

13.0 High Assurance Systems

13.1 There Are (as yet) No Rules of Engagement In Cyberspace

A great deal of attention has been given to the notion of information warfare, with considerable use of terminology and metaphors from more traditional forms of conflict. But there are also a number of ways in which conflict in cyberspace is importantly different. As one example, we will at times not know whether we are under attack, because information attacks can be considerably more subtle than physical attacks. Information attacks can occur from arbitrary physical distances and involve no movement of personnel or materiel.

Even more important, there is not yet any established notion of *rules of engagement*; simply put, there is no agreed on notion of what constitutes a hostile act in cyberspace. Some possibilities are of course relatively obvious, e.g., breaking into password-protected systems. In some cases state law has begun grappling with this via legislation concerning "computer trespass." But even here there is some ambiguity in distinguishing a break-in attempt from an innocent mistake. There is also the difficulty of issues of jurisdiction: given the arbitrary distance involved, acts that may be illegal in the US can be undertaken from other countries. While this phenomenon is not new, this does underscore the need for agreement that is as widespread as possible, ideally global in scale.

As with rules of engagement in other forms of warfare, the crucial properties of rules for cyberspace would be: (a) they are widely agreed on and (b) they are technologically feasible. As such the task of creating such rules is a mixture of policy and technology requiring participation from both communities.

Near-term steps:

The Air Force should assemble a high-level policy and technology task force to formulate draft rules of engagement.

13.2 Cryptographic Coding Will Be Unbreakable; Systems May Be Breakable

Cryptographic techniques currently exist in COTS that can provide very high levels of security to individual systems. *Public-key systems* in particular offer an encoding technique that has withstood considerable testing and appears to be unbreakable. By "unbreakable" we mean keys can easily be provided which ensure any attempt to decrypt an encoded transmission would require arbitrarily great effort. One can, for example, use keys which ensure breaking the code would require tens of thousands of years of computation on machines tens of thousands of times faster than anything available. If that is insufficient, a few more digits can be added to the key to make the effort required hundreds of thousands of years, and so forth.

Over the next 5 years integration of this technology into Air Force software at all levels (networks, operating systems, and applications) will provide security against any attempt to extract information by decrypting intercepted signals.

Important attention should now be paid to Air Force policy regarding cryptology. In particular: 1. as a COTS technology, the major stumbling block to deployment and integration

will be policy rather than technical. Appropriate authorities must permit the use of these systems. 2. we recommend strongly the Air Force employ a key escrow (or similar) system, in order to ensure that internal use of cryptographic techniques cannot provide an impenetrable wall of privacy to unauthorized action by Air Force personnel.¹

Formulating appropriate policy and effecting deployment of cryptographic technology are important near-term steps because existing information intensive systems are currently blatantly vulnerable. Recent studies have shown the domestic electric power grid, major financial systems, and the telecommunications infrastructure to have between modest and virtually non-existent protection against information-based attacks. Break-ins have occurred via techniques as primitive as knowing the phone number of a modem at a site. Military systems have routinely displayed only slightly better protection.

There is no reason for this to be so; basic techniques exist to defeat many of these attacks, systems simply need to be designed to take advantage of what we already know how to do. Continued vigilance and development of counter-measures will of course also be necessary, as new modes of information-based attack will no doubt be created.

Information systems will continue to be vulnerable. Code-breaking is only one of the routes to the cleartext of an encoded transmission. Unbreakable codes offer no new protection against traditional techniques such as traffic analysis or compromising personnel. In fact, we anticipate that with the widespread use of unbreakable codes, attack effort will shift markedly, away from decryption and toward other approaches. This likely reallocation of effort should be considered when developing security policies.

13.3 In the Long Term, Low Probability Events May Impact Encryption

Current techniques have been well tested, but their ultimate status as unbreakable is contingent on certain mathematical hypotheses that have themselves been widely examined, but are not yet proven. One such hypothesis is that factoring large numbers is an inherently time-consuming process; very low probability discoveries may yet prove this untrue. A more general hypothesis in computer science goes by the name of $P \neq NP$; if this turns out to be false, a new basis for unbreakable codes will have to be found. Note these are extremely unlikely events, and even if they were to occur, their initial significance would be strictly theoretical.

Two other lines of development should also be monitored. New models of computation have recently been proposed and explored in a very limited way. One approach—molecular computation—involves the use of sequences of DNA as a way of searching very quickly through a vast number of possibilities. It relies on the ability to create on the order of 10^{17} copies of a molecule in a solution, and the ability of one DNA molecule to bind to another that has a specific sequence of sub-units. It thus provides in effect 10^{17} extraordinarily simple computers that search

1. Key escrow systems involve keeping a copy of cryptographic keys with one or more trusted authorities. Procedures are established by which the escrow agent can divulge a key to appropriate personnel only after the required degree of need and authority have been established. Keys can also be split into two or more fragments, no one of which is sufficient to break the code. The fragments can then be parcelled out to a like number of authorities; in that case no one authority acting alone can break the code.

in parallel for an answer. A second approach—quantum computing—is even more speculative, involving the use of quantum mechanical effects to do computation. While both of these are low probability long-term developments, it will be useful for Air Force personnel to monitor their potential developments over the long term.

Near-term steps:

The Air Force should develop and deploy a key escrow system that is a routine and transparent part of any use of unbreakable advanced codes.

The Air Force should integrate off-the-shelf cryptology into software at all levels (networks, operating systems, and applications).

13.4 Biometric Identification Will Be an Embedded Technology

Biometric identification—identifications via physiological traits such as face recognition, finger-, retina-, or voice-print, are all currently effective laboratory demonstrations. We believe in the next five years they will routinely be embedded in devices and will provide useful levels of security by fusing results from multiple sources: voice, retina, thumb, and face recognition in combination can provide useful levels of performance, including acceptable levels of false negatives, and are difficult to counterfeit simultaneously.

We believe within ten to fifteen years biometric identification will be unobtrusive, continuous and ubiquitous. We predict a world in which “smart locks” can be embedded everywhere control is required. Those locks will be made unobtrusive (i.e., check identity without disturbing the user) and continuous (constantly verify user identity), thereby providing a high level of security at all times.

13.5 Survivability and Assurance Is Significantly More Difficult in Large-Scale Distributed Systems

Difficult problems arise in providing high assurance and survivability for larger-scale distributed systems. A significant body of foundational work exists in fault tolerance for modest scales of distribution, but significant work needs to be done to provide assurance and survivability when potentially every computer in the Air Force will be interconnected. Of particular note will be development of techniques for *graceful degradation*—the ability of a system to provide dynamically selected partial functionality in the face of unanticipated failures, rather than the all-or-nothing functionality provided by today’s approaches to fault tolerance.

One interesting example of survivability is the Internet itself: over the past twenty years it has proven to be a remarkably robust means of communication despite a complete lack of centralized control. Interesting design lessons emerge from considering how and why this is so, lessons that may be of use in future systems. The net achieves its robustness by massive dispersal of functionality—tens of thousands of computers handle the message routing function. As a consequence, it may be difficult to cripple the net: it is too big and too widely dispersed. But that same broad distribution for routing also provides greater access to users of good and bad intent and any broad homogeneity may also be a vulnerability.

One possible reason the Internet itself, as opposed to its attached hosts, has remained relatively unthreatened and intact is that it is often the only means for a network terrorist to access a target host or server. To attack the Internet's routers or gateways would be to remove the conduit through which damage is perpetrated or information sought is recovered. Should one simply want to deny others use of the Internet, then it might not appear so invulnerable. Attacks on routing tables, as an example, could perhaps deny selective segments of a network, leaving other segments in use. This type of vulnerability must be dealt with for any network that becomes part of the AF infrastructure.

The research challenge for the future is to develop design techniques that permit us to provide more complex behavior in a similarly dispersed (and hence survivable) manner.

Near-term steps:

Support work in and through AF Labs to develop the ability to design systems with the ability to degrade gracefully in the face of unanticipated failures.