Arbetsrapport

R2003:012

Internet security issues

Sabine Ehlers

itps INSTITUTET FÖR TILLVÄXTPOLITISKA STUDIER

Internet security issues

Sabine Ehlers
ITPS kontor i Tokyo

itps INSTITUTET FÖR TILLVÄXTPOLITISKA STUDIER

ITPS, Institutet för tillväxtpolitiska studier
Studentplan 3, 831 40 Östersund
Telefon 063 16 66 00
Telefax 063 16 66 01
E-post info@itps.se
www.itps.se
ISSN 1652-0483
Elanders Gotab, Stockholm 2003

För ytterligare information kontakta Sabine Ehlers
Telefon +81 3 5562 5041
E-post sabine.ehlers@itps.se

Förord

För att tillmötesgå en önskan om att även få tillgång till pågående arbeten och icke publicerade underlagsrapporter har vi tagit fram Arbetsrapportserien.

I arbetsrapportserien publicerar vi avrapporteringar, pågående arbeten, ej färdigställda rapporter eller annat underlagsmaterial. Flertalet av dessa arbetsrapporter kommer att publiceras i sin helhet eller som delar i rapporter som ingår i ITPS huvudserie ”A-serien”. Annat kommer att ingå som allmänt underlag i ITPS analys- och utvärderingsarbete.

Eventuella slutsatser och rekommendationer som lämnas i arbetsrapporten står författaren för och är inte nödvändigtvis desamma som ITPS officiella ståndpunkt. Arbetsrapporterna har korta ledtider och huvudsyftet är att snabbt få ut materialet till särskilt intresserade. Vi har därför delvis andra kvalitetskrav på dessa rapporter jämfört med övriga ITPS-rapporter. Vi ber er ha förståelse för detta.

Lena Moritz

Enhetschef

Innehåll

1 Introduction

"Internet" and "security" are two words that were not meant to go together. The World Wide Web started out as a Virtual Wild West; virgin territory where pioneers roamed unrestricted by the laws, rules, borders, and limits that would restrain them in the real world, untouchable by governmental controls, unreachable by commercial interests.

As corporations started connecting themselves for business purposes however, giving their employees access to information and communication over the Internet, they also opened themselves up for access from the outside and needed tools to monitor and control who was accessing what.

As big and small criminals started using the Net for their activities, law enforcement got interested in ways to control and trace contents.

And individuals, who until then had been only mildly concerned with Internet security, definitely started having issues with privacy and authentification as the net became a convenient market place for products and services.

Barriers are now being built across the Internet prairie, not only around specific computers and nets, but also around countries. Geolocation technologies, which attempt to trace a user's geographical location based on the computer's Internet address, in theory enable the internet service provider to bar access to contents and services from users in specific areas depending on local laws. Independent studies have pegged the accuracy rate for this type of software to between 70 and 90 percent.

Gambling sites where among the first to use the geolocation technology last year. When users in areas which do not allow online gambling try to log on, they are barred from making the bet. The technology is also being used by Internet radio stations to prevent access from countries where the programs broadcasted are copyright protected.

Of course there are many less reputable companies who do not care about following laws that cannot be imposed on them until an international treaty or mediation organisation is created. And the technology can also quite easily be evaded by the user through software that cloaks his or her location.

A more general objection to the idea of making the service providers internationally responsible for the contents they are offering is however that this would infringe on the basic idea of the internet as a global platform for free speech and expression. A practical objection is that it would be impossible for any service provider to keep updated on every applicable law in all nations around the world.

Still, many nations are trying to control what reaches its citizens over the net. According to Leonard Sussman, author of "Censor.gov", at least 59 nations today limit the freedom of expression. Singapore works with service providers to block any material that undermines public security, national defence, racial and religious harmony and morals. Hong Kong's government has been debating whether to pass a law that would make it a crime for any overseas gambling site to offer services to

its citizens. A court in Genoa, Italy, recently found the operator of an Internet site in another country guilty of libel. An American judge closed down a Canadian web company re-broadcasting TV programs by forbidding it to broadcast to users in the US. A French judge has ordered Yahoo Inc to stop selling Nazi paraphernalia to French citizens because a French law prohibits it. The French judge ordered Yahoo to use geolocation technology to ensure that users in France would not be able to access pages where Nazi-related material was being sold. An American court in turn ruled the order un-enforceable because a foreign judge cannot impose conditions going against the First Amendment on a US-based company. The French groups have appealed, claiming that the case is not about free speech but about national sovereignty.

Corporations on their side are also slowly beginning to realise that internet security is not a pure technical problem to be left in the hands of the IT department. “Too many practitioners still engage in theological debates about six versus eight digit passwords,” says Bill Bonti, Motorola’s Chief Internet Security Officer in an interview in Financial Times. As the assets of companies are increasingly becoming digital, possible to transport to any corner of the globe in lightning speed with a few taps on the keyboard, the problem of Internet security is not an issue of technology but one of asset protection management. Less time should maybe be spent on implementing technical solutions, and more on taking a comprehensive look at what data needs to be protected, and to what degree.

Until now, many people working with data security have claimed that the biggest financial losses at corporations come not from damage done by outside hackers, but from internal security breaches made by all from well-meaning IT-illiterates to unhappy employees trying to hurt the company. The 20-80 belief, claiming that only 20 percent of security damage is caused by outside access, is widespread.

However, Mr Richard Power, senior analyst at the Computer Security Institute of San Francisco (CSI), claims in his book “Tangled Web” that this is a dangerous myth, no longer holding any truth. He claims that while the insider threat has not gone away, the outside threat has grown so much that companies now have two things they should worry about.

CSI annually surveys hundreds of companies and governmental agencies, and in their survey for 2001 they found that 95% of those polled had employed firewalls, 90% had access control and 61% has intrusion detection systems. In spite of these impressive numbers, 64% had experienced financial losses due to security breaches, and the third of the respondents that were willing to quantify their damages (equalling 186 companies), claimed financial losses from computer crimes totalling 377.8 million USD, up from an annual total of 120 million USD the previous 3 years. The absolute biggest cause was theft of proprietary information, followed by financial fraud.

A new threat is materialising as mobile devices are increasingly being used by employees for information access and storage, and communication. Any networked device used for work constitutes both a source of stored internal information, as well as a possible key in to the internal network. Mobile phones are more easily

lost than laptops, which in turn are more vulnerable than desktops. The problem can be worsened by employees buying their own devices, thereby bypassing security controls put in place by the IT management.

In addition, mobile devices communicating over infrared or Bluetooth are opening themselves up to data theft by other, nearby mobile devices, which are happy to pick up the call. Even a physical package sent to the office could act as a Trojan horse. If it contains a Bluetooth enabled mobile device, a person outside the building could use it to hack into the internal network while the package sits around waiting for delivery. Or your Bluetooth enabled mouse could be exchanged for one that sends characters causing buffer overrun, which in turn exposes your PC to hackers. The potential for security breaches increases directly with convenience and accessibility.

For the private individuals, Internet security became an issue the moment their money started travelling the net. In surveys everywhere, security comes up as the number one issue why consumers are weary about e-commerce. Can I trust the merchant? Is my money safe? Is my privacy protected? This summer Swedish newspapers have carried stories of people who bought cheap plane tickets on the net, and ended up loosing both their money and their trip when the agent could not deliver or even be located. Less frequent, but still occurring, are stories of credit card fraud based on information conveyed over the Internet. For e-commerce to take off, winning the trust of the consumers is vital.

But the consumers are also targeted in other ways. Spam mails and viruses are rampant and the use of countermeasures is increasing, but there is other software, invited in by the unaware user, which may be just as disturbing.

"**Spyware**" is attached to free programs downloaded from the Internet, and often help pay for their development. It collects information about the user's browsing habits and secretly sends it back to the advertisers who can either use it themselves or sell it to others.

"**Web bugs**" are nearly invisible graphic references embedded in a web pages or an e-mail to let a third party know where on a web page you have been, or whether you read a particular message. When your computer requests the graphics from the sender to display it to you, the marketer gets to know your IP address and the page you are on. A technique called "**scumware**" by its critics establishes false links to lure you away from the page you were looking at, to an unrelated ad-page paid for by the scumware sponsor. One company under the name of TopText, for example, highlights specific words on a page, which were not highlighted by the page's designer. When you click them you are whisked to advertisements paid for by TopText's customers. The words are chosen specifically to raise your interest, and both information about your IP address and the word you clicked on will be collected.

To sum up, Internet security is today not only big business for those that work to uphold it, as well as to those that strive to circumvent it; it is also a top concern for corporations and individuals alike, for national and international bodies across the globe. This report does not aim to cover, or even touch upon, all the aspects of this vast area, but will discuss relevant issues that are currently being debated in Japan.

2 Spam[1] and scam goes mobile

2.1 Introduction

A substantial portion of all e-mails are spam; unsolicited and intrusive commercial ads usually pushing sex, get rich quick-schemes, financial services or health related articles of dubious provenance. Most are sent from spoofed or fake e-mail addresses. Hotmail says their customers receive 1 billion pieces of unsolicited mails per day, about 80% of the messages received; not counting the spam that never makes it past Hotmail's own filters. AT&T WorldNet says that 20-25 of every 100 messages their customers receive are spam, not counting an additional 200-300 mails that are sent to non-existing addresses. eMarketer puts the total number of spam mails sent annually to 76 billion messages, and many analysts call that a conservative figure. The bandwidth cost for this is estimated to 8-10 billion USD per year, according to PC World. Other damages include server crashes, time spent going through unwanted e-mails, and pure aggravation.

Inevitably, the spam industry, estimated to 4.8 billion USD for 2003 by Forrester research, has given rise to an as vital anti-spam industry. List blockers, report and complaints generators, advocacy groups, registers of known spammers and spam filters all proliferate. But for every anti-spam measure, there seems to be an anti-anti measure popping up soon after. There is software that hides the mail's origin, software that automatically alters the contents to evade filters, software that makes the contents look like gibberish to a computer while completely readable to a human or hides it in an image.

Spam is unlikely to go away anytime soon. It works, for one thing. To an average cost per posting of about one cent, spam is said to elicit a hit rate of 0.1-1 percent, to be compared with 1-3 percent for direct mail at an average cost of 75 cents. Software robots continually score web pages, chat rooms and postings for e-mail addresses. One site sells 1 million addresses for 59.95 USD, another offers a CD with 15 million addresses for 120 USD. All major credit cards accepted. Meanwhile Internet service providers rely on the data traffic that spam generates for their revenues.

2.2 Mobile spam

No wonder then that this phenomenon has found its way also to the mobile devices. According to Mobile Channel in Britain, SMS advertising attracts a 10 to 20 percent response rate. But in Japan, the only country yet where mobile spam has really taken a hold, it has become an omnipresent nuisance, abhorred by all users. There are two main, mobile-specific, reasons for this. Firstly, expensive and slow connections make it particularly annoying to have to wait for the download of a mail that turns out to be unsolicited advertising. Secondly, the price structure for mobile services in Japan is based on number of packets up- and downloaded, so the user actu-

[1] *Spam is said to be named after the famous Monty Python skit about the canned meat product by the same name. See http://spamcanners.org/montypython.htm.*

ally has to pay to receive spam. And with some users receiving tens of spam mails per day, the cost is not negligible. The mails contain links to web sites with sexual contents, advertise pornographic videos or get-rich-quick schemes, or offer to set up the user with an attractive date. Especially disliked are the mails that threaten to charge the recipient for the mail unless it is forwarded to several other people, and the ones that cause the cell phone to temporarily freeze.

The operators of course have reasons to embrace the spam for its revenue generating ability, but the sheer traffic volume it generates is actually causing especially DoCoMo big technical problems and costs. Between 900 million to 1 billion messages are sent over DoCoMo's popular i-mode service on an average day, but only about 100 million of them actually reach an addressee, indicating that most of the traffic is generated by advertisement servers sending spam mails to randomly generated addresses.

The first event of network problems due to spam came last summer, June 8th 2001, when a single company sent 900 000 messages within an hour, of which 170 000 went undelivered. Another 300 000 messages were sent the following hour. The company sending the mails had already previously been warned against sending such large volumes, but ignored it. By law, the operator is obliged to maintain the confidentiality of the communications, and is prohibited from reading the contents of any mail, which makes it difficult for them to argue that a certain customer's mail is polluting the network with spam and should be refused service. In this case however, DoCoMo could point to actual system failures caused by the mass volume of mail, and based on this a court issued an injunction against the firm sending the mails.

2.3 Countermeasures

This was the first legal action against mobile spamming in Japan, but it turned out to not deter the offenders. By September DoCoMo was still receiving over 70 000 customer complaints each month (down from 143 000 in June) regarding unsolicited mails. To dampen the user frustration over the costly spam, DoCoMo started offering each user 400 free packets per months. As a spam countermeasure, DoCoMo enabled and recommended users to change the e-mail addresses of their mobile phones from the automatically generated, phone number-based address assigned at purchase, to an address containing both letters and numbers. Other measures made available to the users included limiting incoming e-mail to user-specified addresses, blocking user-specified addresses and requiring senders to include a user-supplied password. DoCoMo also asked handset suppliers to develop new models allowing the users to see the subject of a message without downloading it, and promised they should be available within 6 months.

Within a few months 90% of the users had changed their addresses, but spammers kept their address lists updated with existing addresses by noting which addresses targeted by their random mass mailings generated bounced mails, and which were active. November 6th DoCoMo applied to the Ministry of Telecommunications to be allowed to block e-mails sent to large numbers of invalid addresses, thereby also

blocking the spammers' ability to learn which addresses are active. The measure was approved after only 3 days.

By now the government was hard at work with measures to curb the nuisance of spam. Late February the ruling coalition drafted a bill that requires the companies who send commercial mails to inform the recipient that the mail is an advertisement, and include their reply e-mail address. The company would also be forbidden to contact any user who had notified them that he did not wish to receive further ads from them. Early March, the Ministry of Economy, Trade and Industry (METI) also submitted a spam-curbing bill, and a certain degree of controversy broke due to the similarities of the bills and their seeming competitiveness.

While waiting for the law to go into effect, DoCoMo on their side were also coming up with new countermeasures. In January they made it possible for the users to restrict incoming mails to a maximum of 10 selected domains, including the domains of other mobile operators and ISPs. Within a couple of months, more than 1.5 million users were taking advantage of this new function. The spammers however quickly adapted, and started using fake domains for their e-mails, making it seem like the mails came from one of the carriers, i.e. another mobile phone. In April DoCoMo therefore implemented filters in their network to detect and stop mails coming from forged domains.

DoCoMo announced that in the previous fiscal year, ending in March, their anti-spam measures, presumably including the free 400 packets per month offered all subscribers, had costed them 27 billion yen (more than 2 billion SEK).

By July the 1st, the bills drafted during the spring had been approved and the "Law on topics including the appropriateness of sending specified e-mail messages" (law no. 26 of 2002) and the "Law for partial amendment to the specific commercial transaction law" (Law No. 28 of 2002) took effect. The laws require, with some exceptions, that senders of advertisements begin the subject line of each mail message with the Japanese characters for "unsolicited advertisement" plus the mark ※. The message must also include the sender's name, postal address and e-mail address, so that a recipient can send back an "opt-out" request. Once a user has responded negatively, the sender must not send any further e-mails to that address. DoCoMo immediately announced that the possibility to automatically block mails having "unsolicited advertisement" in the subject line would be available from October this year. As with all their other anti-spam measures, the set-up will be possible to do from the handset at no transmission charge.

2.4 The Wangiri scam

By late spring however, also the fixed operators were being affected by the problems on the mobile side. Since late 2001, the detested "wangiri-calls" have become a growing concern. Wangiri means calls that only ring once, and then are hung up. Often they come late at night or very early in the morning. The number of the caller is however stored in the receiver's handset and many users press "Call back" to see who tried to reach them. They are then connected to an automated answering service, usually with sexual contents. Soon afterwards a hugely inflated bill for the

"service" is sent to the user. If he doesn't pay, aggressive letters or phone calls may follow, threatening to expose the user's calls to sex services. There are no legal grounds for the payment demands, but many users still pay the official-looking bill, out of ignorance or fear.

The companies applying wangiri use special software to make thousands of calls per minute to cellular phones and hang up after the first ring-tone, if the call is connected. These calls clog up both the fixed and the mobile networks, and in May several fixed phone companies had applied for a similar change of law that DoCoMo had already been granted, which would allow them to deny service to companies that make massive callings to randomly generated mobile phone numbers. The request has not yet been approved, but already in July NTT's fixed arm decided to cut off a customer citing network damage caused by the company's activities. The firm, based in Osaka, used 216 lines and made more than 4 000 random calls every three minutes for several hours, to be compared with a total of between 2 500 and 7 500 calls made through the affected switches between 10:00 and 11:00 each day the week before. The massive traffic caused network disturbances affecting more than 5.16 million user lines. Complaints started coming in to NTT at around 10:00 in the morning, at which time NTT shut down the switch serving the customer to 50% capacity. At 10:59 the customer was closed down completely, but normal network service was not restored until 14:44, NTT officials said.

"In the past, telephone network disruptions were often caused by an influx of calls made to the same number at a time of natural disasters or fire. These days, one single caller can make numerous calls," NTT's president Norio Wada was quoted as saying in the Japan Times. NTT demanded that the government implements effective measures against wangiri and other schemes, including revision of legislation. An official at the MPHPT was however quoted as saying "Police can lodge charges if phone lines are used for crimes. But at this stage, it is a problem for the telephone companies and their customers." The minister himself asked to be allowed some more time to study the circumstances before making any decisions. He said that the first step, before taking legal measures, was to strengthen the contract clauses of the telecom operators towards their customers.

Tokyo police made their first arrest of a wangiri operator in April, but they arrested him for charges of pornography. Although most of the calls to the Tokyo Consumer Lifestyle Centre today are about worried people who have received bills after returning wangiri calls, "At the moment all we can do is tell people they have to take care of themselves, since there is no law that can protect them," an official working there was quoted by Reuter as saying. "This is purely a contractual agreement between NTT and a subscriber, so it's not really criminal, more a breach of contract", a senior telecom analyst at Merill Lynch in Tokyo explained.

NTT and the public do however not agree with this view. "The wangiri practice is a challenge to … (Japan's) social contract," the conservative Yomiuri newspaper said in an editorial August 5th, comparing the perpetrators to the noisy gangs that roam city streets at night. "If wangiri were to be carried out with political intent, it would be tantamount to cyber-terrorism," it railed.

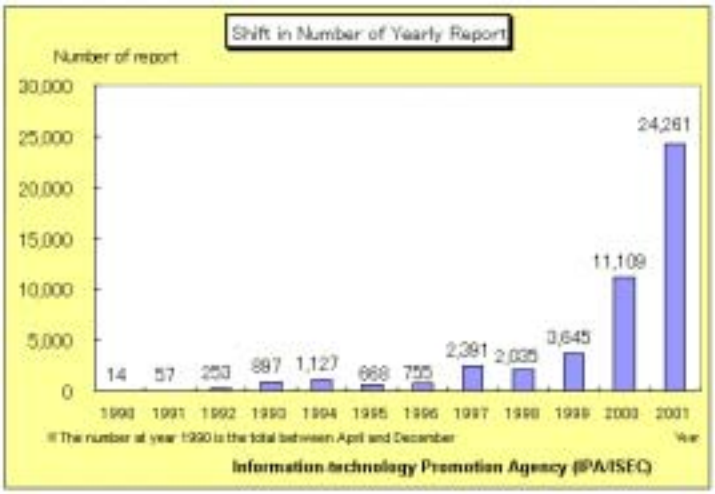
Meanwhile NTT has made the recommended revisions in the contracts with their customers, and August 20th they for the first time suspended service for a customer citing risk of network disruptions since the customer was “deliberately making a massive number of calls intended to go unanswered”. The suspension will remain in effect until the company in writing pledge to stop making wangiri calls. The revision in the contracts also allows NTT to refuse applicants that are considered potential wangiri operators.

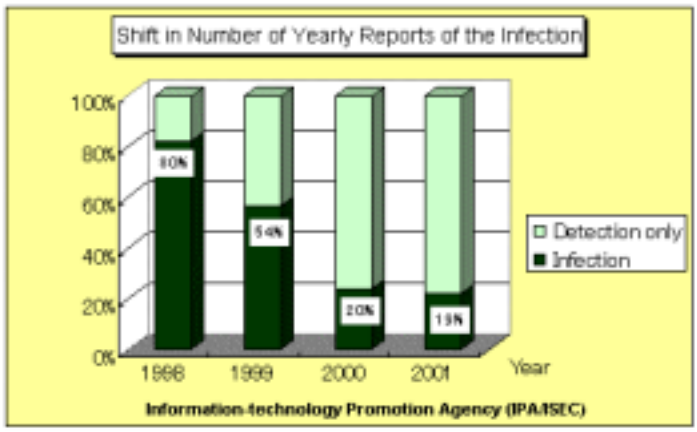
3 Computer viruses

In 1990, the Ministry of Economy, Trade and Industry (METI) issued the "Computer Virus Prevention Guidelines" including expectations for all victims of virus attacks to file a report with the Information-Technology Promotion Agency (IPA) (http://www.ipa.go.jp/ipa-e/index-e.html). The IPA was given the task to deal with each reporter (user) on an individual basis as a consultant, and also work as a public research institute for antivirus measures by analyzing problems occurring in the damage reports. They issue monthly reports with statistics, as well as the results of their research and analysis on computer virus incident. The data in this chapter comes from reports published by the IPA. It is important to keep in mind that the numbers only include cases that were reported by the victim of the attack to the IPA, making the real numbers presumably much higher.

3.1 Number of occurrences

The IPA stated in their virus discovery report for 2001 that there had been twice as many incidents reported 2001 as during 2000. The number of reports from individual users increased almost ten-fold.The good news however is that only 19% of the virus attacks were actually able to do any harm compared with for example more than 50% 1999. For the first half of 2002 that number had gone down even further, to 9%, while the number of reports had only increased 20% compared to the same period 2001.


Shift in Number of Yearly Report
Number of report
30,000
25,000
20,000
15,000
10,000
5,000
0
14
57
253
887
1,127
668
755
2,391
2,035
3,645
11,109
24,261
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
Year
※The number at year 1990 is the total between April and December
Information-technology Promotion Agency (IPA/ISEC)


Shift in Number of Yearly Reports of the Infection
100%
80%
60%
40%
20%
0%
80%
54%
20%
19%
1998
1999
2000
2001
Year
Detection only
Infection
Information-technology Promotion Agency (IPA/ISEC)

The individual users had a considerably higher occurrence of damaging attacks, indicating not surprisingly that the private users have implemented less virus protection than corporations have. Those seemingly least protected against damage by viruses were however educations and research institutes, where about one third of the reported attacks caused harm.

	2000				2001				2002 (Q1+Q2)	
	Total number of incident reports		Harmful incidents		Total number of incident reports		Harmful incidents		Total reports	Harmful incidents
Corporate users	**9 975**	*89.9%*	**1 480**	*14.8%*	**17 332**	*71.4%*	**2 793**	*16.1%*	*Not yet available.*	
Private, individual users	**920**	*8.3%*	601	65.3 %	5 643	23.2 %	1 479	26.2 %		
Education or research institutions	214	1.9%	101	47.2 %	1 286	5.3%	404	31.4 %		
Total	**11 109**		2 182 (19.6%)		24 261		4 676 (19.3%)		11 569	1 037 (9.0%)

3.2 Types of viruses

There were 112 different types of viruses reported during 2001, of which 22 types (occurring in 11 712 reports) were new. During last year most viruses still infected through the email systems, but the increase in viruses that infect through system weaknesses was dramatic, and so far during 2002 they have been dominating. There were 3 main types of viruses exploiting system weaknesses:

- Viruses that infect if the body of the virus-carrying email is viewed using Microsoft's Outlook or OutlookExpress (including Badtrans (a variant), Aliz and Nimda)
- Viruses that infect the computer even if the mail is not opened, but just previewed with Microsoft's OutlookExpress (including Badtrans (a variant), Aliz and Nimda)
- Viruses that infect when an infected web page is surfed using Microsoft's InternetExplorer (Nimda)

There are also many more new viruses that propagate themselves, such as W32/Aliz and W32/Badtrans (a variant).

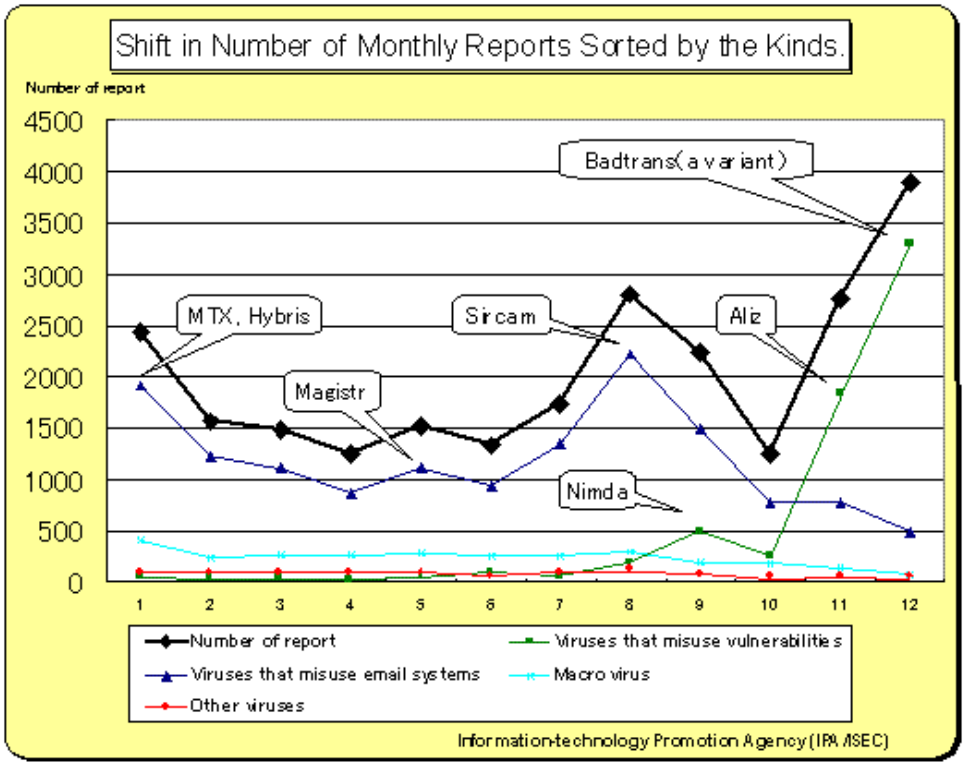
	2000		2001		2002 Q1+Q2		Major viruses
E-mail-using viruses	6 692	60.2%	14 263	58.8%	2 326	20.1 %	Hybris, Sircam, MTX
System weak-ness- using viruses	507	4.6%	6 338	26.1%	8 604	74.3 %	Badtrans, Aliz, Nimda
Macro viruses	3 393	30.5%	2 812	11.6%	480	4.1%	Laroux, Divi
Other	528	4.7%	848	3.5%	159	1.5%	QAZ, Funlove
Total	11 120		24 261		11 569		

Note: Those viruses that use both email systems and system weaknesses to infect, such as Nimda, are sorted under weakness-using viruses. Macro viruses include Melissa and Prilissa.
Since each report can include several types of viruses, the total number of viruses and reports are not the same

The virus that occurred in most reported instances was Hybris, followed by Badtrans which received more than 1000 reports in one single month (2701 reports in December 2001), Sircam (1257 reports in August) and Aliz (1020 reports in November).

For the first half of 2002, the most occurring viruses were W32/Klez (5005 reports), W32/Badtrans (2973 reports), and W32/Hybris (615 reports).

Virus name	2000	2001	E-mail-using viruses	System weakness –using viruses	Macro viruses
W32/Hybris	181	4,915	*		
W32/Badtrans(*)	-	3,281	*	*	
W32/Sircam	-	3,017	*		
W32/MTX	2,136	2,934	*		
W32/Magistr	-	1,894	*		
W32/Aliz	-	1,402	*	*	
XM/Laroux	1,041	1,034			*
W32/Nimda	-	891	*	*	
X97M/Divi	541	584			*
W32/Navidad	1,202	477	*		
Other viruses	6,019	3,832			
Total number	11,120	24,361			



3.3 Source of viruses

In an even higher degree than before, viruses arriving via e-mails dominate. The high numbers are a result of the very effective self-propagating viruses that have occurred recently, forwarding themselves to addressees in the Outlook address book in an infected computer.

Source of virus	1999		2000		2001		2002 Q1+Q2	
By e-mail	**2 443**	67.0%	**10 014**	90.1%	**21 581**	89.0%	**11 365**	98.2%
Downloaded	**195**	5.3%	**82**	0.7%	**593**	2.4%	**42**	0.4%
External media	**611**	16.8%	**428**	3.9%	**677**	2.8%	**49**	0.4%
Unknown	**396**	10.9%	**585**	5.3%	**1 410**	5.8%	**113**	1.0%
Total	**3 645**		**11 109**		**24 261**		**11 569**	

3.4 International comparison

During 2001, The Mitsubishi Research Institute performed an international survey on behalf of IPA, with the purpose of estimating damage done by virus attacks in USA, U.K., Germany, Korea and Hong Kong. 5000 questionnaires were sent out per country and about 500 responses were received from each.

The survey results can be found at the following site:

http://www.ipa.go.jp/security/english/virus/press/200204/E_PR200404refer.html

3.5 Mobile viruses

The Japanese mobile phones are now becoming so advanced that the first viruses specifically developed for them can be expected to appear soon. There have been occurrences of mails containing misleading links, and attachments that make the phones freeze, but so far most problems have been due more to badly designed and annoying programs or attachments than to purposefully malicious attacks.

In March this year IPA published the results of a test they had done to see whether viruses developed for PC-based Java could damage Java equipped mobile phones when sent to them. (http://www.ipa.go.jp/security/fy13/report/mobile_security/java-keitai.pdf, Japanese only.)

They tested the viruses Homer, Hijacker, Attacker, StrangeBreew and BeanHive, but the conclusion was that the compliers of the mobile Java are not yet powerful enough to compile the virus code, and no harm was therefore done. As the mobiles become more advanced however, the threat grows and operators and phone makers need to start thinking pre-actively about countermeasures.

4 Mobile dating services base for violent crimes

Here are some widely publicized and discussed crimes in Japan from the last couple of years:

- In January 2000, a medical doctor outside Tokyo was found guilty of paying to have sex with girls aged 17 or younger. The doctor told police that he had purchased sex from more than 100 young women.
- In March the same year, police arrested several men in Kyoto on suspicion of together raping a woman. The men did not know each other before they committed the rape.
- In May 2001, a Tokyo High Court judge was arrested on charges of violating the law against child prostitution by paying for sex with a 14-year-old schoolgirl.
- The same month a man in Kyoto was arrested for murdering two women.
- In June the same year an unemployed, homeless man was found guilty of drugging, robbing and abandoning two women -- a 24-year-old and a 20-year-old -- resulting in their deaths.
- Later that summer a 12-year-old girl was killed on an expressway as she handcuffed tried to escape the car of her abductor, and was hit by oncoming traffic.

The common denominator of all these violent crimes: the victims and the offenders got in contact with each other through dating services. In the case of the gang rape in Kyoto, it was the perpetrators who were recruited via the internet.

In Japan, telephone dating clubs have been popular for several years, but the fact that they let people get in touch with each other anonymously make them a convenient hunting ground for predators in crimes like the ones listed above. In response to this, the Diet in June 2001 passed a bill revising a law controlling the sex industry to prohibit people under 18 from using telephone dating clubs. The revised Law Regulating Businesses Affecting Public Morals requires telephone club operators to confirm that their clients are age 18 or over, and stipulates that calls from women to men are only allowed after the female customers have faxed identification documents to the club operator. Operators of clubs with no fixed premises are able to issue membership cards to females, with passwords to enable connection to the clubs, through video rental shops and other outlets after the woman has proved her age by an ID card. The law also requires Internet service providers to make efforts to prevent distribution of child pornography and prostitution.

As mobile internet became ubiquitous however, dating sites immediately turned up readily available on the cellular phone menus. With the recent boom of camera-equipped mobile phones, a large portion of the ads come with pictures. One editorial in the Asahi Shimbun in September 2001 read: "*Parents have taught their children not to go to entertainment districts alone and not to hang out late at night. People know from experience there are many temptations in amusement areas and danger is greater at night. The mobile phone, however, instantly transcends distan-*

ce and time and thus lessens people's hesitation and caution. And it makes dangerous meetings easily possible."

Many of the mobile postings are really thinly disguised ads for sexual services against payment. In Japan it has been a crime to buy sexual services from minors and to sell or distribute child pornography since 1999, but teen prostitution is still considered to be widespread. Numbers are difficult to come by since the problem is widely discussed more as a sign of the moral decline of the society than as a real issue that should be addressed by the authorities. But many high school students are alleged to see going out with elder men, or enjo kosai (compensated dating), as an easy way to make some extra money. With the mobile phone based services, it has become cheap and uncomplicated to post an ad, communicate with a prospective customer and set up a possible meeting. A typical ad on one of the mobile sites might read "17 year-old high school student wants yen. Is there a kind person who can meet me now in Shibuya? Please help! Make it 2 [=20 000 yen, about 1 600 SEK]. If so, I will send you my picture."

As use of the services proliferate, so do the crimes initiated by contacts taken via them. In year 2000, the police reported in total 104 crimes in connection with dating services. By 2001 the figure had risen to 888. Between January and June this year, already 793 cases had been reported. Out of these, mobile phones had been used in 758, or 96%, of the cases (2001: 85%). Of the 692 victims, 518 or 75% were minors (2001: 77%). Of these 508, or 98%, were girls.

The types of crimes included are listed below, with the numbers for the same period previous years listed within parenthesis:

- 400 cases of child prostitution (2001: 133, 2000: 41)
- 213 cases where juvenile-protection ordinances were violated (2001: 59, 2000: 20)
- 33 cases of blackmail (2001: 8)
- 23 cases of rape (2001: 20, 2000: 8)
- 13 cases of intimidations, theft and fraud (2001: 8)
- 1 murder (2001: 5, 2000: 1)

Sources: Reports from the National Police Agency as quoted in Asahi Shimbun Aug 23d 2002 and Nov 2nd 2001, Japan Times August 10 2001 and Japan Today March 1st 2001

In December 2001 the law against child prostitution was used for the first time to arrest an operator of a mobile messaging board that the police claim was set up for men to hire teenage girls for sex. Eight underage girls were found to be listed on the site, and one customer to one of the girls, a 17-year old, was arrested and subsequently fined 400 000 yen (about 32 000 SEK).

In March this year, one 16-year old boy, the youngest to face charges under the law ever, was investigated for having paid 35 000 yen (about 2 800 SEK) to have sex with a 14-year old girl. An 18-year old boy had introduced the two of them, without ever meeting any of them, via a mobile dating site, and mediated fees and meeting place.

5 A citizen database – convenience or police state?

In Japan there are no official, central databases, and no uniform way to identify yourself. Information about the citizens is stored, and often computerized, but the data is contained within each governmental body, and accessed only by sections at that local office. Various ID numbers, such as basic pension numbers or passport numbers, each belong to a separate, local numbering system.

Take a moment to reflect on the consequences. It means that if you want to change your address in the local registry you have to go to the municipality office where you are registered, in person, fill in the forms with your personal data, get them stamped, and then go to the new municipality office where you want to register. If you get caught speeding, you have to go back to the police district that issued the ticket, in person, to handle the administration. Same thing goes for applying for pensions, passports, or social benefits. Even the banks apply the same system: If you want a new code for your ATM card you have to go, in person, to the bank office where you opened your account, and where your original signature is stored, to identify yourself and have it issued. Data about you for a certain purpose is only stored and accessible from one point, with a different access key for each storage point. Central governments have to contact each different, local registry every time they need information about a citizen confirmed.

In August 1999 an amendment to the Basic Resident Register Law was approved, deciding that a nationwide, consolidated database was to be created in which every citizen has a serial number under the same system. The inaugural date for that database, the so called Juki Net, was set to August 5th 2002.

In this system, each citizen will be assigned an 11-digit number used to store a computerized resident's card with the individual's number, name, date of birth, gender, home address and record of changes to the data. The information will be stored online in a dedicated database, and be accessible from any local government office for pre-approved purposes. On request, the local government will give citizens individual Basic Resident Register Cards, containing a memory chip and the above information. The local governments will be able to use these cards for welfare and other public services, such as library loan registration, etc. And at a farther horizon, the card plays a role in the e-government plan, where citizens will be able to handle all official paperwork from their own home computers.

To start with, the ID numbers will be used in 93 kinds of administrative services, including issuance of resident certificates. A government bill now on the table is designed to increase the number by 175, including issuance of passports. The new system offers the "convenience of taking one's resident ward office wherever one happens to be," as officials have explained it.

Considering the simplifications it brings to the lives of the Japanese people, the government had not counted on much resistance to the online registry. But surprisingly the Juki Net was the subject for an increasing number of critical newspaper articles, protest marches and rallies during the months before inauguration. In a

survey taken during the summer among 3 241 local governments by the Japan Federation of Bar Associations, with a 46% response rate, 14 percent of city governments said the network should be postponed, while 60% remained ambivalent. In addition, 36 percent said the cost of the network is too high.

The main concern is privacy and security, and fear of what a state with centralized control and access over citizen information can become. No matter that representatives for the government and some newspaper editors repeatedly have urged for calm and reason, stressing that the new system is necessary and safe, that the responsible ministry is implementing dedicated lines, encryption technology, fire walls and intrusion-detection programs to protect the individual's privacy. Newspaper headlines and protesters' signs have been screaming "We are not numbers!" and "Police state". Makoto Sataka, a social and economic critic said to the Japan Times in connection with a rally: "In the resident registry network system, the state will become a stalker with control over personal information. … Prison is the only place where the authorities control people with numbers. With this system, the Japanese system will be put in a prison state."

Even around the lunch table here at the embassy the discussion has been heated, with the mistrust of the new system being genuine and deep-felt. Everyone knows that the same data is already being stored in databases everywhere. They know that the current system is in no way safe from abuse (imposters wanting to use someone else's identity only has to sit down at one of the many writing tables at the local municipality, and look over the shoulder of someone filing in a form with his or her personal data, and copy it for their own purposes.) Still, the thought of personal data being accessible from anywhere in the country, and accessible with the same ID number as key, has made the whole nation uneasy.

The responsible ministry, MPHPT, has not managed to implement a consistent information strategy that might have succeeded in dampening the fears. Preparations have been elaborate but guarded. All that is known physically about the system is that it will be centered within Tokyo. Asked to provide more information, the minister replied, "More cannot be disclosed for security reasons."

About three years ago, then Prime Minister Obuchi explained in the Diet that the condition for implementing the Juki Net was a swift preparation of a system including the development of a personal information protection law covering the private sector, something that today does not exist. Also the current health, labor and welfare minister stated at the time that "a comprehensive personal information protection law is indispensable to [the Juki Net's] implementation".

The personal information protection bill was drafted and widely debated this spring. Critics found it wanting in terms of preventing data leaks and other abuses. Moreover, it included questionable plans to control media activity. Faced with public criticism, the proposed privacy legislation was carried over to the next session. Lacking a legal protection of the data stored in the Juki Net, voices have been raised asking for a postponement. Replying to this, Chief Cabinet Secretary Fukuda said, "In general, the words spoken by a former prime minister at the Diet will not - legally speaking - technically bind the actions of the Cabinet that follows. I believe,

however, that we should take heed of Prime Minister Obuchi's words in a political sense."

Nonetheless, on the day the Juki Net was to be taken in service, and the 11-digit codes were to be distributed to the citizens, four municipalities refused to join the system, citing fear the system could be ripe for abuse. Another city, Yokohama, said it will only register its 3.45 million residents with their consent. As a result, about 4 million people nationwide were left off the network.

In addition, a city which had joined the system said it would probably pull out in September, and another city delayed registering its residents for one hour to express its "humble protest". The press also gleefully reported that 32 of the 3 300 municipalities had experienced computer related problems during the first day of operation, while the responsible ministry said that problems in such small numbers were expected and unavoidable, and that, as a whole, the introduction had been a success.

6 Trying to regulate the net auction jungle

Japan's online auction sites have been doing a roaring trade. Yahoo! Japan has more than 90 percent of the market, with some 1.3 million of its 23 million users actively using the auction service. Daily transactions have reached the hundreds of millions of yen, and participating in online auctions is now one of the most popular Web activities for PC users in Japan. But almost from the beginning, online auction sites have been dogged by fraud and the fencing of stolen and illegal goods, raising the spectre of tighter regulation.

In the beginning, all you needed to sell something on Yahoo!'s auction site, for example, was an email address. Coverage of fraud and fencing in the media has forced all sites to start requiring positive ID, and in March 2001, Yahoo! even went so far as to establish a fixed ID registry for all sellers, for which it charged a monthly fee by credit card. EBay established an insurance system to ensure that any buyer who failed to receive the product purchased could be compensated.

But all this none withstanding, Japanese police have seen a steep increase in complaints, particularly in the pre-Christmas season of November-December 2001, and the existing regulations and laws don’t cover the cases occurring. The current law predates the Internet, and police here have not applied its provisions as stringently as they do to off-line auction companies. As an example, only off-line auctions must be licensed, and online auctions are also relieved of the obligation to identify the seller. They now try to do so anyway, but in many cases of fraud, the seller's information turns out to be fake or the ID belongs to an innocent third party.

In February, Japanese and US media including the Nihon Keizai Shimbun and New York Times carried reports of a proposed shakeup in Japan's online auction industry initiated by the national police agency, NPA. The controversy focused on a package of legislative proposals floated by the agency late in December that would require operators of online auction sites to obtain licenses, post their contact information and license numbers on their auction sites, inform police if they discover any stolen goods being offered for sale via their site, maintain transaction records, and submit to supervision by prefectural public safety commissions, which would have the power to suspend a Net auction operator found to be in violation of the rules.

With public opinion in mind, several online auction sites have publicly endorsed the proposed NPA regulations. Yahoo! has posted supporting commentary on its site, and one spokesperson for DeNA says customers could "participate in online auctions with more confidence and feel safe under the regulations," adding that "they might help prevent bad sellers from selling stolen goods."

There are however several weaknesses in the NPA proposals. They do not make clear which sites would be deemed 'official' (and hence be obligated to obtain licenses and submit to supervision). Sites offering free or limited auction services may end up outside the police control. The proposed legislation also lacks a clear standard for determining whether an item is stolen.

METI disputes the propriety of the proposed regulation on the grounds that it could run counter to the government's policy to foster the development of new industries. Many Japanese also use auctions sites operated by foreign auctioneers, and it is not explicitly clear whether the proposed law would apply to foreign-owned online auction sites. Some worry that regulations that apply only to Japanese businesses, without equivalence in other countries, could hurt the competitiveness of Japanese internet firms.

Internet security expert Gohsuke Takama says in JapanInc, regarding the potential problems with implementing the regulations across borders: "*Applying one country's local laws to any Internet industry will cause problems -- especially international jurisdiction issues -- and the people who put this legislation together clearly didn't consider that. How can a used-goods broker law in Japan be applied to an Internet auction company which is registered outside of Japan, owned by non-Japanese, has transactions processed through a credit card company located outside of Japan, operates on Web servers located outside of Japan, but has Japanese pages?*"

The auction sites also, naturally, worried about this aspect. "We strongly hope these regulations don't over-control us and will not be an obstruction for free competition in a free Internet market," a spokesperson for DeNA, one of the auction sites in Japan is quoted as saying. An editorial in Nikkei Weekly commenting the issue read: "…*But companies around the world are engaged in ruthless competition in the rapidly evolving cyberspace. Any effort to set rules for Internet businesses should not rely solely on the initiative of government authorities. Such an attempt would require flexible thinking and feedback from those outside the government.*"

7 Web sites allowed in election campaigns

A government advisory panel proposed early August to lift a ban on the use of Internet sites pages for election campaigns. "We cannot discuss democracy in the 21st century without taking the Internet into consideration. The use of Web sites will enable voters to easily gain information about candidates," Ikuo Kabashima, who leads the panel on election campaigns, told a press conference, as reported by Kyodo News agency.

Meanwhile, the panel does not recommend allowing candidates to send campaign e-mails due partly to concerns they may be sent unsolicited to voters who do not want to receive them.

The Ministry of Public Management, Home Affairs, Posts and Telecommunications will consider revising the current public office election law, based on the proposals, its officials said.

8 Abbreviations used in this newsletter:

NPA:	National Police Agency
MPHPT:	Ministry of Public Management, Home Affairs, Posts and Telecommunications
MEXT:	Ministry of Education, Culture, Sports, Science and Technology
MHLW:	Ministry of Health, Labour and Welfare
METI:	Ministry of Economy, Trade and Industry
IPA/ISEC:	Information-technology Promotion Agency Security Centre
ISP:	Internet Service Provider
NTT:	Nippon Telephone and Telegraph (Japan's incumbent operator)
DoCoMo:	NTT DoCoMo (NTT's mobile arm, Japan's largest mobile operator)

ITPS, Institutet för tillväxtpolitiska studier
Studentplan 3, 831 40 Östersund
Telefon: 063 16 66 00
Fax: 063 16 66 01
info@itps.se
www.itps.se

itps INSTITUTET FÖR TILLVÄXTPOLITISKA STUDIER