AA∀∀AaAA

AAAA AAtuAAAA

AAAn∀∀∀∀AAAA∀ɐAAaAAA∀ ∀n∀u AAAuuAA AaA

AAUA aA aAAAAaAA AAaAAUAA AA AA AAAAA AaAU AU AA AA AAaUA UAAAAa

AAAAAaAA a∀tu∀∀ ∀∀∩∀∀ ɐ∀∀∀AA AAA ∀ ∀∀∩∩∀∩ ∀∀∀ ∀∩∀∀∀∀∀∀∀A AAAAaAA

A AA∀∀∀ ∀∀ɐAaAuA AAaAu

Au ∀∀ɐ∀∀ AAAu AAAAAu uA AAtAAaAu AAu ɐ∀∀n∀AA A

• •• •

∀AAaAtAAAAAA∀uA∀∀∀∀∀∀∀∀∀AAu tAAAaAtut AAA AAAAuAAA AAA∀

AA A∀AAaA AAAA ɟ∀ɟ ∀∀∀ ∀ɐu AAu A∀∀ ɟu∀∀uA

a AaAt

AA tAAAA A$_{∀}$ $_{∀∀}$tAAAA AAAuuA aAt a tu$_{∀ɐ∀ɟ}$ ∀∀∀ AAu AA$_{∀∀∀ՈՈ}$ ՈՈ∀^{A}

AAUAA aAt AAUA UAAA∀∀Ո∀ ∀∀∀ ∀∀∀∀ɐ∀Ո∀ ∀∀∀∀ ∀ɐ∀ ∀Ոɟ ∀∀ ɐ ∀Ո∀

aAAaAAA ∀ ∩AAAU A∀∩∀∀∀∀∀ɐ∀ UaAAUAAUAA AaAAAAA A∀ɐU a AUA AA AAU

Aat AA ɐ∀Ո AAA AAAuAAA AAA AAAA AuaAAAA AAu A Ո∀ɐ∀∀ ∀ AuAtuAuAtut

AAU tAAAUAAUA AAAUAAA AAU AAAAAAAAAUA ᵍ∀ ∀∀∀∩∀ɟ∩ɟ ∀∀ ∀∀∀

ℒ

aA AAA AAAU a ∩∩∀ ∀∀∀ ∀∀ UaAAA ∩ A∩UAA AAaA a∀AAU AA AA∀∩UAAUAAU

∀∩∀∀AAAAAAAA∀∀∩∀∀ɟɟ

AAUA∀∀ɐ∀ɟ∀∀ɐ∀∀∀∀ɐ∀∀AAAa∀ɐ∀∀∩∀∀∀∩∀ɐ∀∀∀∀∀

AuAAAuAuaAAAAAAAAAuuAAAAaAAAꓵ∀∀∀ꓵ∀AAaAAuAAuAA

AA∀∀∀ɟAAAAuAuAAA

4.1 Why the threat model was wrong

During the 1980s, there was an industry wide consensus on the threat model, which was reinforced at conferences and in the literature. Designers concentrated on what could possibly happen rather than on what was likely to happen, and assumed that criminals would have the expertise, and use the techniques, of a government signals agency. More seriously, they assumed that implementers at customer sites would have either the expertise to design and build secure systems using the components they sold, or the common sense to call in competent consultants to help. This was just not the case.

So why were both the threat and the customers' abilities so badly misjudged?

The first error may be partly due to an uncritical acceptance of the conventional military wisdom of the 1970s. When ATMs were developed and a need for cryptographic expertise became apparent, companies imported this expertise from the government sector [C3]. The then current military model stressed secrecy, so secrecy of the PIN was made the cornerstone of the ATM system: technical efforts were directed towards ensuring it, and business and legal strategies were predicated on its being achieved.

Nowadays, however, it is clear that ATM security involves a number of goals, including controlling internal fraud, preventing external fraud, and providing fair arbitration of customer disputes. This diversity was just not understood well enough in the 1970s.

The second error was probably due to fairly straightforward human factors. Many organisations have no computer security team at all, and even if they do, they have a hard time finding it a home within the administrative structure. The internal audit department, for example, will resist being given any line management tasks, while the programming staff dislike anyone whose rôle seems to be making their job more difficult.

Security teams thus tend to be 'reorganised' every few years, leading to a loss of continuity; and in the rare cases where a security department manages to thrive, it usually has difficulties attracting and keeping good engineers (who get bored once the initial development tasks have been completed). For example, a recent study shows that the average tenure of computer security

• • •

∀∀n∀ɐ∀n∀uAAAAuu

AAAAAt∀∀∀∀∀n∀nn∀∀∀∀∀∀ɐ∀∀∀∀∀ɐuaAAuAAAutun∀∀∀n∀∀∀∀∀∀∀∀ɐ∀n∀∀

$\mathrm{AUAUAAA}_{\forall\cap}\mathrm{UaAUtAAAAU}_{\forall\forall g\forall\forall\forall\cap\forall\forall\forall\forall\forall\forall g}{}^{\mathrm{Aa}}{}_{\cap\forall\forall\forall\forall\forall}{}^{\mathrm{UaAA}}$

$\cap\cap\forall\ \forall^{\mathrm{AUAA\ AA}}$

[DP] DW Davies and WL Price, *'Security for Computer Networks'*, John Wiley and Sons 1984.

[E] J Essinger, *'ATM Networks - Their Organisation, Security and Future'*, Elsevier 1987

[G] J Gleick, *'Chaos'*, Cardinal, 1988

[GO] G Garon and R Outerbridge, "DES Watch: An examination of the Sufficiency of the Data Encryption Standard for Financial Institution Information Security in the 1990's, in *Cryptologia*, **XV**, no. 3 (July 1991) pp 177 - 193

[H] HJ Highland, "Perspectives in Information Technology Security", in *Proceedings of the 1992 IFIP Congress, 'Education and Society', IFIP A-13 vol II* (1992) pp 440 - 446

[ITSEC] *'Information Technology Security Evaluation Criteria'*, June 1991, EC document COM(90) 314

[J] RB Jack (chairman), *'Banking services: law and practice report by the Review Committee'*, HMSO, London, 1989

[JAJP] HL Johnson, C Arvin, E Jenkinson, R Pierce, "Integrity and assurance of service protection in a large, multipurpose, critical system" in *proceedings of the 15th National Computer Security Conference*, NIST (1992) pp 252 - 261

[JGKLM] DB Johnson, GM Dolan, MJ Kelly, AV Le, SM Matyas, "Common Cryptographic Architecture Application Programming Interface", in *IBM Systems Journal* **30** no 2 (1991) pp 130 - 150

[K1] D Kahn, *'The Codebreakers'*, Macmillan 1967

[K2] TS Kuhn, *'The Structure of Scientific Revolutions'*, Chicago 1970

[L1] B Lewis, "How to rob a bank the cashcard way", in *Sunday Telegraph* 25th April 1992 p 5

[L2] D Lane, "Where Cash is King", in *Banking Technology*, October 1992, pp 38 - 41

[M1] S McConnell, "Barclays defends its cash machines", in *The Times*, 7 November 1992

[M2] R Morris, invited lecture given at Cambridge 1993 formal methods workshop (proceedings to appear)

[M3] JA McDermid, "Issues in the Development of Safety Critical Systems", *public lecture, 3rd February 1993*

[MB] McConville & others v Barclays Bank & others, High Court of Justice Queen's Bench Division 1992 ORB no.812

[MM] CH Meyer and SM Matyas, *'Cryptography: A New Dimension in Computer Data Security'*, John Wiley and Sons 1982.

[N] I Newton, 'Philosophiae Naturalis Principia Mathematica', University of California Press 1973

[NSM] *'Network security Module - Application Developer's Manual'*, Computer Security Associates, 1990

[NSP] *New Security Paradigms Workshop*, 2-5 August 1993, proceedings to be published by the ACM.

[P] WR Price, "Issues to Consider When Using Evaluated Products to Implement Secure Mission Systems", in *Proceedings of the 15th National Computer Security Conference*, National Institute of Standards and Technology (1992) pp 292 - 299

[RM] R v Moon, *Hastings Crown Court*, Feb 92

[RSH] R v Stone and Hider, *Winchester Crown Court* July 1991

[SSWDC] L Sutterfield, T Schell, G White, K Doster and D Cuiskelly, "A Model for the Measurement of Computer Security Posture", in *Proceedings of the 15th National Computer Security Conference*, NIST (1992) pp 379 - 388

[VSM] *'VISA Security Module Operations Manual'*, VISA, 1986

[W1] G Welchman, *The Hut Six Story*, McGraw-Hill, 1982

[W2] MA Wright, 'Security Controls in ATM Systems', in *Computer Fraud and Security Bulletin*, November 1991, pp 11 - 14

[W3] K Wong, 'Data security - watch out for the new computer criminals", in *Computer Fraud and Security Bulletin*, April 1987, pp 7 - 13