IV

SATAN AND MURPHY

R M Needham

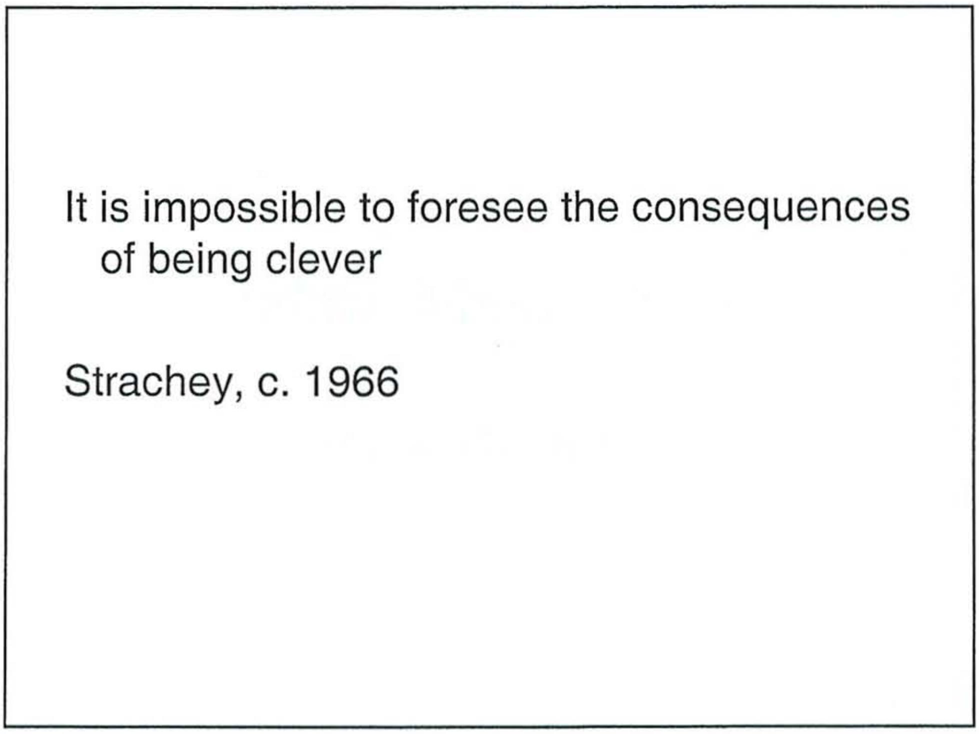
Rapporteur: Dr J A Smith

Satan and Murphy

Roger Needham

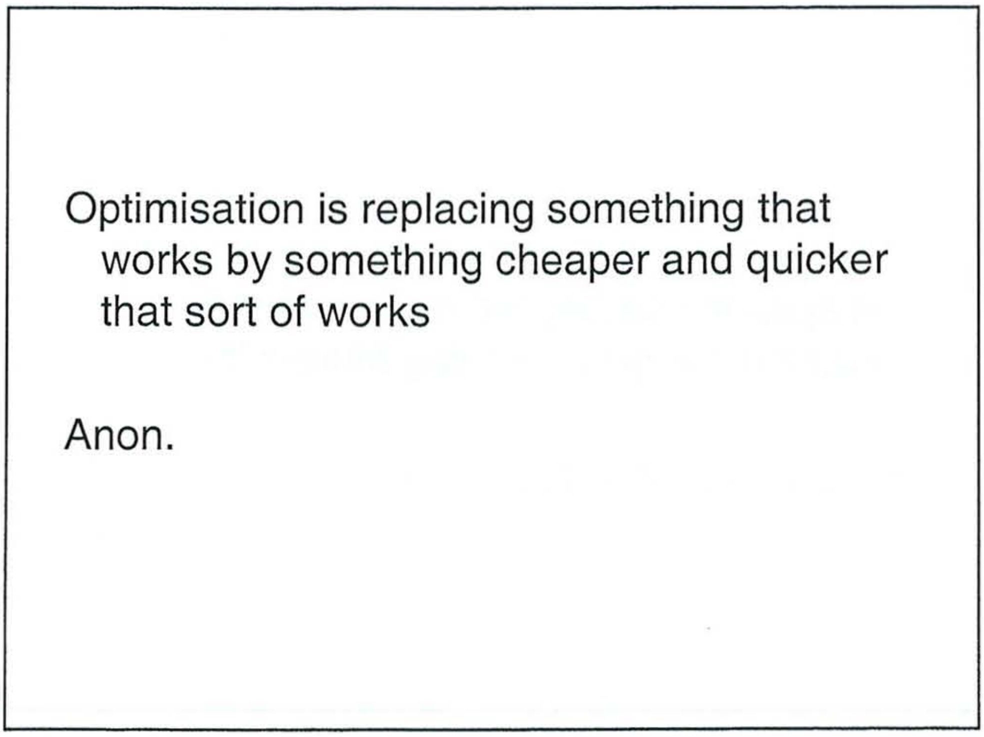
We hope that the lessons learned from programming Satan's computer may be helpful in tackling the more common problem of programming Murphy's

Anderson & Needham, 1995



It is impossible to foresee the consequences of being clever

Strachey, c. 1966



Optimisation is replacing something that works by something cheaper and quicker that sort of works

Anon.

Tradition in security protocols

- Minimise number of messages
- Minimise amount of stuff sent
- Minimise amount of stuff encrypted

Result:

Frequent errors

Woo & Lam's protocol

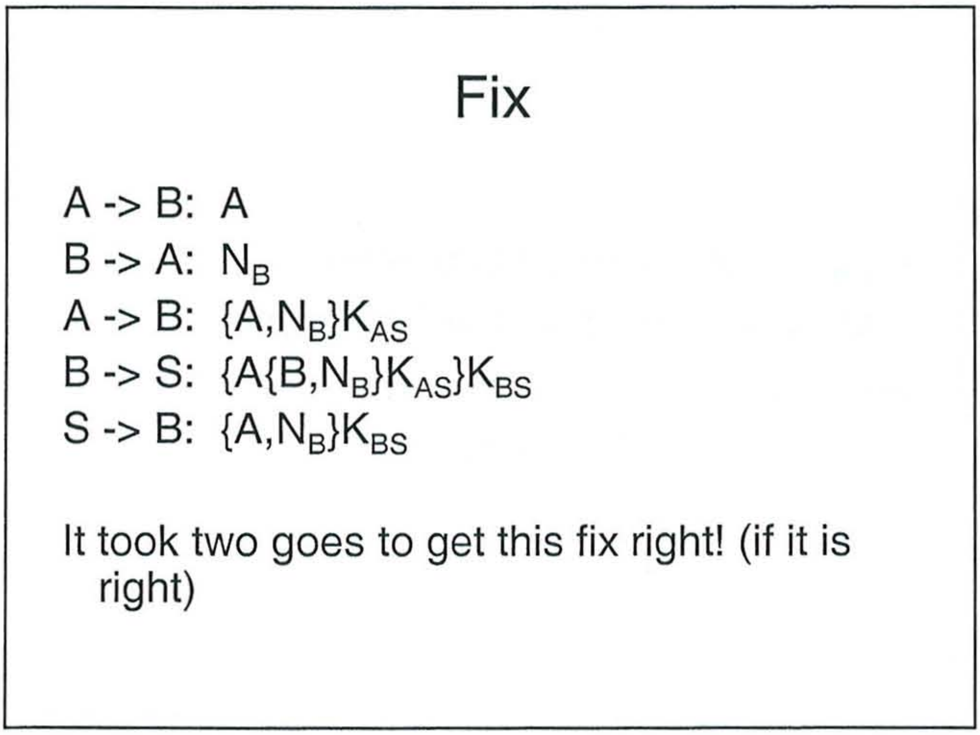
A -> B: A

B -> A: N_B

A -> B: $\{N_B\}K_{AS}$

B -> S: $\{A\{N_B\}K_{AS}\}K_{BS}$

S -> B: $\{N_B\}K_{BS}$



Fix

A -> B: A

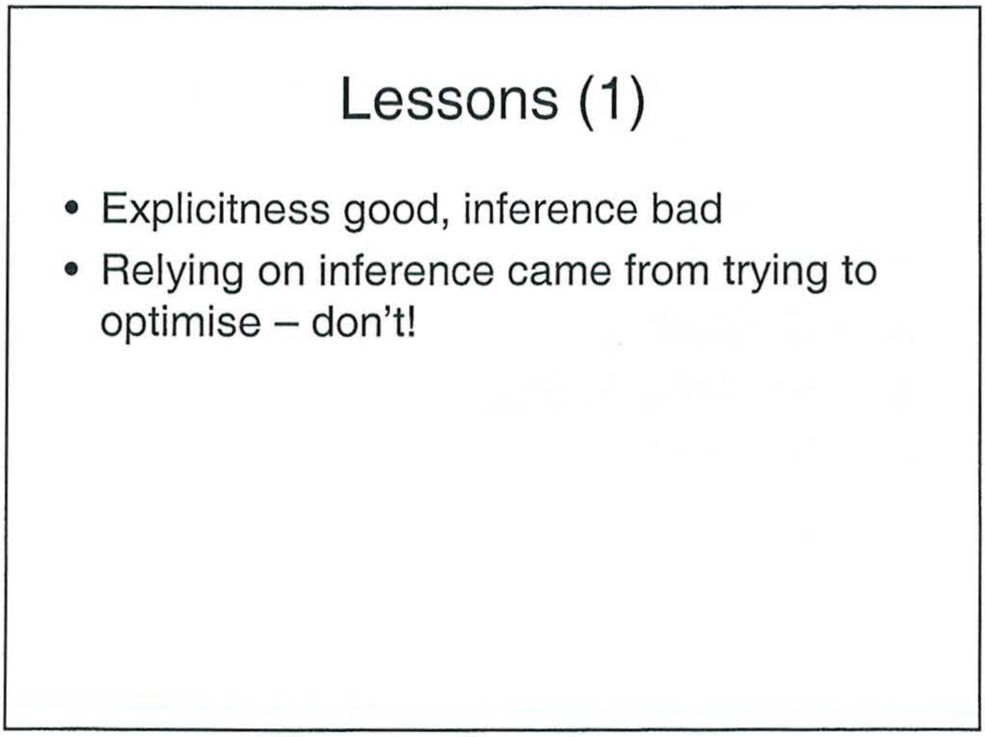
B -> A: N_B

A -> B: $\{A,N_B\}K_{AS}$

B -> S: $\{A\{B,N_B\}K_{AS}\}K_{BS}$

S -> B: $\{A,N_B\}K_{BS}$

It took two goes to get this fix right! (if it is right)



Lessons (1)

- Explicitness good, inference bad
- Relying on inference came from trying to optimise – don't!

Lessons (2)

- Be clear as to goals. One could say that anyone who could interfere enough to defeat the Woo and Lam protocol would be able to hijack the session anyway.
- Is it POSSIBLE to be clear about this? It may be a Satan/Murphy differentiator.

A different sort pf problem

- The TMN protocol

A -> S: R_A^3 (mod N)

B -> S: R_B^3 (mod N)

S -> A: $R_A \oplus R_B$

At which point R_B is used as a key.

Simmons' attack

- C and D collude

C -> S: $R_B{}^3R_C{}^3$ (mod N)

D -> S $R_D{}^3$ (mod N)

S -> C $R_BR_C \oplus R_D$

Thus revealing R_B

Lesson

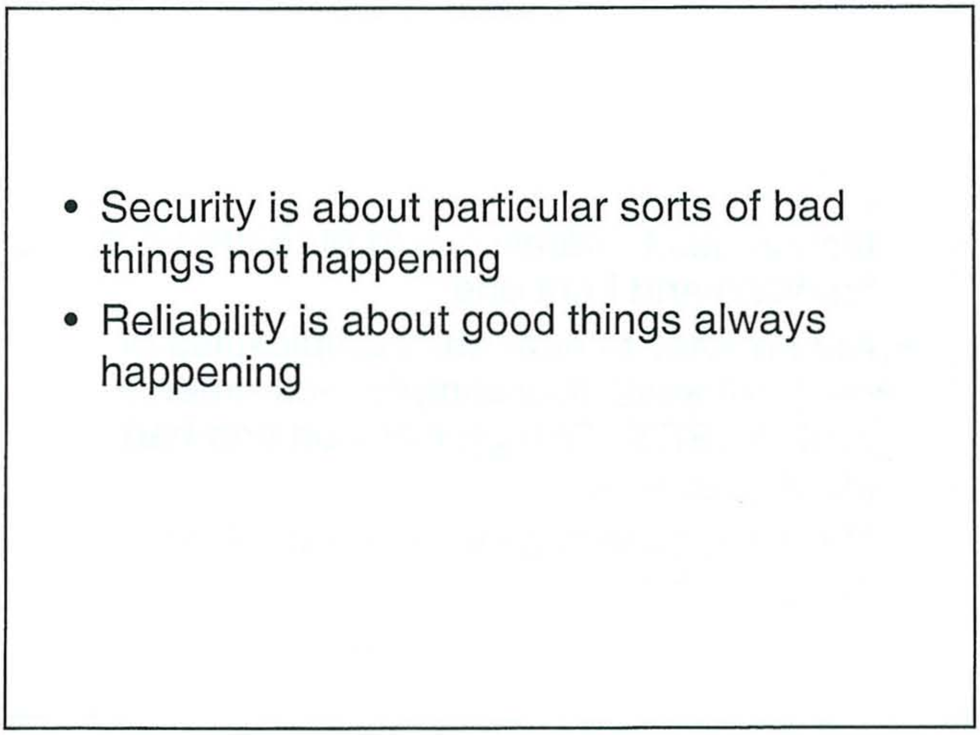
- Remember that other people, particularly villains, may not keep their secrets

Formal techniques

- Huge progress in last decade in formal techniques for dealing with problems like the Woo and Lam one
- Not so easy to deal with complexities of real protocols, for example e-commerce such as SET (Though Paulson has had a lot of success).
- Not so good at attacks exploiting the mathematics

What about reliability?

Does Satan-proof imply Murphy-proof?



- Security is about particular sorts of bad things not happening
- Reliability is about good things always happening

DISCUSSION

Rapporteur: Dr J A Smith

Lecture One

Dr Lomet suggested that surely users require systems to be both secure and reliable, not just secure; that making a system secure (only) is trivially achieved by locking everything in a box and throwing away the key. Professor Needham agreed that a system which never works would be very secure and not much use. He continued to say that some sort of failure is inevitable and, by way of example, that a cash machine which occasionally doesn't deliver money when it should is probably preferable to one which delivers the money when it shouldn't. Overall he agreed that in most cases you want both (security and reliability). Referring to his second presentation, Professor Needham suggested that an important issue is to get agreement about what one should try to achieve by technical means and what one should try to achieve by other measures. In the subject of security protocols, an insecurity is regarded as occurring if there is anything which you could conceivably do which produced the bad result, whereas the engineering difficulty of conducting the attack is very rarely talked about.

Professor Randell suggested that the last slide was really talking about availability rather than reliability, adding that there are many systems where there is a safe stopped state and one tries to achieve that state if necessary. He suggested that a banker who very carefully kept only one set of non-redundant ledgers might be just as liable to a form of security failure as he would to disaster such as flood or fire. Professor Needham agreed, adding that security needs are typically ill-expressed and that stopping people stealing is easy to accomplish trivially. He added that the notion of risk is never mentioned, let alone a quantified notion of risk. He suggested that in general the text books give no hint as to how to design in the face of an assessment of risk, though there is some measure of this in Dr Anderson's recent book on security engineering.

Referring to approaches of minimisation for security and duplication for reliability, Professor Malek mentioned a possible compromise suggested by Michael Rabin whereby a sensitive message is hidden in a flood of data; only the recipient knowing how to extract the significant contents. This he suggested might hint at approaches for security where redundancy is more useful. Professor Needham agreed that this sort of approach may be possible, but suggested that it is not clear how generally applicable the approach would be. He further pointed out that the approach assumes essentially infinite memory and free bandwidth, and is less effective if memory is not infinite and bandwidth not free.

Professor Bloomfield expressed surprise at the apparent lack of any notion of risk or probabilistic metrics in security. Professor Needham suggested that no-one really knows how to do it. He referred to the notion of a "British standard burglar" as a metric for safe design, and added that designers of security systems for cars similarly have an understanding of how difficult it is to break into various cars, but that in the computer security world there is no concept like the British standard burglar and that lack makes quantitative risk assessment very difficult. He pointed out that it is always possible to go on making something more and more secure; the issue being where to stop so as to avoid overkill leading to a completely clumsy and unusable system. He suggested that having a better concept of risk would facilitate deciding where to stop in a more rational way. He also added that banks may have this sort of intuition in connection with their own procedures. He suggested that possibly writers on security have confused themselves by trying to write about their subject in more generality than is appropriate. He explained that in a particular context the designer of a security system can make assessments about the environment, e.g. by talking to bankers or insurance companies, but trying to fully generalise may be just inappropriate.

Professor Randell commented that a lot of the work on security has been done by agencies who have wanted to apply secrecy not just to what they are trying to keep secret but also to the methods they have used to obtain secrecy and that such agencies regard as some of their most valuable knowledge their understanding of what the real risks and statistics about risks are. He compared this with the reliability world where the corresponding information has been public, all-be-it sometimes only after extended court proceedings. He suggested that this difference must have a big impact and asked what sort of knowledge is available to the people who are working in the secrecy area and at least appearing to work in the open. Professor Needham replied that there is not a lot. He added that Dr Anderson points out that in most sorts of engineering progress it is due to exhaustive analysis of failures but that in finance and security the typical reaction to failure is to pretend it hasn't happened, and certainly not to analyse the causes of it. He suggested that this makes security engineering a strange kind of engineering as it typically works without the very piece of methodology which could be said to distinguish engineering from science.