Protecting Embedded Systems – The Next Ten Years

Ross Anderson

Computer Laboratory,
Pembroke Street, Cambridge, England
Ross.Anderson@cl.cam.ac.uk

Abstract. In this talk, I will speculate about the likely near-term and medium-term scientific developments in the protection of embedded systems.

A common view of the Internet divides its history into three waves, the first being centered around mainframes and terminals, and the second (from about 1992 until now) on PCs, browsers, and a GUI. The third wave, starting now, will see the connection of all sorts of devices that are currently in proprietary networks, standalone, or even non-computerized. By the end of 2003, there might well be more mobile phones connected to the Internet than computers. Within a few years we will see many of the world's fridges, heart monitors, bus ticket dispensers, burglar alarms, and electricity meters talking IP. By 2010, 'ubiquitous computing' will be part of our lives.

Some of the likely effects of ubiquitous computing are already apparent. For example, applications with intermittent connectivity will have to maintain much of their security state locally rather than globally. This will create new markets for processors with appropriate levels of tamper-resistance. But what will this mean?

I will discuss protection requirements at four levels.

Invasive attacks on hardware are likely to remain possible for capable motivated opponents, at least for devices that cannot be furnished with effective tamper responding barriers. That said, even commodity smartcards are much harder to probe than was the case five years ago. Decreasing feature sizes, 32-bit processors, and layout that makes bus lines harder to find and to probe, all combine to push up the entry cost. Attacks that could be done in a few weeks with ten thousand dollars' worth of equipment now take months and require access to equipment costing several hundred thousand dollars. However, this field rides on the coat-tails of the semiconductor test industry, and will remain unpredictable. Every so often, bright ideas lead to powerful new low-cost testing tools, that may be used in attacks. The scanning capacitance microscope may be one such.

Non-invasive attacks on hardware – such as power and glitch attacks – might become infeasible against even the smallest processors. However, this is not as easy as it seemed three or four years ago. Current techniques, such as randomised clocking, can only do so much. New ideas are needed, and I will discuss an EU-funded

Ç.K. Koç, D. Naccache, and C. Paar (Eds.): CHES 2001, LNCS 2162, pp. 1–2, 2001.

research project (G3Card) to develop these. Its goal is produce a prototype smartcard CPU that is inherently resistant to noninvasive attacks. The prototypes currently being designed at Cambridge under G3Card use asynchronous (self-timed) dual-rail logic, which holds out the prospect of power consumption that is independent of the data being processed. This technology holds out the prospect of important side benefits as well, such as reduced RFI/EMI and lower power consumption.

Protocol-level attacks continue to be a terrible problem. The design of ordinary authentication protocols is well known to be hard; yet a typical cryptographic processor performs much more than one protocol. Its API may have to support somewhere between a few dozen and a few hundred different cryptographic transactions. The paper in these proceedings by Mike Bond shows that attacks can be found on even the most mature and thoroughly-studied cryptographic APIs. Developing the tools and concepts to design robust cryptographic APIs looks set to be a major research challenge for some years to come, and may be the next big topic for the protocol research community.

Business process failures are coming to be recognised as perhaps the main cause of attacks on real systems. Once the principal providing the protection is no longer the same as the principal who will suffer loss if it fails, things become messy. While a traditional monolithic pay-TV operator might have owned the smartcard designer, the satellite transponder, the set-top boxes and indeed the entire customer base, things are now becoming much more fragmented. Design, evaluation, implementation and operations are being ever more widely distributed, and this is starting to introduce serious evaluation and assurance issues. There are also economic issues such as network externalities, asymmetric information, moral hazard, adverse selection, liability dumping and the tragedy of the commons.

The above themes interact in unexpected ways. For example, even a completely tamper-proof chip can have its design read out by a litigation attack; the attacker buys a vaguely relevant patent, brings a lawsuit against the device designer for infringement, and obtains full design details as part of the legal discovery process. This may be a further argument in favour of Kerckhoffs' principle. On the other hand, a highly obscure design can greatly complicate matters for an attacker whose tools allow him to observe only partial information about the computations being undertaken.

Ultimately, though, information security is about power. While at the technical level it is about controlling who may use which resource and how, while at the level of business strategy it is increasingly about raising barriers to trade, segmenting markets and differentiating products. A final point is that sometimes insecurity is welcome. For example, it may foster economic growth by making monopolies harder to defend.