CHAPTER

27

Conclusions

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

Ten years ago, the security manager of a large company was usually a retired soldier or policemen, for whom 'computer security' was an unimportant speciality 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 that she'll farm out to a facilities management company, with an occasional review by outside specialists.

Ten years ago, security technology was 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 the world ended at our shore. Security engineering is now on the way to becoming an established discipline; the islands are already being joined up by bridges, and practitioners now realise they have 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, are poor value as employees. In ten years' time, everyone will need to have a systems perspective and design components that can be integrated into a larger whole.

Ten years ago, information security was said to be about 'confidentiality, integrity and availability'. These priorities are already reversed in many applications. Security engineering is about ensuring that systems are predictably dependable in the face of all sorts of malice, from bombers to botnets. And as attacks shift from the hard technology to the people who operate it, systems must also be resilient to error, mischance and even coercion. So a realistic understanding of human stakeholders — both staff and customers — is critical; human, institutional and economic factors are already as important as techincal ones. The ways in which real systems provide dependability will become ever more diverse, and tuning the security policy to the application

will be as essential as avoiding technical exploits. In ten years' time, protection goals will not just be closer to the application, they will be more subtle: examples include privacy, safety, and accountability. Conflicts between goals will be more common; where one principal wants accountability and another wants deniability, it's hard to please them both.

Ten years ago, the better information security products were designed for governments in secret and manufactured in small quantities by cosseted cost-plus defence contractors. Already, commercial uses dwarf government ones, and the rough and tumble of the marketplace has taken over. In ten years' time it'll be interesting to see whether civil government uses any technologies different from standard commercial ones, and even the military will make increasing use of off-the-shelf hardware and software.

Ten years ago, government policy towards information security was devoted to maintaining the effectiveness of huge communications intelligence networks built up over the Cold War. Crypto controls turned out to be almost irrelevant to real policy needs and were largely abandoned in 2000. Surveillance is still an important policy issue, but privacy, DRM, consumer protection and even electronic voting are acquiring comparable importance.

The biggest technical challenge 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 m 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. Instead, security has become part of the larger dependability problem. We build better and better tools, and these help the system builders to get a little bit further up the complexity mountain, but in the end they fall off. A proportion of large complex system projects fail, just like in the 1970s; but we build much bigger disasters nowadays.

Complexity is the real enemy of security. The distinction between outsiders and insiders used to simplify the business, but as everything gets connected up 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 caused them, the new corporate culture of transient employment and 'perpetual revolution' (as Mao described it) has trashed corporate memory. Economics will continue to ensure that insecure systems get built — and the liability will be dumped on others whenever possible. Governments will try to keep up, but they're too slow and they can often be bought off for a while. So there will be many regulatory failures too.

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.

Finally, the rampant growth of the security-industrial complex since 9/11, and the blatant fearmongering of many governments, are a scar on the world and on our profession. We have a duty to help it heal, and we can do that in many different ways. My own path has been largely research — developing the disciplines of security engineering and security economics, so that we can tell not just what works in the lab but what can be made to work in the world. The dissemination of knowledge is important, too — that's what this book is about. Economic growth also helps, and education: it's the poor and the uneducated who are most swayed by fearmongering (whether from Western leaders, or from bin Laden). At least in countries with educated populations, the voters have started to recognise the excesses of the 'War on Terror' and to deal with them. Just as individuals learn through experience to compensate for our psychological biases and deal more rationally with risk, so our societies learn and adapt too. Democracy is the key mechanism for that. So the final way in which security engineers can contribute is by taking part in the policy debate. The more we can engage the people who lead the discussions on emerging threats, the faster our societies will adapt to deal with them.