日本財団 The Nippon Foundation 助成

IIPS

Institute for
International Policy Studies
・Tokyo・

IIPS International Conference

“The IT Revolution and Security Challenges”

Tokyo

December 10-11, 2002

“IT Revolution: Security Challenges”
by

Dieter Gollmann
Microsoft Research

IT Revolution: Security Challenges

Dieter Gollmann[*]
Microsoft Research
7 J J Thomson Avenue, Cambridge CB3 0FB, United Kingdom,
E-mail: diego@microsoft.com

Discussion paper

When talking about the IT revolution, we tend to refer to the changes brought about by the great success of the Internet in the last decade. For people working in IT, email is now the standard medium of communications. In my professional lifetime editing conference proceedings has become a much easier task since authors submit their papers electronically, making the final editorial work a fairly painless exercise. Travel planning – at least for journeys in familiar territories – has become more straightforward as flights and hotels can be booked directly on the Internet. The more reliant we become on these services, the more concerned we become about potential disruptions. In addition, we must also consider the possibility that others will use this technology for purposes that impair our own interests.

To understand the security challenges posed by this IT revolution we will try to identify its defining characteristics. In our analysis, we should not forget that there are lessons to be drawn from the IT revolution of the 19th century: Telephony and telegraphy.

You can communicate with people all over the world

It is often claimed that the Internet revolutionized the way we communicate because it gives us the chance to get in contact with people we never met before. A brief moment of reflection should remind us that we could do so well before the days of the Internet. The telephone system already provided a global communications infrastructure, and actually carries a fair share of Internet traffic. Even earlier, postal services carried letters all around the world, potentially to people one had never met before.

Thus, if there are tangible effects of the IT revolution, they have to reach beyond the mere ability to communicate. On the Internet we can certainly communicate much faster and much cheaper than in the past, but I do not see any immediate security challenges arising from this observation.

We also can get easy access to a wide range of information resources. This leads to a first security challenge. More precisely, a familiar security challenge has to be met in a new environment. At many levels of society we find controls on data access. In a family, parents may have a moral (or legal) duty to know what their children are doing. In a company, management may have a right or duty to control how employees are using the company's IT system. In a country, there may be laws prohibiting or regulating the distribution of certain kinds of material (like pornography). To a large extent this challenge can be addressed at the societal level by defining 'rules of engagement' for using the Internet[1]. In theory, we may also try to regulate the distribution channel, but the current nature of the Internet is such that our best chance to effect control is at the boundaries to the end systems (home

[*] The views expressed in this paper are entirely the author's and are in no way indicative of Microsoft's position on these matters.

[1] For example, http://www.wiseuptothenet.co.uk/ contains advice to parents on Internet use by children

PC, intranet), both at the point where traffic enters an end system and at the point where traffic leaves an end system. We will return to this issue below.

There is a corollary to the ‘ability to communicate with everyone’. Everyone can communicate with you. Spam is today a major grievance of email users and has to be included among the IT security challenges. Again, this is not a totally new problem. Unsolicited mass mailings have been deemed enough of as nuisance for some countries to regulate this business. In this case there is also an up-front cost to the sender, whilst with email the cost to the sender may be less than the costs for the receiver. Technical anti-spam measures are today investigated by companies like Yahoo, regulatory anti-spam measures are being drafted, for example, in Europe[2].

The mode of communications has changed

So far, we have encountered old challenges in new disguises. To understand the security challenges specific to the Internet we must have a closer look at the technology itself. In the telephone system a call establishes a connection. Signals sent over this connection are transient and are normally not stored. Over time, most countries have passed laws that establish who is allowed to intercept communications and under which circumstances. In consequence, callers can expect a reasonable degree of privacy but no absolute privacy. Similar rules regulate the postal system.

Internet protocols running over TCP/IP work quite differently. Data is copied from one machine to another until it arrives at its final destination. There are no connections and data transmitted within a session may travel along different routes.

This raises a number of security challenges. First, consider the legal interception of traffic. As there are no connections, communications on the Internet are not that easy to intercept at a point ‘within’ the network. In the UK, for example, there is an ongoing discussion between the Home Office and Internet Service Providers (ISPs) about the technical ramifications of using the ISPs as the points of interception. The challenge here is for legislation to catch up with the realities of the Internet. As a corollary, targeted unauthorized interception of traffic is not that easy either. Quite probably, the major challenges for user privacy do not arise at the point of data transmission. Anecdotal evidence suggests that criminals are more likely to obtain credit card numbers from a merchant site that is badly protected than by scanning Internet traffic.

On the other hand, wholesale monitoring of communications has become a concern, and not only for citizens[3]. The concern is not new and countries have to decide on their priorities when setting protection goals for the communications systems.

The mode of transmission on the Internet does not match familiar intuitions associated with sending mail through the postal system or making a telephone call. Data that are part of a conversation may still be stored at various places after the end of a session. Equally, copies of an email may still exist at the sender’s site and with various intermediaries. When the receiver deletes a message, the message quite probably still exists somewhere else, a feature some companies recently discovered to their disadvantage. Here, the security challenge concerns the users who have to learn that IT services are not one-to-one substitutes of ‘old technology’ services they are familiar with.

[2] Directive2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

[3] Speech by Ms. Birte Weiss, Minister for Research and Information Technology, Denmark, at the Hearing on Encryption, Monday 17th of January 2000: “In December there was a debate about surveillance and Echelon in the Danish Parliament and the unanimous conclusion was quite simple: all nations are listening to everyone. They have been doing this from time immemorial by one means or another and very probably they will continue to do so in the future. It is up to ourselves to protect our communications against illegal monitoring – and the way to do this is by using encryption.”

The end system have changed

On the Internet a typical end system is a computer, a device meant to be programmable and adaptable to new types of use. In my view, this is the most crucial aspect of the IT revolution with the most far ranging impact on the security challenges.

When your end system is a computer callers can potentially manipulate your system. They could not do so by letter, nor with a call to a simple telephone receiver. There is thus a challenge in software engineering to make end systems more resistant to attacks. Secure software has become the focus of research interest only recently. Two books on this topic were published in 2001[4]. There is a security management challenge – and potentially a commercial opportunity – to keep the security of end systems up to date.

There is a challenge in network design to catch attacks before they reach vulnerable end systems or before they spread widely. Intrusion Detection has been receiving considerable attention in the last few years. It is also a challenge to find the most effective points of control. Today it is usual to filter traffic coming into a local system. We may also filter outgoing traffic (legislation in Italy has created a potential liability for system owners for damages their users cause to third parties) and consider security probes within the Internet.

With respect to privacy, the end systems 'at the other end' automatically record data during a conversation and will keep it by default unless their owners take deliberate steps to delete it. Cookies stored in a user's machine can reveal information during a later conversation. Once information has been collected, it is beyond the user's technical means to control how it is further processed. It is to some extent up to users to decide how much they are prepared to disclose about themselves. It is up to legislators to set the rules for data collection and processing, and for the authorities to enforce those rules.

As stated above, badly protected servers storing customer data are a prime source for illegal collection of personal data (aka identity theft). This is a further reason to include privacy enhancing technology (PET) among the security challenges. The most effective way of protecting personal information is not to collect it in the first place. For historic reasons, so called user identities play an important role in access control, to the extent that it is often assumed that access control requires user identities. This is blatantly wrong and today's challenge in access control is the search for policies and access control models that work with attributes other than user identities.

Cryptography has so far only appeared briefly in the list of challenges. Traditionally, cryptographic mechanisms protect traffic between secure end systems that have to use an insecure communications medium. On the Internet, however, our first task is to secure the end systems. It is therefore no surprise that we cannot expect too much help from cryptography.

Interface between the legislation and technology

We have mentioned areas where legislation can meet IT security challenges. Electronic signature legislation was not among them. Many countries have passed laws on digital signatures and electronic signatures expecting that e-commerce would flourish once cryptographically generated evidence had a well established basis in law. There is little evidence that this has happened[5], and there is evidence that well intentioned legislation can become an impediment when it imposes too high a burden on prospective users of cryptographic technology[6].

[4] John Viega, Gary McGraw: *Building Secure Software*, Addison Wesley, 2001; Michael Howard, David LeBlanc: *Writing Secure Code*, Microsoft Press, 2001

[5] SwissKey [http://www.swisskey.ch/]: In the international environment as well, the indications are that the demand for branch-independent, universally applicable certificates will not reach a level quickly enough to cover the costs of issuing and administering IDs for the digital world."

[6] Ahmad Abu El-Asa, Martin Aeberhard, Frank J. Furrer, Ian Gardiner-Smith, David Kohn: *Our PKI-Experience*, SYSLOGIC Press, Birmensdorf, Switzerland, 2002

Moreover, a much more fundamental legal problem has to be resolved. If there is a dispute about an e-commerce transaction, which court has jurisdiction, if any? (The Internet community prides itself in having abolished national boundaries, but these boundaries are relevant for the legal process. Even more, legal proceedings in one country can have extraterritorial effects, as in the case of law suits in France persuading US sites to stop auctioning Nazi memorabilia.) Even if there were a court with jurisdiction, a party may find that the court is in a foreign country and decide that recourse to the legal system is simply too expensive. To mitigate commercial and legal risks, a party may thus involve intermediaries like banks or credit card companies in their transactions. Intermediary and party are subject to the same jurisdiction. Electronic transactions may again use cryptography but can now be regulated by contract. Disputes are adjudicated based on local law, even without digital signature legislation. Intermediaries of this nature are already well established and can provide the foundations for global e-commerce. Legislation for e-commerce would probably be more effective if its focus were more on regulating business processes than on regulating the use of cryptography.

The challenge for the legal and technical communities is to understand the other side. In the cryptographic literature one frequently finds comments that digital signatures are unforgeable evidence, superior to a handwritten signature because they are tied to the document signed. However, by signing a contract a party indicates its intent and it is not clear that a digital signature generated by a device is an indication of the signer's intent [7].

As another example, current European privacy legislation states that the user's consent has to be sought when personal data is written to a record. This rule is also applied to cookies so the user should be asked for consent when the cookie is written on his machine (no information disclosed yet) although information is being disclosed only when the cookie is read by a remote server[8]. In this case, legislation drafted for centralized database systems of the 1970s is (mis)applied to IT systems that are designed quite differently.

The particular challenge for the legal profession is thus to define the principles but remain 'technology neutral'. If legislation gets too close to the technology of the day it can become an impediment for the future. It is of course not always easy to see when the technology of the day is only a clumsy implementation of a more general principle. As a precaution, we may try to use as little as possible concepts from current IT systems when formulating laws related to IT.

Summary

Already before the latest IT revolution we had gained experience in dealing with the opportunities and dangers that come with the deployment of communications systems and with international commerce. In these domains, we are unlikely to face fundamentally new security challenges.

The major technical security challenges posed by the IT revolution derive from the fact that we connect general purpose computers managed by users who are rarely technical experts (and even more rarely security experts) to the Internet where they can be attacked by everyone:

- Make end systems more secure, but do not expect that perfect security can ever be achieved.

- Educate users so that they can manage their systems (or have their systems managed) and understand that perfect security can ever be achieved.

[7] Jane K. Winn: *The Emperor's New Clothes: The Shocking Truth About Digital Signatures and Internet Commerce*, Revised Draft, faculty.smu.edu/jwinn/shocking-truth.htm, 2001

[8] Giles Hogben, Tom Jackson, Marc Wilikens: *A Fully Compliant Research Implementation of the P3P Standard for Privacy Protection: Experiences and Recommendations*, Proceedings ESORICS 2002, Springer LNCS 2502

- Find ways of policing the Internet (‘police’ as in ‘traffic police’), i.e. stopping spam and attacks efficiently.

Finally, there is the challenge to draft legislation that regulates the use of technology in such a way that it does not unintentionally force new technology to simulate older systems.