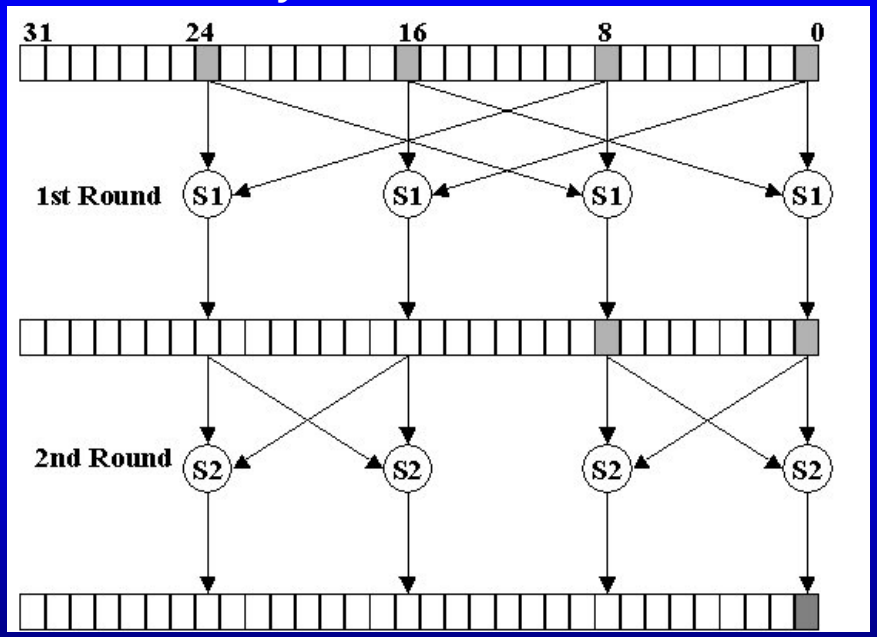
# Overview of Mobile Communication Security (3G)

- Observations
  - A published algorithm makes it easier to implement a clone if you know the secrets
  - Operator customisation (OP) is a global secret (although not usually stored directly on the USIM – instead OPc)
  - Also operator specific R& C values
  - Modern smart cards have sophisticated functionality so there are more secrets than just the 'K' – but how do you get them??



# Logical Attacks on SIM/USIM

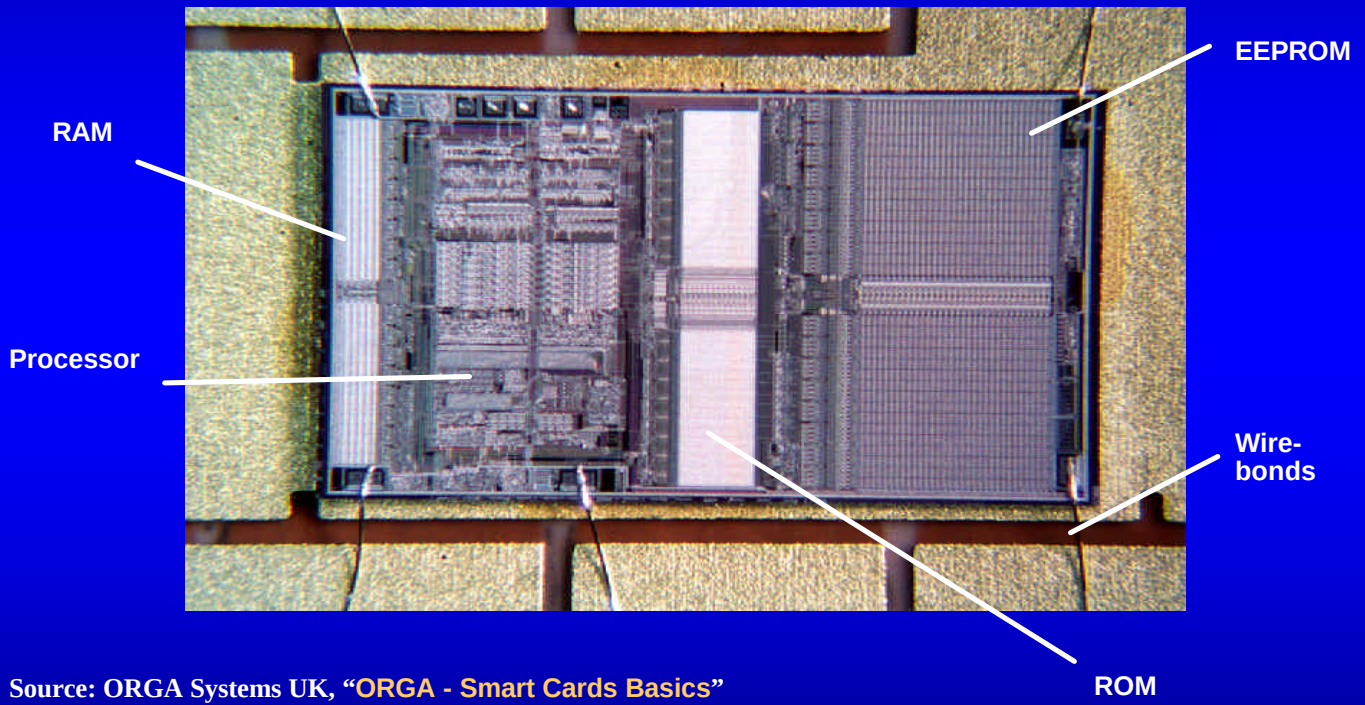
- Logical Attacks = Looking for Bad Design/Implementation
  - Repeated attempts (brute force)
  - Overflow, look for bugs/errors
- Comp128-1 Example
  - Algorithm had 128 bit key so how could brute force be feasible?




- General Verdict
  - Would be very lucky indeed to succeed against modern, well implemented USIM smart card

# Physical Attacks on SIM/USIM (1)

- Physical Attacks = Direct tampering with chip hardware
  - Reading memories/monitoring busses
  - Modifying circuitry, Reverse engineering algorithms



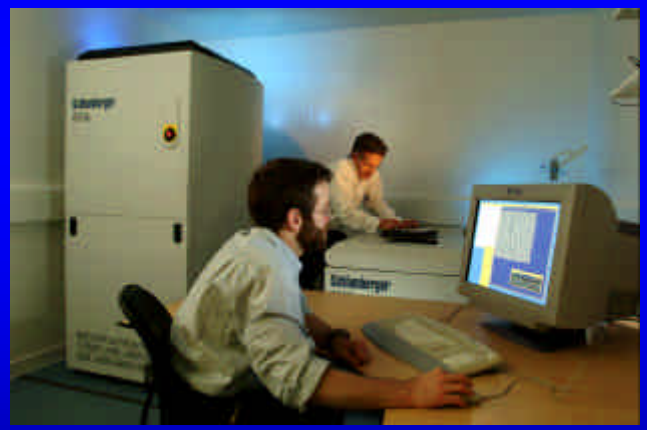

Source: ORGA Systems UK, "ORGA - Smart Cards Basics"

- Modern chips have sophisticated countermeasures
  - Physical and active shields
  - Scrambled circuit layout
  - Encrypted memories and busses
  - Tamper detection sensors

# Physical Attacks on SIM/USIM (2)

- Physical Attacks - what you need….
  - Old SIM technology – perhaps just a Probe Station
    - $10,000 e-bay?
  - New SIM/USIM technology need proper preparation and FIB equipment
    - $100,000 - $1,000,000?



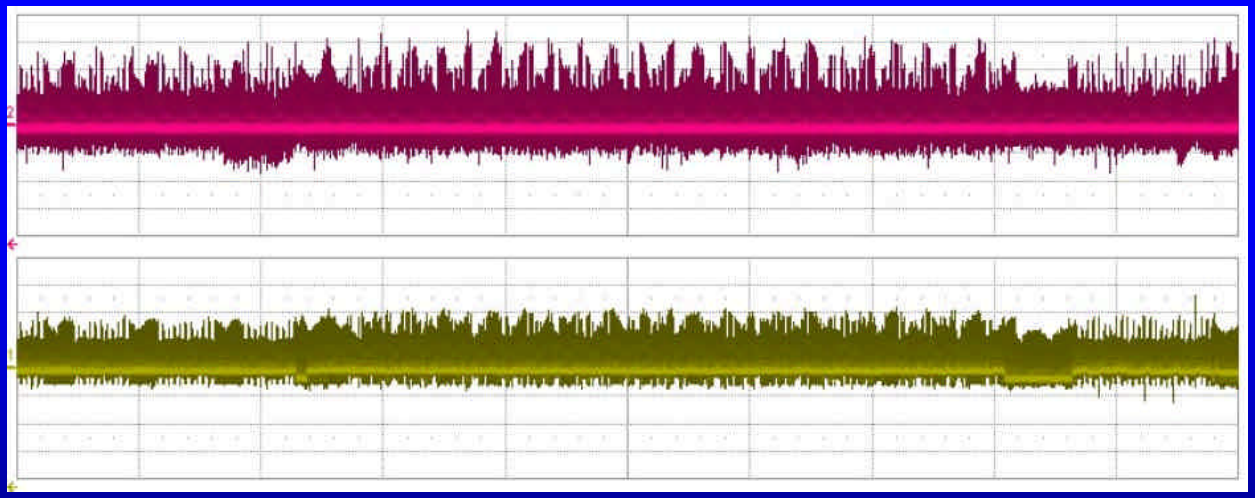


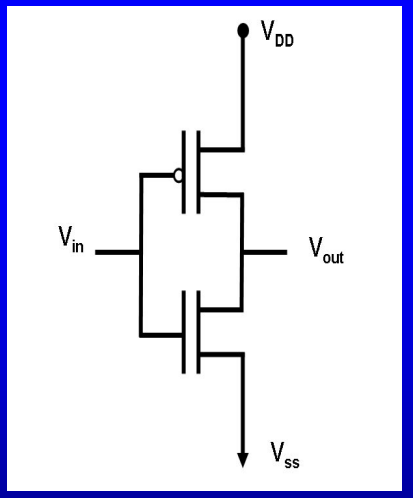
Pictures from SiVenture www.siventure.com

- General Verdict
  - A determined/well-equipped attacker will eventually succeed – but what is gained if there are no global secrets?

# Side Channel Attack on SIM/USIM

- Side Channel Attack – exploits information leakage, usually via variation in electrical current or electromagnetic radiation
  - Far less equipment than Physical attack
  - Require high speed capture & analysis expertise
  - Smart card not necessarily damaged






- General Verdict
  - Should not be practical against well designed & tested modern SIM/USIM
  - Countermeasures obscure the leaked information

# Secret Response Data & Back Door Cloning

- When a batch of USIM cards is ordered the supplier is sent an input file that sets the initial values and customisation parameters for use in the cards
- The supplier generates a response file that is intended for loading into the Authentication centre
- It may be sent to the customer in a PGP encrypted file
- A “trusted employee” will see the information in clear
- The data should be encrypted in the AuC but this is doubtful
- If this file is leaked by “trusted employees” or IT managers then widespread cloning is possible regardless of the design/implementation of the normal smart card solution.
- The file could provide all secret data associated with say 1 million cards - & this is not just the ‘K’ values

# What's in a File ?

- Input file
  - Could contain OP & R/C values used to customise the milenage algorithm – i.e. global secrets
  - The values could be changed per supplier and per batch – but its doubtful that all networks will do this
- Output File may include
  - ICCID, IMSI, K
  - User PINS/PUKS
  - Administrative PINS
  - Card Manager PIN
  - OTA Keys
- Aside from cloning a hacker could create havoc with this data

# *Impact of Cloning ?*

- Cost
  - If SIM costs sat $4 then to replace it normally costs about $40 due to admin systems, customer care, database changes etc
  - To investigate a suspected or claimed clone can be much more expensive - requires technical staff and use of databases and fraud engine equipment
- Fraud opportunity
  - If $100 of calls can be made before a clone card is detected and disabled then our response file could be worth $100 Million to organised criminals
    - Worth paying a corrupt employee $1Million for it
  - Opportunist individuals may also make false claims of cloning – knowing it is cheaper for the operator to refund them than investigate the case

# Practice of Cloning ?

- The Clone business works if a suitable T=0 plug-in smart card platform can be obtained and programmed with at least the following information;
  - Algorithm (plus customisation)
  - Main secret key ‘K’
  - IMSI
- If we assume an “inside-man” then we have all the information we need for to populate a clone card
- The clone stations is simply a PC with a card reader
- Today there are many available clone cards to chose from including sophisticated T=0 java card platforms.
  - Some are not supplied in plug-in form but it is simple to punch them from full sized cards.

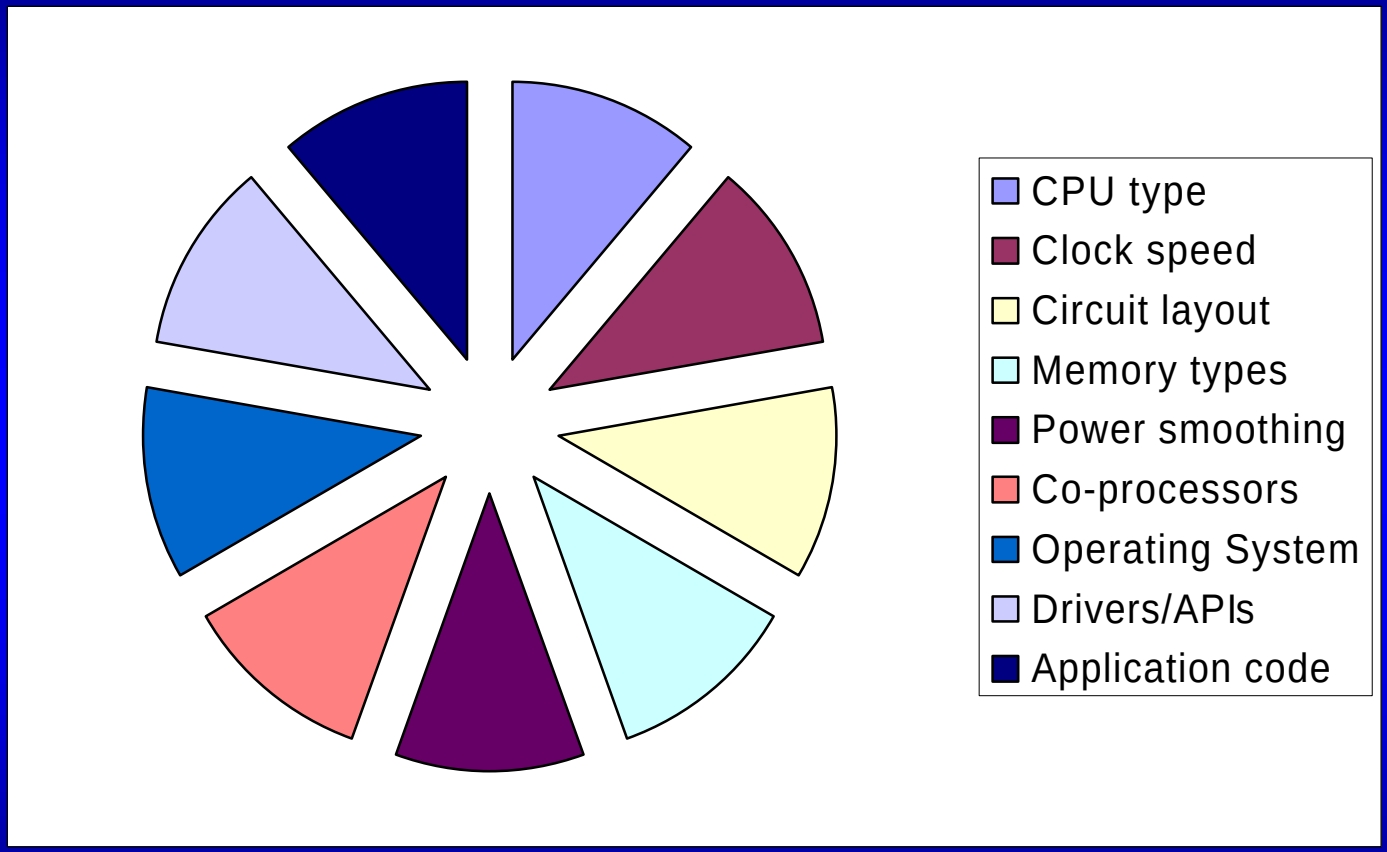
***….However the clone is unlikely to be implemented on the same platform type as the genuine original….***

# *How can we practically detect the platform type?*

- It must be assumed that the clone could recreate the logical functionality of the original
- A “secret” cannot be used as we assume that all such info has been compromised
- The normal communication channel is not reliable to determine the platform type but what about a side-channel?
- The easiest side-channel to monitor would be the supply current for the card –as used in power analysis attacks

# Side Channel Signal Contributions

- Several elements contribute to the leaked signal

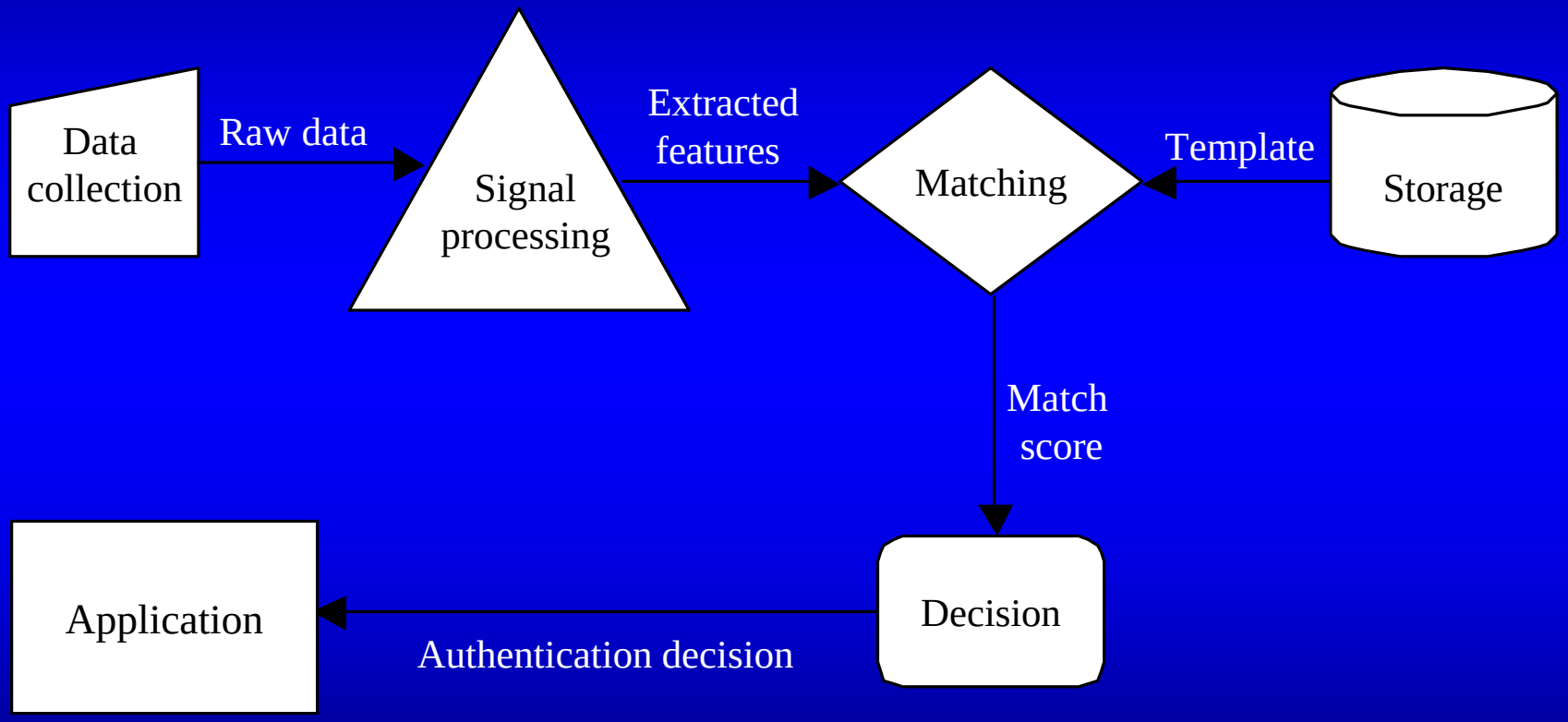



- Whilst the clone may duplicate the application, there are other elements outside its control
- But the leaked signal is not secret – so is it still of use?

# *Biometric Analogy*

- Human biometrics may be regarded as “leaked” or “side-channel” information about identity e.g.
  - Finger-print
  - Appearance
  - Voice pattern
  - Iris pattern
- The information is regarded as having great value in identity/authentication systems
- The information is not secret but is relatively easy to collect yet difficult (not  impossible) to recreate

# Biometric System Model

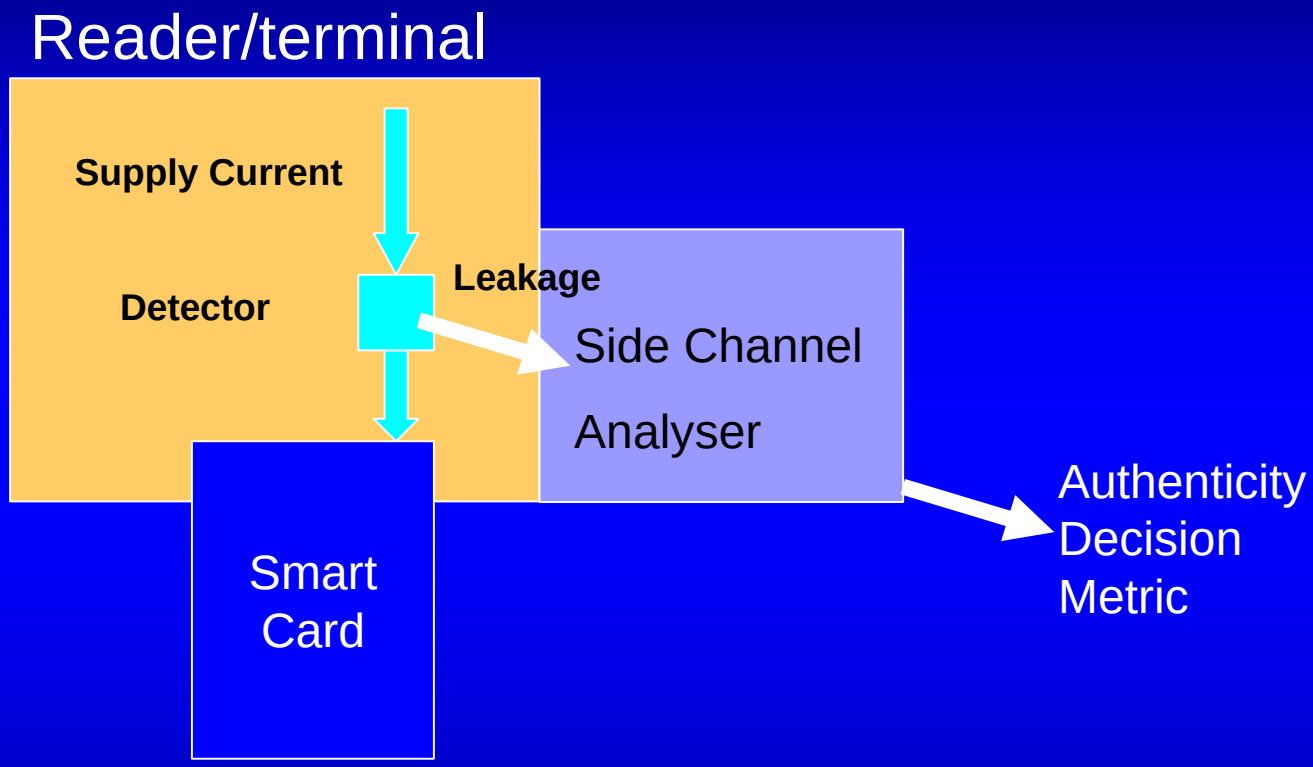



- Normally we try to put biometric matching algorithm and templates in tamper resistant hardware – e.g. smart cards
- However we can't use this approach for card platform "fingerprinting"

# *"Platform Fingerprint" qualities*

- Data Collection
  - Simple resistor carrying the supply current
  - Attack detector might normally have say 300MHz bandwidth & say 100Mbs/s -1Gb/s sample
- Feature Extraction
  - Waveform or statistical features
  - Speech compression analogy
- Template storage/Matching/Decision
  - Would need to be in reader/network
- Spoofing
  - Specialised equipment could recreate convincing signals
  - Cheap smart card platform could not – the transitions are at the clock/transistor level so very difficult to influence and control

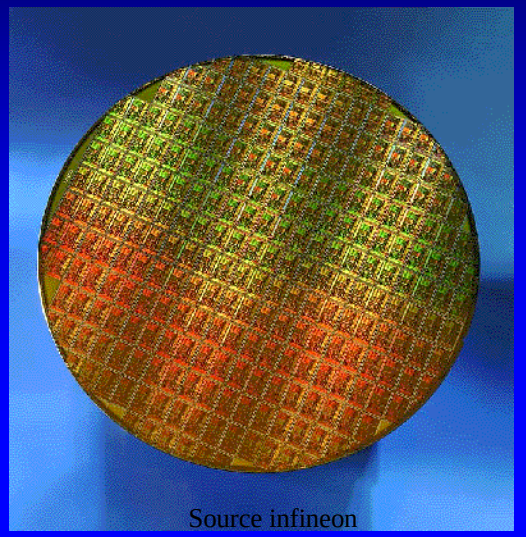
# Platform leakage detector

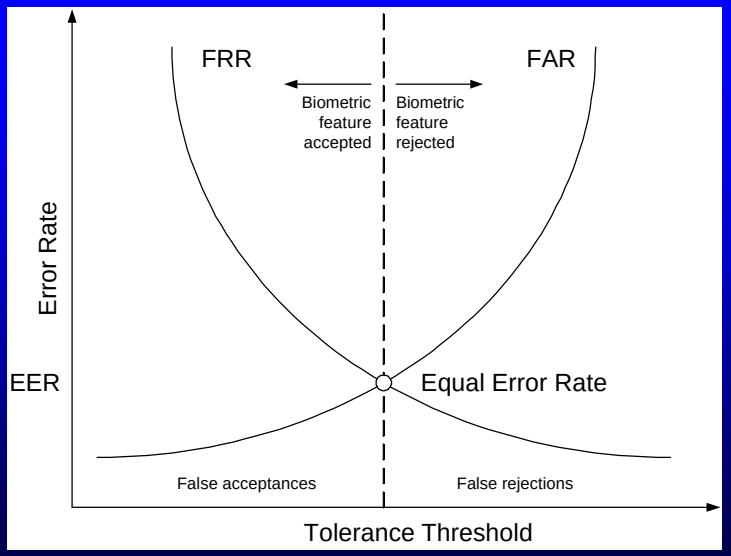



- An authenticity decision is made based on the side channel leakage
- The decision is independent of the logical function of the smart card (which would have been duplicated in the clone)

# Perceived problems (1)…

- Side channel signals can vary with environmental conditions such as temperature and voltage and so a card may not always give a consistent result
- Smart card chips are produced on silicon wafers and there are slight fabrication tolerances between wafers and across the surface of particular wafers - so chips may not “leak” identically
- The tolerances may give rise to false acceptance and false rejection curves similar to those in biometric detectors


Source infineon



# Perceived problems (2)…

- Side channel signals are normally associated with attacks on smart cards rather than the detection of clones
- Attack countermeasures including random delays, power smoothing, added noise etc - may reduce the usefulness of the detected signal
- It might be possible to produce the equivalent of an un-protected training sequence before normal processing – however the countermeasures may be very low level and difficult to enable/disable
- The countermeasure effects might be overcome by using attack techniques
- Gathering statistical data over a long period may allow information to be retrieved and used in a more confident authenticity detector
- The statistical gathering may not be appropriate for an ATM where the transaction is relatively short however might be considered for a phone that is in constant contact with the SIM/USIM

# Concluding Remarks

- Mobile communication security has evolved, learning from the lessons of the past
- Whilst dependency on algorithm secrecy has eased, fundamentally the entire solution relies on network information being kept securely
- If this secret information is sold/leaked then the prospect of wide-spread cloning remains
- Many clone platforms are available but they are unlikely to be the same as the originals
- Side channel leakage from smart cards results from many platform influences and cannot easily be recreated on an alternative platform
- Side channel leakage is therefore a candidate for the detection of authentic and cloned card platforms having properties that are analogous to biometrics
- The use of this signal is not without problems arising from tolerances and countermeasures used to protect conventional side-channel attacks

# Refs


- M. Mouly, M-B Pautet, The GSM System for Mobile Communications, Cell & Sys. Correspondence 1992
- GSM & UMTS – The Creation of Global Mobile Communication – Wiley 2002
- COMP128-1 attack - http://www.isaac.cs.berkeley.edu/isaac/gsm-faq.html
- SAGE S3-000730.pdf – General report on the design, specification and evaluation of the Milenage algorithm set – ETSI 22.11.2002
- M. Witterman - Advances in Smartcard Security - Information Security Bulletin July 2002
- M. Aigner and E. Oswald. "Power Analysis Tutorial" Institute for Applied Information Processing & Communications - University of Technology Graz.
- Kocher, P., Jaffe, J. and Jun, B. (1999), Differential Power Analysis. In Wiener, M. (Ed.), Advances in Cryptology – CRYPTO '99 Proceedings (pp. 388–397). LNCS 1666, Springer-Verlag.
- A. Matthews "Electromagnetic Analysis on DES", MSc Project Report 2005, submitted as part of the Masters in Information Security at Royal Holloway University of London.
- Anderson, R. and Kuhn, M. (1996), Tamper Resistance – a Cautionary Note, In the Second USENIX Workshop on Electronic Commerce Proceedings (pp. 1–11)
- S. Scwiderski-Grosche - An Overview of Biometrics, ISG IC3 Module 2004 – Royal Holloway University of London
- O. Kocar – DPA attacks on keys stored in CMOS cryptographic devices through the influence of the leakage behavior – IACR Cryptography ePrint Archive 192/2006
- W. Rankl and W. Effing – Smart card handbook 3rd edition John Wiley 2000

# *Thank you for your attention ☺*

- Questions?


- Keith.mayes@rhul.ac.uk
- www.scc.rhul.ac.uk
- www.isg.rhul.ac.uk
- www.rhul.ac.uk