Supplemental Access Control

Tom Kinneging

ISO/IEC JTC1 SC17 WG3/TF5

New Technology Working Group (NTWG)

TAG/MRTD 19

19th Meeting of the Technical Advisory Group on Machine Readable Travel Documents

Doc 9303 Volume 2 Evaluation

- Specifications celebrate 5th anniversary
  - Technology evolution
  - Increasing computer power
- Technical Report “LDS and PKI Maintenance”
  - Preserve level of accuracy and security
  - Next TAG
- IP02: “LDS and PKI Maintenance”

Basic Access Control Entropy

- Document Number
  - Numeric: 10^9 possibilities → 30 bits
  - Alpha Numeric: 36^9 poss. → 46 bits
- Date of Birth
  - Oldest traveler 100 years: 365*100 poss. → 15 bits
- Date of Expiry
  - 5 years validity: 365*5 poss. → 11 bits
  - 10 years validity: 365*10 poss. → 12 bits

Basic Access Control Entropy

- Limitation
  - Sequential Document Numbers
  - Correlation Document Number – Expiry Date
  - Limitation Expiry Dates
  - Guessing the age of the bearer
- Practical entropy estimation
  - 50 bits – random alphanumeric Document Number
  - 40 bits – sequential numeric Document Number

Strong or Weak?

- Skimming
  - Short distance
  - Chip is slow
  - Delay on false attempts
- Eavesdropping
  - Longer distance
  - Off line attack

Moore’s Law

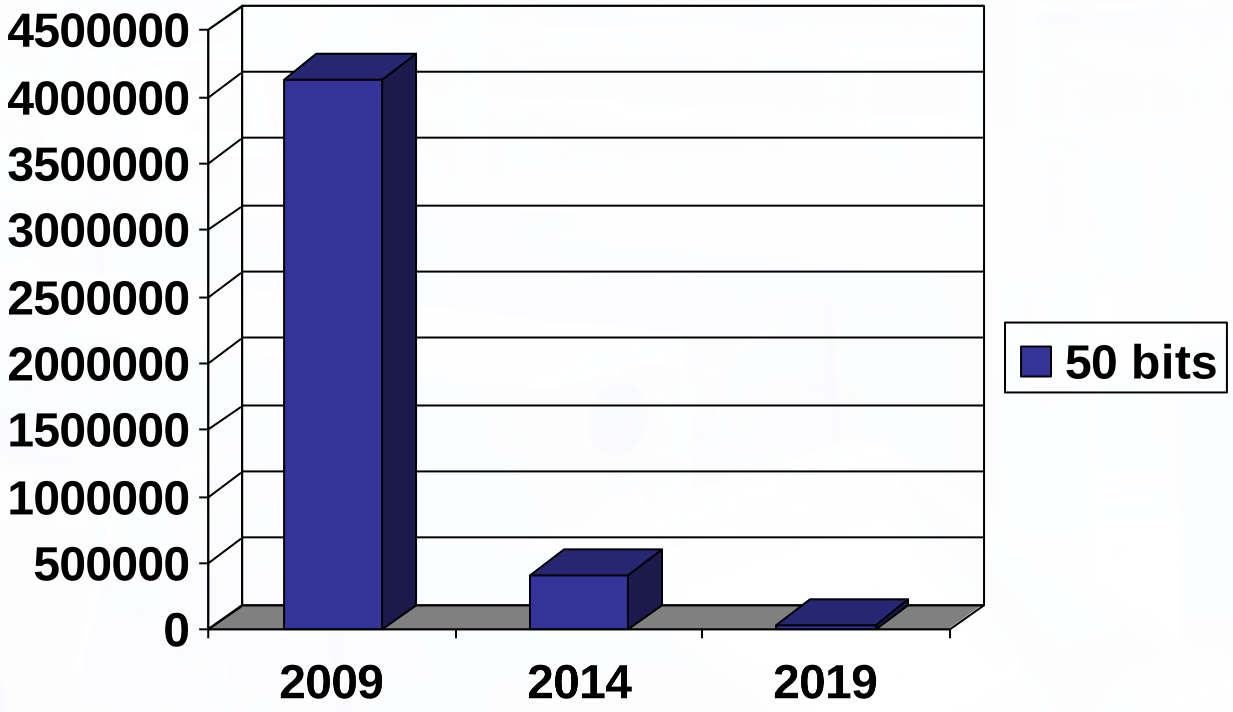
- Every 18 months
  - Double speed
    or
  - Half the price
- 1998: Deep Crack
  - $250,000 – 88,000,000,000 DES keys/s
- 2006: Copacobana
  - $10,000 – 65,000,000,000 DES keys/s

Moore’s Law and BAC

- Entropy
  - 40 – 50 bits
- Validity period
  - 5 or 10 years
  - 2009 → 2014 → 2019

Moore’s Law and BAC

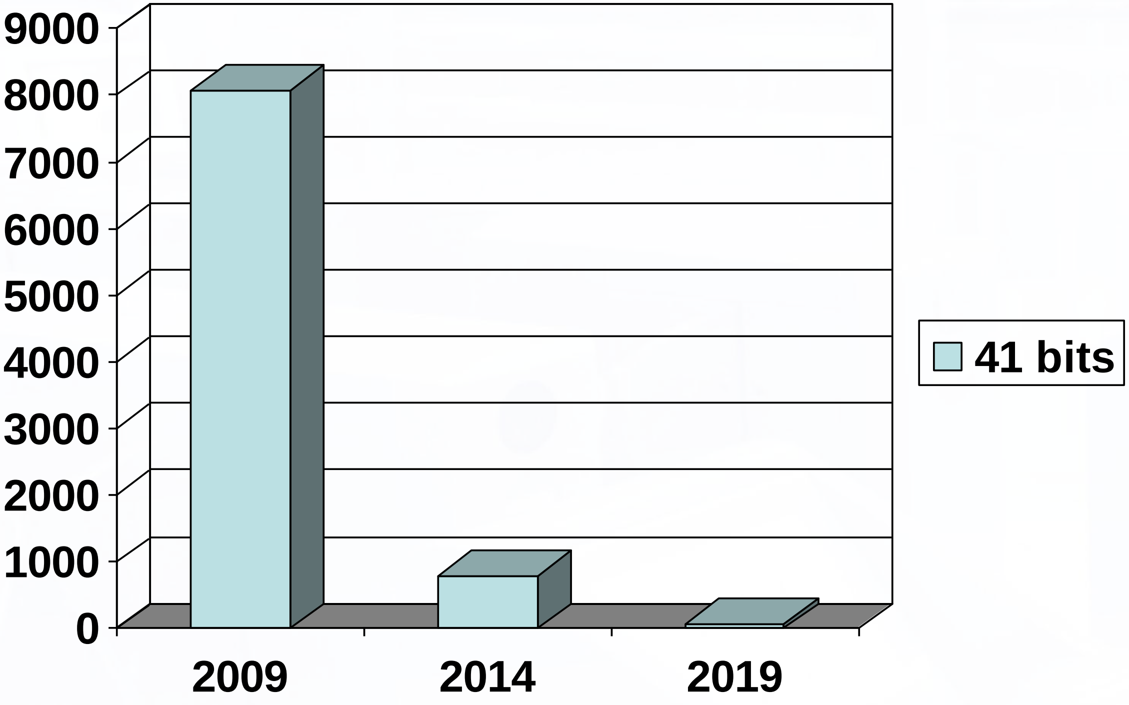
- 1 hour



$ 4,128,509 $ 409,600 $ 40,637

Moore's Law and BAC

- 1 hour



$ 8,063 $ 800 $ 79

Supplemental Access Control

- Based on PACE V2
  - Password Authenticated Connection Establishment
- Similar to Basic Access Control
  - Enforces Authorized Access
  - Secure Communications
- Less influence of entropy on strength
  - 6 digits number sufficient

Supplemental Access Control

- MRZ
  - Document Number, Date-of-Birth, Date-of-Expiry
  - Mandatory
- CAN
  - Card Access Number
  - On data page or front side of td1 card
  - Optional

Patent Consideration

- Generic mapping
  - Diffie Hellmann
  - Elliptic Curve Diffie Hellmann
- Integrated mapping
  - Diffie Hellmann
  - Elliptic Curve Diffie Hellmann → patent pending IP01: “SAC Patent Consideration”

Implementation strategy

- BAC default access control mechanism
- SAC optional and *supplemental*
  - Inspection systems SHOULD use SAC if present on MRTD
- Gradual change over in 10-20 years

Working Paper

- The TAG-MRTD is invited to
  - Recognize the necessity to specify an access control mechanism supplementary to Basic Access Control
  - Mandate the NTWG to negotiate the solutions with respect to the mentioned patent consideration and incorporate the conclusion in the final version of the Technical Report
  - Approve the Technical Report “Supplemental Access Control” containing this specification for inclusion into Document 9303
  - Promote the implementation of “Supplemental Access Control” in eMRTDs and Inspection Systems within a period of 5 years from the date of this Working Paper

Thank you for your attention

Tom Kinneging

ISO/IEC JTC1 SC17 WG3/TF5