We Need Assurance

Brian D. Snow

National Security Agency, USA

Abstract. Today's commercial cryptographic products have sufficient functionality, plenty of performance, but not enough assurance. Further, in the near term future, I see little chance of improvement in assurance, hence little improvement in true security offered by industry. The malicious environment in which security systems must function absolutely requires the use of strong assurance techniques. Most attacks today result from failures of assurance, not function.

Am I depressed? Yes, I am. The scene I see is products and services sufficiently robust to counter many (but not all) of the "hacker" attacks we hear so much about today, but not adequate against the more serious but real attacks mounted by economic adversaries and nation states. We will be in a truly dangerous stance: we will think we are secure (and act accordingly) when in fact we are not secure.

Assurance techniques (barely) adequate for a benign environment simply will not hold up in a malicious environment.

Despite the real need for additional research in assurance technology, we fail to fully use that which we already have in hand! We need to better use those assurance techniques we have, and continue research and development efforts to improve them and find others.

Recall that assurance are confidence-building activities demonstrating that system functions meet a desired set of properties and only those properties, that the functions are implemented correctly, and that the assurances hold up through manufacturing, delivery, and life-cycle of the system.

Assurance is provided through structured design processes, documentation, and testing, with greater assurance coming through more extensive processes, documentation, and testing. All this leads to increased cost and delayed time-to-market – a severe one-two punch in today's marketplace.

I will briefly discuss assurance features appropriate in each of the following five areas: operating systems, software modules, hardware features, third party testing, and legal constraints.

Each of us should leave today with a stronger commitment to quality research in assurance techniques with strong emphasis on transferring the technology to industry. It is not adequate to have the technique; it must be used. We have our work cut out for us; let's go do it.

Ç.K. Koç and C. Paar (Eds.): CHES'99, LNCS 1717, p. 1, 1999.