Chapter 21

OPERATING SYSTEMS THAT POSE SECURITY RISKS

INTRODUCTION

The threats to international security posed by operating systems (OSs) are significant, and must be addressed quickly. This chapter discusses here in turn the problem in principle, OSs and its actions in relation to those principles, and the social and economic implications for risk management and policy [1].

THE PROBLEM IN PRINCIPLE

Computing is essential to industrialized societies. As time passes, all societal functions become more deeply dependent on it: power infrastructure, food distribution, air traffic control, emergency services, banking, telecommunications, and virtually every other large scale endeavor is today coordinated and controlled by networked computers. Attacking national infrastructures is also done with computers – often hijacked computers. Thus, threats to computing infrastructures are explicitly and inherently risk harm to those very societies in proportion to those society's dependence on them. A prior history of catastrophe is not required to make such a finding. You should not have to wait until people die to address risks of the scale and scope discussed here. So, with the preceding in mind, this part of the chapter focuses on the following:

- Your society's infrastructure can no longer function without computers and networks.
- The sum of the world's networked computers is a rapidly increasing force multiplier.
- A monoculture of networked computers is a convenient and susceptible reservoir of platforms from which to launch attacks; these attacks can and do cascade.
- This susceptibility cannot be mitigated without addressing the issue of that monoculture.
- Risk diversification is a primary defense against aggregated risk when that risk cannot otherwise be addressed; monocultures create aggregated risk like nothing else.
- The growth in risk is chiefly amongst unsophisticated users and is accelerating.

- Uncorrected market failures can create and perpetuate societal threat; the existence of societal threat may indicate the need for corrective intervention [1].

Regardless of where or how it is used, computing increases the capabilities and the power of those who use it. Using strategic or military terminology that means what it sounds like, computing is a force multiplier to those who use them – it magnifies their power, for good or ill. The best estimates of the number of network connected computers show an increase of 50% per year on a worldwide basis. By most general measures what you can buy for the same amount of money doubles every eighteen months ("Moore's Law"). With a conservative estimate of a four year lifetime for a computer (in other words, consumers replace computers every four years on average) the total computing power on the Internet therefore increases by a factor of 2.7 per annum (or doubles every 10 months). If a constant fraction of computers are under threat of misuse, then the force available to misusers will thus double every 10 months [1]. In other words, the power available to misusers (computer hackers, in popular parlance) is rising both because what they can buy grows in power per dollar spent and because the total number of networked computers grows, too [1].

> **Note:** This analysis does not even include attacks enabled by storage capacity, which doubles in price-performance twice as fast as CPU (doubles every nine months rather than eighteen).

Internetworked computing power makes communication feasible. Communication is of such high value that it has been the focus of much study and much conjecture and not just recently. For one-way broadcast communication, the value of the network itself rises proportionally to N, the potential number of listeners ("Sarnoff's Law"). By way of example, advertisers pay for television time in rough proportion to the number of people viewing a given program [1].

For two-way interactive communications (such as between fax machines or personal email) the value of the network rises proportionally to N2, the square of the potential number of users ("Metcalfe's Law"). Thus, if the number of people on email doubles in a given year, the number of possible communications rises by a factor of four [1].

Growth in communications rises even more when people can organize in groups, so that any random group of people can communicate with another. Web pages, electronic mailing lists and online newsgroups are good examples of such communications. In these cases, the value of the network rises proportionally to 2N, the potential number of groups being an exponential growth in N ("Reed's Law") [1].

Assume for now that the Internet is somewhere between the Metcalfe model, where communications vary according to the square of the number of participants (N^2), and the Reed model, where communications vary according to two raised to the Nth power (2^N) [1].

If you make this assumption, then the potential value of communications that the Internet enables will rise somewhere between $1.52 = 2.3$ and $21.5 = 2.8$ times per annum. These laws are likely not precisely accurate. Nonetheless, their wide acceptance and historic record show that they are good indicators of the importance of communication technology [1].

To extend this simple mathematical model one final step, you have to assume so far that all communications are good, and assigned to the value of the network a positive number. Nonetheless, it is obvious that not all communications (over computer networks, at least)