Providing Security With Insecure Systems

Andrew Odlyzko
School of Mathematics, University of Minnesota
127 Vincent Hall, 206 Church St. SE
Minneapolis, MN 55455, USA
odlyzko@umn.edu
http://www.dtc.umn.edu/∼odlyzko

Categories and Subject Descriptors

C.2 [**Computer Systems Organization**]: Computer-Communication Networks; D.4 [**Software**]: Operating Systems; J.4 [**Computer Applications**]: Social and Behavioral Sciences
General Terms: Security, Economics, Human Factors

Extended Abstract

A Martian who arrived on Earth today would surely conclude that computing and communications security are in a crisis situation. The popular media as well as technical publications are full of stories of new vulnerabilities being discovered and systems being compromised. Government and business leaders call for a fundamental rethinking of how information and communication technologies (ICT) systems are designed and operated.

But that Martian would surely have come to the same conclusion 10 years, and 20 years, and 30 years ago. The alarms and complaints have been practically the same all this time, only their volume and stridency have grown. Further, for the last few decades security professionals have been getting more and more frustrated. They have been complaining that they were not being listened to, and that their expertise was not being used properly. They have also been repeating constantly the mantra that once some ICT insecurity leads to a big disaster (such as bankruptcy of a major bank), society will finally take notice and rethink its approach to the issue.

Sherlock Holmes noted that the "curious incident" in the *Silver Blaze* story was that the dog did not bark. In ICT insecurity, there are two curious incidents that so far seem not to have attracted much notice:

- Why have none of the giant cybersecurity disasters that have been threatened for so long taken place?
- Why is the world in general doing as well as it is?

There simply have not been any big cybersecurity disasters, in spite of all the dire warnings. As this is being written in early 2010, the world is grappling with the effects of the great financial crash of 2008. Yet that crash, and the bubble that led to it, were not caused by cyber–*in*–security. Even taking the crash into account, the world economy has been doing very well over the last decade or more, and much of the credit for this has been assigned to ICT, even though it has been and continues to be terribly insecure.

Further consideration of these issues leads to some heretical thoughts, which suggest that cybersecurity is not as critical an issue as is often thought, and that one should adopt a different philosophy to the design of ICT systems. If there is anything that the last half a century has taught us, it is that human beings are incapable of building secure systems. Furthermore, if we could build them, we could not live with them. People insist on a degree of flexibility in their work and private lives that is not consistent with formal systems. So, if we can't do what everybody says we should do (namely re-architect all our systems so they are secure), let's adopt a Dr. Strangelove approach, and

Learn to love the bomb.

In other words, accept that our systems will be insecure, and figure out how to live and prosper anyway.

Security is not the paramount goal by itself.

Some degree of security is needed, but it is just a tool for achieving other economic and social goals. Our ordinary physical lives are full of insecurities. Aside from terrorism, wars, and the like, we have ordinary accidents (with automobile deaths in the U.S. taking more lives each month than the 9/11 attack did), as well as hurricanes, earthquakes, and so on. Yet human society has coped. Further, there are studies which show that people willingly take on some risks, and even compensate for increased security by engaging in riskier behavior. Thus society is used to dealing with a certain level of insecurity, and it is only necessary to ensure that this level is not exceeded.

To move away from the idea of absolute cybersecurity is a major step, but it appears an essential one. Once it is taken, it is much easier to explain what has happened in the past, in particular how to answer the two bullet-point questions. It is also possible to see how to move forward without butting our heads into the wall. (The wall in this case being the combination of inability to design completely secure systems, and the human refusal to accommodate to secure systems.)

It is very hard for technologists to give up the idea of absolute cybersecurity. Their mind set is naturally attracted to the binary secure/insecure classification. They are also used to the idea of security being fragile, with the general mantra being that "a chain is only as strong as its weakest link." They also tend to think of ICT systems as isolated. This attitude is represented beautifully by the famous 1996

WiSec'10, March 22–24, 2010, Hoboken, New Jersey, USA.
ACM 978-1-60558-923-7/10/03.

creation of John Perry Barlow, "A Declaration of the Independence of Cyberspace." This proclamation, which today seems outlandishly ludicrous, proclaimed the existence of a new realm, Cyberspace, that was divorced from the physical world, and did not need or want traditional governments or other institutions. The key assumption was:

> Cyberspace consists of transactions, relationships, and thought itself, arrayed like a standing wave in the web of our communications. Ours is a world that is both everywhere and nowhere, but it is not where bodies live.

Indeed, if cyberspace were totally divorced from human space, and if all the "transactions, relationships, and thought itself" depended just on some mathematical relationships, then an opponent factoring a public-key RSA modulus, or stealing a password, could wreak unlimited havoc.

What makes our lives tolerable is that the Barlow vision is divorced from reality. Cyberspace is intimately tied to what I will call Humanspace, the convoluted world of physical objects and multiple relations, including institutions such as governments, and laws, and lawyers. In fact, we can say:

> *The dream of people like Barlow was to build a Cyberspace that would overcome the perceived defects of Humanspace. In practice we have used the defensive mechanisms of Humanspace to compensate for the defects of Cyberspace.*

Even though the famous mantra was that "on the Internet, nobody knows you are a dog," in practice there is less privacy there than in Humanspace, and many people know not only that you are a dog, but also that you are a mutt and what kind of fleas you have. Subverting a "standing wave" does not gain an attacker too much when there is little immediate gain to be obtained, and leaves traces of the action that is taken. That is what enables tools such as digital forensics to be used. Even when criminals use cryptography to protect the security of their messages, traffic analysis (part of the web of relationships in Humanspace everybody is in) is a productive tool for investigation. We can go on and show many other ways in which the ordinary approaches of Humanspace also work in Cyberspace.

Additional assistance towards providing tolerable levels of security comes from the mistakes that actors who try to subvert ICT systems make. They are human, and very fallible. Even if the main movers are very clever, and manage to avoid mistakes, for large scale exploitation of their attacks they usually need to involve more people (for example, to launder the money they receive), and with growing organizations, chances of stupidity and mistakes grow. Note that this is exactly how Humanspace is kept at tolerably levels of order and security.

The main distinction between Cyberspace and Humanspace is that the former enables actions that are less expensive, much more widespread, and much faster. That is why Cyberspace is so useful to Humanspace, promoting a variety of social and economic functions, and leading to economic growth. It is also why Cyberspace is so dangerous, since malicious agents find these features facilitate a variety of undesirable attacks.

How can the dangers of Cyberspace be mitigated? Well, how have the dangers to Humanspace from other technologies (the telegraph, the telephone, the airplane, etc.) that lowered costs and increased the speed and reach of physical actions been contained? By slowing things down. And that is largely how society has managed to cope with ICT insecurity, and prosper. Consider voting. Electronic voting is convenient, and loved by voters for its convenience. But all deployed systems have been shown to be suspect. So we are now moving towards reliance on electronic voting with a physical record, which allows for ex-post audits. Physical ballots are not secure, there is a long history of vote tampering, but their insecurity can be controlled. Thus by tying the Cyberspace scheme of electronic voting to the traditional Humanspace system of physical ballots, we can provide tolerable security for the hybrid system. This can be thought of as a prototype for approaches to solving other ICT insecurity problems. Another key element to providing adequate, but imperfect, security, comes from consideration of fax signatures. While technologists were obsessing about secure digital signatures back in the 1980s, insecure fax signatures were proliferating, and continue to be used. Why do they work? Because a single forged fax signature can seldom do serious harm. It is usually part of a web of transactions, involving personal meetings, phone calls, emails, bank money transfers, and the like. The art of using fax signatures securely is to embed them in a web of highly intertwined relations, so that an opponent cannot subvert it by gaining control of a single "standing wave in the web of our communications." Thus exploitation of context is another key tactic for dealing with insecurity.

So what is the lesson to be drawn? None of the ideas mentioned here for providing ICT security are truly novel. They come from systematic observations of how society has coped so far with ICT security. The suggestion, therefore, is not for a radical departure in what is done in practice, but in the design philosophy of ICT systems. Instead of trying for the unattainable, let us accept that perfect security cannot be provided, and learn from what has worked in the past.

This train of thought leads to some interesting, if contrarian, ideas. Instead of the systems engineering commandment to "build clean," we should "build dirty." That way opponents will not be able to easily subvert our systems, or even be able to explore them fully. Build in many logging mechanisms, with write-only capabilities, so it is harder for attackers to avoid detection. Provide many verification mechanisms, to check for context of transactions, and detect illegitimate ones. Build systems in meshes, so many interactions among heterogeneous elements provide more opportunities for checking. Use code obfuscation, so that the source code might be indeed clean and maintainable, but the deployed systems would present to attackers puzzles that are hard to solve. Change the obfuscation method periodically. And don't underestimate the value of "security through obscurity." Attackers have limited resources, and not everything on the Internet moves at the speed of photons through fiber. We have a plethora of examples of weaknesses that had been known in principle for ages, but were not exploited. These are all suggestions contrary to the basic design philosophies applied so far, but they have contributed to the success of ICT so far.

The general conclusion is that we should not despair. The natural evolution of ICT already points us in the direction towards achieving acceptable levels of security, and provides the tools we need. We should just change our system design philosophy.