

Extreme Events Involving Computer Systems and Networks  
Mikhail Atallah  
CERIAS and Computer Science Department  
Purdue University  
West Lafayette, IN 47906  
mja@cerias.purdue.edu

As society increasingly relies on computing and networks for commerce, government, social services, entertainment, and communication, it also becomes more vulnerable to accidents, disasters, criminal behavior, and malicious activity involving this crucial infrastructure. However, the current infrastructure was simply not designed for the kind of usage it is being put to today. An event that involves and/or affects the computing/communications infrastructure in an extreme way is uncomfortably likely. The recent outbreaks of denial-of-service attacks and computer viruses are, unfortunately, the tip of a very large iceberg that is still largely out of the public view: What could easily occur is orders of magnitude worse than what has occurred. Many events that routinely occur today could easily take on an "extreme" character in the future, but two prime candidates are financial fraud and accidental losses:

- Financial fraud using computers and networks is already occurring on a frightening scale and is still largely under-reported by the victim institutions (because of incentives to under-report). The scale of a future fraud can easily be large enough (e.g., bankrupting a large multinational corporation) to have devastating repercussions on confidence and financial markets.
- Even without malice, purely accidental events can cause huge disruptions. The scale of each individual occurrence has so far been (relatively) modest, but the frequency of their occurrence is so large that one of them is bound to eventually have severe consequences (one accident was initially of magnitude \$30 billion but was quickly reversed, and the final loss was less than \$10 million). Planes, rockets, missiles, and (most importantly) hundreds of lives were lost to computer errors.

What makes the occurrence of such events so frequent? In a nutshell:

- (i) the state-of-the-art in security and reliability is not reflected in what is most widely deployed, and
- (ii) the state-of-the-art itself needs considerable advancement through a vigorous research agenda.

The reason for (i) is part historical and part "incentives." The "historical" part may be corrected in due time as systems evolve, but the "incentives" part requires policy and legislative initiatives. Accountability is needed, including a wise placement of liability on the entities most capable of taking steps to decrease risk; in this manner society maximizes the likelihood of correcting problem (i). For example, in consumer products, liability tends to be placed on the manufacturer (unless there is blatant consumer misuse of

the product) and this has led to large improvements in the safety of consumer products. British researchers have observed that, in countries that place the liability for ATM fraud largely on the consumer (rather than on the bank), ATM fraud is much more prevalent than in the U.S. (where liability is largely placed on the entity that is most capable of doing something about decreasing the risk—the bank).

Part (ii)—advancing the state-of-the-art—is also of crucial importance: Even if the practice of the art reflects the best knowledge we currently have, that would still be inadequate because we need much more research, not only in such technical areas as secure operating systems, networks, protocols, cryptography, firewalls, intrusion detection system, etc., but also in related fields like those represented at this workshop, and in others as well. Criminologists, psychologists, economists, ethicists, etc. have as much to contribute as technologists.

In most computer incidents involving loss of life or money, it was usually not the cryptography that failed but rather the protocols that made use of it, the software that implemented it, the humans that used those systems, etc. And yet a huge potential for a catastrophic failure comes from the fact that modern cryptography is based on largely unproven assumptions about the computational difficulty of some problems (that is, it is crucial that some problems be computationally intractable in order for a cryptographic system to work). Even though most research (this one included) are confident of the validity of the assumption of intractability of such computationally problems, one cannot rule out a breakthrough through which a new algorithm is discovered that efficiently solves one such problem (like factoring a large integer, that is the product of two large primes, into its two constituent primes—this would wreak havoc on electronic commerce, whose security is based on the presumed difficulty of this factoring problem). Even if such a breakthrough is made by "the good people" who subsequently act in a responsible manner, it would be quite disruptive (on the other hand, a breakthrough by organized crime would qualify as an economic mega-event of hugely negative impact).

The greatest challenge we face is how to decrease the likelihood (and mitigate the impact of) extreme events without damaging those very same things that drive the expanding use of our computers and networks: communications, connectivity, open access, use of common protocols, etc. The challenges are to find cost-effective and dependable means of protecting the infrastructure without substantially decreasing its usability and its tremendous potential for economic progress. The issues for society as a whole are not quite the same as for smaller entities like corporations or universities, but there are many commonalities: The need for formulating an effective information security policy and implementing it (including the associated training and education), identifying the critical assets and evaluating how vulnerable they are, developing or acquiring the proper tools and procedures (both managerial and technical) for the protection of these assets, and having in place the extreme-event response capability well before the event occurs ("thinking the unthinkable" and having detailed plans for dealing with the various scenarios that can unfold).