CHAPTER

24

Conclusions

We are in the middle of a change in how security is done.

Ten years ago, the security manager of a large company was usually a retired soldier or policeman, for whom 'computer security' was a relatively unimportant speciality which he left to the computer department, with occasional help from outside specialists. In ten years' time, his job will be occupied by a systems person; she will consider locks and guards to be a relatively unimportant speciality which she'll farm out to a facilities management company, with an occasional review by outside specialists.

Ten years ago, security technology consisted of an archipelago of mutually suspicious islands—the cryptologists, the operating system protection people, the burglar alarm industry, right through to the chemists who did funny banknote inks. We all thought that the world ended at our shore. In ten years' time, security engineering will be an established discipline; the islands are being joined up by bridges, and practitioners will need to be familiar with all of them. The banknote ink man who doesn't understand digital watermarks, and the cryptologist who's only interested in communications confidentiality mechanisms, will be poor value as employees.

Ten years ago, information security was said to be about 'confidentiality, integrity and availability'. In ten years' time, this list of priorities will be the other way round (as it already is in many applications). Security engineering will be about ensuring that systems are predictably dependable in the face of all sorts of malice, and particularly in the face of service denial attacks. They will also have to be resilient in the face or error and mischance. So tolerance of human carelessness and incompetence will be at least as important as tolerating dishonesty, and this will mean paying close attention to economic and institutional issues as well as technical ones. The ways in which real systems will provide this dependability will be much more diverse than today: tuning the security policy to the application will be an essential part of the engineering art.

Ten years ago, the better information security products were the domain of government. They were designed in secret and manufactured in small quantities by cosseted cost-plus defense contractors. Already, commercial uses dwarf government ones, and in ten years' time the rough and tumble of the marketplace will have taken over completely.

Ten years ago, government policy toward information security was devoted to maintaining the effectiveness of huge communications intelligence networks built up during the Cold War. It was run in secret and along the same lines as the nuclear or missile technology non-proliferation policy: only enough could be exported to prevent the development of competent manufacturers in other countries, and control had to be maintained at all times by vetting end-users and enforcing export licensing. Already, it is becoming clear that crypto controls are almost irrelevant to real policy needs. Issues such as data protection, consumer protection and even online voting are more important. In ten years' time, information protection issues will be pervasive throughout government operations from tax collection through market regulation, and many decisions taken hastily now, at the behest of empire-building police agencies, will have to be changed at some expense.

The biggest challenge though is likely to be systems integration and assurance. Ten years ago, the inhabitants of the different islands in the security archipelago all had huge confidence in their products. The cryptologists believed that certain ciphers couldn't be broken; the smartcard vendors claimed that probing out crypto keys held in their chips was absolutely physically impossible; and the security printing people said that holograms couldn't be forged without a physics PhD and $20 million worth of equipment. At the system level, too, there was much misplaced confidence. The banks claimed that their automatic teller machines could not even conceivably make a mistaken debit; the multilevel secure operating systems crowd sold their approach as the solution for all system protection problems; and people assumed that a security evaluation done by a laboratory licensed by a developed country's government would be both honest and competent. These comfortable old certainties have all evaporated.

Many things will make the job more complicated. The distinction between outsiders and insiders used to be central to the business, but as everything gets connected, it's disappearing fast. Protection used to be predicated on a few big ideas and on propositions that could be stated precisely, while now the subject is much more diverse and includes a lot of inexact and heuristic knowledge. The system life-cycle is also changing: in the old days, a closed system was developed in a finite project, while now systems evolve and accumulate features without limit. Changes in the nature of work are significant: while previously a bank's chief internal auditor would remember all the frauds of the previous thirty years and prevent the data processing department repeating the errors that had caused them, the new corporate culture of transient employment and "perpetual revolution" (as Mao Tse-Tung described it) has all but destroyed corporate memory. Finally, there are the economics of networked information systems: strong externalities dictate that time-to-market will remain much more important than quality.

The net effect of all these changes is that the protection of information in computer systems is no longer a scientific discipline, but an engineering one.

The security engineer of the twenty-first century will be responsible for systems that evolve constantly and face a changing spectrum of threats. She will have a large and constantly growing toolbox. A significant part of her job will be keeping up to date technically: understanding the latest attacks, learning how to use new tools, and keeping up on the legal and policy fronts. Like any engineer, she'll need a solid intellectual foundation; she will have to understand the core disciplines such as cryptology, access control, information flow, networking and signal detection. She'll also need to understand the basics of management: how accounts work, the principles of finance and the business processes of her client. But most important of all will be the ability to manage technology and play an effective part in the process of evolving a system to meet changing business needs. The ability to communicate with business people, rather than just with other engineers, will be vital; and experience will matter hugely.

I don't think anybody with this combination of skills is likely to be unemployed—or bored—anytime soon.