

Creating trust in critical network infrastructures

Danger can come from almost anywhere...

Network predators, disgruntled employees, corporate spies, electronic criminals, cyberterrorists, hostile nations... Threats to the world's communication networks come in many guises. Yet, as information communications increasingly become the underpinning of our global economy and society, we are ever more dependent upon these very networks. The security of our global networks is a pressing issue that merits constant attention — ensuring our collective cyber-security needs to be a top policy priority.

By all accounts, the threats to our networks are growing, and the financial impact alone is alarmingly high.

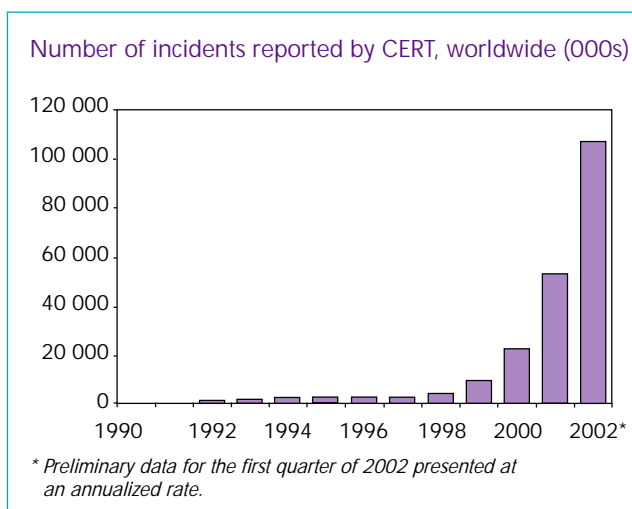
Almost every country that collects statistics on security incidents has reported the growing scale of the problem. Data compiled by the Computer Emergency Response Teams Co-ordination Centre (CERT/CC) based at Carnegie Mellon University in the United States shows, for example, that more security incidents (52 658) were reported in 2001 alone than for the entire period since 1988, when records began. And the trend seems to be continuing: preliminary statistics for the first quarter of 2002 show that the rate of growth is still accelerating (see Figure 1, left chart). Japanese Government statistics show that the number of virus incidents almost doubled, and

Chain reaction

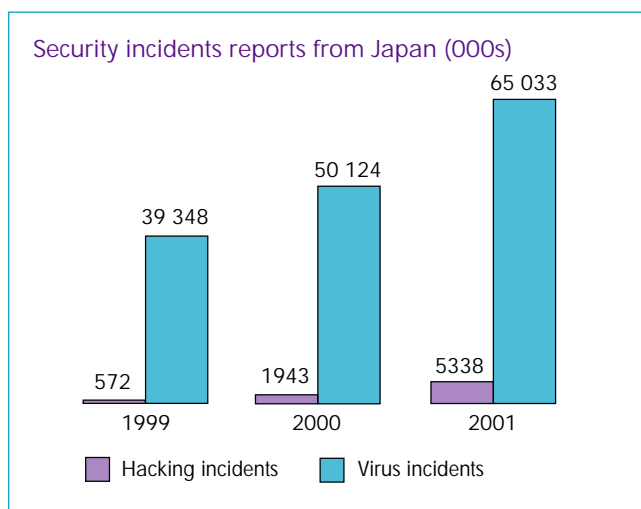
The potential extent of damage is illustrated by a recent incident in which a handful of optical cables located in a European country's harbour were cut. This not only disabled the Internet, but it also resulted in the partial loss of that country's mobile and fixed telephone services, emergency numbers, fax and data traffic, as well as financial and PIN (personal identification number) code services. With so many major services at risk, it is easy to understand why everyone should feel concerned.

Figure 1- A growing menace

Computer security incident reports worldwide (1990–2002), and in Japan (1999–2001)



Source: Computer Emergency Response Teams Co-ordination Centre (CERT/CC).



Source: Ministry of Public Management, Home Affairs, Posts and Telecommunications (MPHPT), Japan.

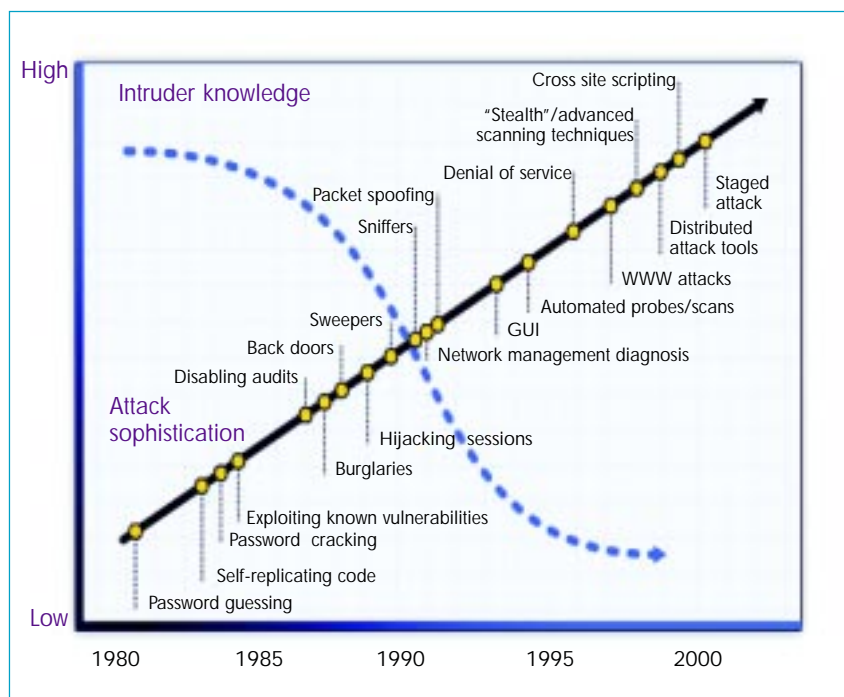
hacking incidents increased ten-fold, between 1999 and 2001 (see Figure 1, right chart). The cost of cyber-security breaches is currently estimated at hundreds of billions of dollars annually.

elite networks, the Internet, and the many private networks used for critical services such as banking and health care. Measures should also include a full assessment of physical infrastructure, both hardware

of current levels of collaboration. Moreover, activity at the national level is insufficient and patchy in almost all countries. It was concluded that critical infrastructure protection is urgently needed at three levels: international, national, and sub-national.

Figure 2 – Sophisticated attacks: child’s play for “script kiddies”

Network growth has resulted in more public users and a wider distribution of attack software tools, making it easier for intruders to break into systems. The scale and sophistication of intrusions are often strikingly disproportionate to the level of knowledge required for the attack; which is why today’s typical network intruders are sometimes dubbed as “script kiddies”.



Source: Counterpane Internet Security, Inc.

More networks, greater vulnerability

After over 100 years of development, even the global telephone network is not entirely secure. But the telephone network security still compares well with that of the Internet, which has even greater shortcomings. With today’s rapid convergence of voice and data networks, security issues need to be addressed in a context which covers the global telephone network, wireless and sat-

and software, as these form an integral part of any effective solution.

An ITU Strategic Planning Workshop entitled “Creating Trust in Critical Network Infrastructures” was held in Seoul (Republic of Korea) from 20 to 22 May 2002*. A recurring theme in the workshop presentations and discussions was the need for international collaboration for the protection of critical network infrastructures. The workshop served to highlight the inadequacy

of current levels of collaboration. As well as identifying the status, needs and priorities of network security, the workshop also discussed the form that international collaboration might take. As an example, in his paper to the workshop, Professor Goodman sets out a fivefold framework for international collaboration involving:

- **International standards.** International cooperation in developing standards is increasingly important, even in competitive markets. But equally important is cooperation in the creation and implementation of standards. For instance, the IEEE 802.11 Wireless LAN security standard (WEP) is successfully implemented on fewer than 15 per cent of Wireless LANs in operation, and it is relatively easy to break.

- **Information sharing.** There is an understandable unwillingness to share information about cyberattacks, if only for fear of exposing failings and undermining public confidence. There may be a role for a clearinghouse function — a role that an international organization could play, as a trusted repository of up-to-date information. Such a clearinghouse could provide anonymity to the victims as well as coordinating information gathering and dissemination.

* All of the workshop documents, including country case studies, papers, presentations and the Chairman’s Report, are available on the ITU website at www.itu.int/osg/spu/ni/security/docs/cni.

- **Halting cyberattacks in progress.** One of the most useful steps would be to develop a standard methodology for the sharing of information across borders, especially during cyberattacks, when time is of the essence. Stephen Bryen, in his paper, proposed the creation of a “cyber-warning centre”, which could set common data reporting standards and could serve as an alert service. This could be combined with the clearing-house function mentioned above.

promote safety and security in civil aviation. Similar assistance is necessary to counter cybercrime.

National and international responsibilities in the face of a global problem

Nowadays, networks are typically operated and managed by the private sector. Nevertheless, responsibility for our personal security, social well-being and protection of life clearly lies with national

national networks do not recognize national boundaries, making this a global problem requiring global action. Uncoordinated measures taken by individual industry sectors or governments in isolation are likely to fail. Governments, regulators, industry, hardware manufacturers, software developers and users will all need to work together to assure our collective cybersecurity. In this regard, the Chairman’s Report of the workshop suggested a number of possible action areas for ITU. This



ITU 020100/EyeWire

With today’s rapid convergence of voice and data networks, security issues need to be addressed in a context which covers the global telephone network, wireless and satellite networks, the Internet, and the many private networks used for critical services such as banking and health care

- **Coordinating legal systems.** If defence against criminal or terrorist activities is to be active, rather than passive, then there needs to be some coordination of legal systems so that hackers cannot find safe havens.

- **Providing assistance to developing nations.** This will require collaboration between ITU Member States at different levels of economic and technological development. For example, the International Civil Aviation Organization (ICAO) has played a similar role in providing technical assistance to

governments. Where appropriate, governments, in consultation with the relevant industry sectors, need to begin a process of risk assessment of the vulnerabilities and risks to national networks, with a view to producing a follow-up action plan. In addition, existing mechanisms, activities, and institutions already at work on aspects of critical infrastructure protection need to be identified with a view to future coordination and collaboration without duplication of efforts.

That said, national efforts will clearly not be enough: today’s inter-

included a suggestion that ITU quickly review its current work programme *vis-à-vis* information systems security and network infrastructure protection, and that it take action to reinforce its activities accordingly. It was considered that ITU, as an organization with across-the-board representation from governments and the private sector, and with responsibility for coordinating global telecommunication networks and services, including IP-based networks, provided a potential valuable international forum for cooperation in this area. ■

ITU case study on Internet diffusion in Ethiopia

The Federal Democratic Republic of Ethiopia is one of the oldest countries in Africa. In 2001, the country had some 343 000 fixed lines in service, and teledensity reached 0.54 per cent. The following is a summary based on the field research and case study (see www.itu.int/osg/spu/casestudies) carried out by ITU and the Commonwealth Telecommunications Organisation in March 2002.

ETC — still a monopoly

In the wake of market reforms to develop a more efficient and reliable telecommunication service, the Government of Ethiopia created the Ethiopian Telecommunications Agency as an independent national regulatory authority in 1996. Yet, all telecommunication services (fixed, mobile and Internet) are still under the monopoly of the incumbent operator, the Ethiopian Telecommunications Corporation (ETC).

The Government's plans are still on course to partially privatize ETC to allow the participation of a strategic investor. This should bring new funding and new management techniques and skills to ETC.

Poor infrastructure, limited services and unsatisfied demand

With a national switching capacity of 550 000 lines, of which only 61 per cent are in use, the growing demand for telecommunication services is not being met: the fixed-line waiting list stood at 153 000 in February 2002, or an average waiting time of around eight years.

Mobile services are not faring well either, despite growing demand — the waiting list is over 40 000 and there are no plans to allow another operator onto the market in the near future. Ethiopia has some 28 000 mobile subscribers. New subscriptions were suspended in 2001, two years

after the launch of the service, when the maximum capacity of the system was attained. Only basic voice telecommunications are provided (with no international roaming), and are relatively affordable. A mobile-to-mobile call costs ETB 0.75 (around



ITU 020099/Claudia Sarrocco

Public telephone booths in Addis Ababa

Until the fixed and mobile networks are expanded to meet needs, for many Ethiopians telephone access is limited to public payphones

one third of a US cent) a minute. But this is failing to generate revenue to expand the network.

Internet policy

Ethiopia had full Internet access in 1997, when ETC started providing Internet services using a 256 kbit/s international satellite link. Today, a 2-Mbit/s symmetric international link is provided by France Telecom. The number of Internet subscribers reached 6000 in 2001, for a total of 30 000 estimated Internet users, the large majority of

whom are located in the capital city, Addis Ababa. The average cost of Internet dial-up services is heavily influenced by the high subscription fees charged by ETC. A basic private subscription with 8 hours of access costs USD 19, and USD 4 for each extra hour. Telephone charges however, are not particularly burdensome, with the standard local tariff applied throughout the country.

Conclusion

Aside from Ethiopia's low level of economic development, Internet diffusion has been constrained by ETC's monopoly and the lack of a clear policy on value-added services such as Web design, site hosting or cybercafés. The institution of a regulatory authority and the plan to partially privatize ETC are important steps towards an open market.

However, care should be taken to avoid a simple shift from a public monopoly to a private one, which can become even more difficult to control — especially if backed by a large foreign partner.

The licensing of new mobile operators, Internet service providers, cybercafés and call centres would provide impetus for the provision of much-needed value-added services. This would go some way towards demonstrating the market benefits of liberalization, and the improvements this will bring for users. ■