SECURITY - A TECHNICAL PROBLEM OR A PEOPLE PROBLEM

R M Needham

Rapporteur: Dr J A Smith

Security – a technical problem or a people problem?

Roger Needham

Needs (1)

- Security policies. Who is allowed to know what, by role or identity. Who is allowed to do what, when, and how. What sort of information is protected, how many kinds of protection are there?

Needs (2)

- Implementations. Technological support to the policies – cryptographic means of identity verification, physical access control, software-based access control, secure verification of program identity and integrity.

Needs (3)

- Metadata that relates the policy to the mechanisms – access lists, privilege lists, status of individuals.

Needs (4)

- People to construct and maintain the metadata

Thesis

- Many if not most security researchers have worked on Need 2 – the mechanism
- This isn't any longer right, if it ever was

Policies

- In an organisation, vast, informal, and incomprehensible
- No good notation for them
- Some derive from law
- Some from prudence

Real Life Difficulties

- Not altering things that have been signed off

Metadata(1)

- Access lists
- Security libraries
- Role lists

Metadata(2)

- Possibility of error – difficulty of audit
- Problems with new employees
- Distant administrators

Recovery issues

- The Needham-Schroeder Protocol
- Military needs

People

- Are fallible, lazy, and uncomprehending
- Security is a nuisance
- People are good at circumvention
- People don't understand

Agenda

- Can we express security policies so that we can check that technical measures are capable of meeting the requirement?
- Can we check that the implementation plus the metadata do the right thing?
- Can we express local operating rules so that their rationale is apparent to local operators, so they might take them seriously?

DISCUSSION

Rapporteur: Dr J A Smith

Lecture Two

During the talk, Professor Randell asked whether there might be benefit in regard to recovery from security failure from examining reliability, e.g. forward recovery. Professor Needham agreed.

Dr Rushby suggested that the problems Professor Needham described are not unique to security, but are in fact found in all areas where automation is brought to bear on human problems, that human factors people refer to the generic problem as "clumsy automation", and that much of what is done in the area of human centred automation and such topics tries to address these issues. He suggested it might be fruitful to look there rather than the places Professor Needham suggested. Professor Needham replied that this is certainly something that the security community does not address, and that that should be fixed.

By way of counter example to the situation where inaction by security personnel causes difficulty, Professor Malek referred to a problem where a very keen security officer who is always trying to implement the latest methods prevented him this week from accessing his email through implementing some new policy. He asked what would be the right compromise. Professor Needham replied that he didn't know and referred to a paper at the first ACM security conference which gave a horrifying account of security at NASA. He went on to describe how the NASA security group had had a lot of authority and more or less unlimited budget and brought the organisation to a halt. He reported that reassessing how much information was seriously confidential led them to reduce the security group to one person, or so, and they could get on with normal work, though apparently the consequences were particularly dire. He concluded that hyperactivity by security officers is extremely dangerous.

Professor Randell expressed a wish that it had been possible to cite this presentation in the recent dependability IRC proposal. He continued to suggest that closing the loop in a computer based system is beneficial in finding the right balance between what should be computerised and what should not, such as an operating system designed by a group of people who will be forced to use the operating system they are designing or security mechanism that is to influence the work of the security people themselves, or parking regulations that will apply to the person who is in change of parking regulations. Professor Needham agreed that this is true but that in the security context, the people devising computer security policies are not disjoint from the locksmiths. He added that it is very difficult to get people who have the locksmith's privileges to behave in a totally responsible manner.

Concerning the issue of expressing rules in a way such that people would take them seriously, Dr Maxion suggested that it is difficult to influence the way people intuitively

want to behave. By way of example, he referred to the common practice whereby airline regulations require, in the event of a depressurisation, a passenger to put on their own oxygen mask before helping anyone else with their's and pointed out that a mother travelling with a small child will most likely see that her child is wearing a mask before putting on her own. He suggested that it is only necessary to add a few words to the safety drill to explain that the mother, for instance, would die before the child could be helped. He concluded that in general examining such procedures to see how people are likely in practice to respond would be beneficial. Professor Needham agreed that insufficient care is often taken, referring to a pathological tendency for secrecy leading to security officers issuing rules without explaining the rationale behind them. He concluded that if secrecy of the mechanisms is important to the security of the whole then a new security team is needed, and that a fundamental principle is that while secrets should be private, mechanisms should be public.

Professor Nehmer suggested that some of these problems are unavoidable. Referring to the case of telephone network providers he suggested that by changing from mechanical switching systems to computer based exchanges which became more and more intelligent and handled all the accounting information introduced a large internal security problem, without realising it. He continued, saying that at that time there was not the understanding to handle such a problem and that now the telecommunications companies face more attacks from within their own organisations than from outside. Professor Needham agreed saying that there is a tendency on finding a security problem to think insufficiently about the problem and erect inadequate defences, leading to a sort of arms race. He referred to cash machines as an example of this and suggested that the ATM fraud industry would never have got off the ground if a bit more thought had been put in at the beginning, rather than by patching the systems in response to each separate type of attack. He said that the same was true of pay television apparatus and that, as in the case of the telephone companies the providers didn't anticipate the magnitude of the problem before putting the systems in place.

Mr McKeag suggested that as a general rule when designing a computer system it is a good principle to write programs to simulate the people who will be using that system. Such programs he suggested need not be extremely detailed, but would help to address the point Dr Rushby made about the need to have a mental model. He also suggested that during the formalisation of such a model in a program might often become extremely complex, which would suggest that the original system should be revised. He concluded that programming the people is an excellent way of setting out the system design and can influence both the requirements and the training manuals. Professor Needham agreed.

Dr Anderson referred back to a suggestion in the talk that within an organisation it might be appropriate instead of barring unpermitted access, to flag such violations in messages to the security officer, on the grounds that it is likely that the person has just acquired the relevant access rights and the appropriate system update been delayed. He referred to experience in banks where it has happened that established employees have after a long period of honest working turned to fraud through having got into major debt problems. Professor Needham acknowledged this problem and added that the principle he had

described was not suited for universal application since in some cases even a single incorrect access should be prevented so global access is quite inappropriate, pointing to information on individual's salaries and bonuses as one example. He suggested however that there is much information which is not universally available, but for which no very great harm is done by single access, and probably less harm than is done by the administrative unreliability of getting people the proper privileges.

Dr Neumann agreed with Dr Rushby that the agenda for security research presented by Professor Needham might apply to any large design problem, except that the danger that rules are intended to protect against is mostly invisible, and that if people follow the rules laid out the enemy will probably be even more invisible. He wondered if it would be useful for the enemy to be a bit more visible in terms of our understanding, as is the car thief. Professor Needham replied that the food hygiene regulations might be regarded as having an invisible enemy, and that the speaker might be seen as coming close to suggesting that everyone who prepares food should have suffered food poisoning.