APNIC

Apster

Apster is the quarterly newsletter for APNIC members and the Internet community.

Issue 19 - September 2006

Internet in Taiwan

As APNIC holds its 22nd Open Policy Meeting in Kaohsiung, we look at the development of Taiwan's Internet industry, from the early educational networks of the 1970s and 80s through to its current position as a world leader in Internet technology.

Early days and development

In the 1970s, Taiwan established a contract with Stanford Research International in the USA to assist in developing Internet knowledge and infrastructure. During this time, Taiwan also developed its own cable communication industry with the help of Japanese investment.

In the 1980s Taiwan's Ministry of Education played a key role in the early stages of Internet development in Taiwan. Using IBM's mainframe, the Ministry of Education Computer Center (MOECC) established a teaching service station servicing some private university campuses in 1986. This was the earliest prototype of the heterogeneous inter-campus Network (IFNET/Decnet, UNINET/Cybernet, BITNET) in Taiwan.

In 1987, the first international academic network in Taiwan was built and connected to SUT (Science University of Tokyo) and transited to the USA. Several projects were also initiated by other key governmental or private institutions, such as the SEED (Software Engineering Environment Development) project by the MOEA (Ministry of Economic Affairs), and FMAN (Fiber Metropolitan Area Network) by the MOTC (Ministry of Transportation And Communications).

Between 1996 and 1999 community Internet penetration rates rose from three percent to 22 percent. Two commercialised ISPs (HINET and SeedNet) commenced operation in the mid-1990s. The first six months of 1999 marked the most significant phase of Taiwan's Internet growth. By the end of the 1990s, the number of Internet users had reached four million.

Current situation

Telecommunications liberalisation has brought about rapid growth in Taiwan's online population and increased Internet usage by individuals and companies. A recent report by Point Topic (courtesy of Taiwan's Focus on Internet News & Data service) indicates that Taiwan is now ranked fifth in the world in household broadband penetration (83%) and eleventh in the number of broadband subscribers (4,442,000 lines). Most broadband users are located in the metropolitan centres, Taipei City and Kaohsiung.

The future

In 2006 the New York-based Intelligent Community Forum acknowledged Taiwan for its continuing efforts in Wi-Fi development. Currently, wireless access is available in major business areas and MRT stations throughout Taipei. As part of the official 'Wireless Taipei' project, Tamsui became Taiwan's first region to offer 100 percent wireless access.

In 2001, Taiwan launched 'E-Taiwan' as part of the Challenge 2008 initiative. E-Taiwan aims to build upon Taiwan's existing networking capabilities, establish an IPv6 development plan, and move towards e-government. According to the fourth annual global e-government study conducted by Brown University, Taiwan ranks first in e-government. The survey criteria included availability of online publications; databases, disability access, and services; and the level of privacy and security.

TWNIC

Taiwan's NIR, TWNIC, is responsible for both domain name registration and address space allocation. The establishment of TWNIC can be broken down into three major stages:

Stage 1: 1994 to 1996, Taiwan Network Information Centre established as a 2-year experimental program

Stage 2: 1996 to 1998, TWNIC administered by the Computer Society of the ROC (CSROC);

Stage 3: TWNIC was officially registered as a corporation on 29 December 1999.

Taiwan's evolution into a high-tech economy is reflected by the fact that APNIC 22 in Kaohsiung is the third APNIC meeting TWNIC has hosted (two meetings have previously been held in Taipei).

Many thanks to Ian Chiang at TWNIC for his invaluable assistance in preparing this article.

Tina Bramley

Sources:

TWNIC http://www.twnic.net.tw

Digital Review of Asia Pacific 2005/2006
http://www.digital-review.org

FIND – Focus on Internet News & Data
http://www.find.org.tw/eng

22nd APNIC Open Policy Meeting
4 - 8 September 2006 Kaohsiung - TAIWAN

P 2

▲ Kaohsiung, on the south-west coast of Taiwan, is the venue for APNIC 22.

APNIC invites anyone with an interest in Internet address policy to attend the 22nd APNIC Open Policy Meeting (APNIC 22), which will be held from 4-8 September, 2006 at the Grand Hi-Lai Hotel in Kaohsiung, Taiwan.

The APNIC 22 program includes the APNIC Member Meeting, tutorials, and sessions covering issues such as protecting your network, IPv6 policy, and member fee schedules.

For more information on any aspect of APNIC 22, visit:

http://www.apnic.net/meetings/22

APNIC 22 policy proposals

Below is a summary of the nine policy proposals to be discussed at APNIC 22 meeting in Kaohsiung, Taiwan. If you are not able to attend the meeting in person, you are invited to participate remotely. For information on how to do this, see:

http://www.apnic.net/meetings/remote

To read the proposals in detail, go to:

http://www.apnic.net/policy/proposals

Policy SIG proposals

prop-033-v001: End site allocation policy for IPv6

This proposal removes the minimum assignment size of /48 for an end site, allowing the unit of assignment to be the LIR's decision. If only one subnet is anticipated for an end site, the minimum assignment size is proposed to be /64. To cater for the differing assignment sizes allowed under this proposal, it is further proposed that APNIC measure utilisation of IPv6 address space in terms of the bits to the left of the /56 boundary.

prop-034-v001: IPv6 portable assignment for end user organisations

This proposal allows portable IPv6 assignments of at least /32 to be delegated to end user organisations that multihome, plan to multihome or require a portable IPv6 assignment for other administrative or technical reasons. It is proposed that these assignments should be made from a designated 'super block'. It is proposed that if an alternative technical solution is found for multihoming, assignments made to multihomed organisations under this policy should be returned within three years of the technical solution being deployed.

prop-035-v001: IPv6 portable assignment for multihoming

This proposal allows end sites that currently multihome or plan to multihome to receive a portable assignment. The minimum assignment size would be /48, which is the same as the minimum size of non-portable assignments.

prop-036-v001: Proposal to allow end sites to receive IPv6 allocations

This proposal expands the criteria for an initial IPv6 allocation to include end sites and broadens the types of sites an organisation can provide IPv6 connectivity to. The proposal removes the requirement to have a plan to make 200 /48 assignments in two years and replaces it with a plan to make a reasonable number of /48 assignments in two years. The proposal also removes the requirement for LIRs to document the need for assigning multiple /48s to a single end site.

prop-037-v001: Deprecation of email updates for APNIC Registry and whois data

This is a proposal to phase out email updates to whois data. It is proposed that before deprecating email updates, the APNIC Secretariat would provide an alternative mechanism that is suitable for automated and secured registry transactions.

prop-038-v001: Amending APNIC's lame DNS reverse delegation policy

This proposal modifies the definition of lame DNS to be consistent with the definitions used by the other RIRs. Under the proposal, if a delegated nameserver for a domain fails to return a valid authoritative answer for the domain's SOA, it will be considered to be lame. The proposal also simplifies the process for monitoring and removing lame reverse DNS delegations.

prop-039-v001: A proposal to improve reachability of new IANA blocks

This is a proposal to establish a full-scale service operated by all RIRs to establish a site for ISPs to confirm reachability of new IPv4 and IPv6 prefixes allocated by IANA to the RIRs.

prop-041-v001: IPv6 assignment size to critical infrastructure

This proposal modifies the existing critical infrastructure assignment policy by clarifying that the maximum assignment size of IPv6 address space to critical infrastructure is /32 per operator.

APNIC Member Meeting

prop-040-v001: Proposal for APNIC non-member annual service fee

This proposal updates the service fees for non-member services, including the maintenance by APNIC of historical resources (that is, resources obtained prior to the establishment of APNIC). The proposal introduces a clearer and more consistent fee structure, incorporating account keeping and per-resource fees for all resources.

APNIC membership fee structure proposal

This informational presentation introduces a proposed new fee structure for APNIC membership. The proposed structure is designed to address problems with the current fee structure, including fairness, affordability for small members, and consistency of NIR fees. While this proposal will not be the subject of a membership vote during APNIC 22, it is hoped that a new structure can be established and implemented by 2008.

'APNIC Interactive' CD update

The purpose of the APNIC Interactive CD is to provide information about APNIC services in an easily navigable and entertaining way. The CD format assists community members with low bandwidth problems to access information, and showcases a range of in-house-produced multimedia presentations.

The CD was launched at APNIC 21, and will be included in the meeting pack for APNIC 22, as well as being available to training attendees and anyone wishing to obtain a copy from the Secretariat. The information contained on the disc covers five areas:

- APNIC information – useful to both prospective and current members
- Meetings – including highlights and webcast presentations
- Training – considerably reducing paper usage (the cover is also printed on recycled cardboard)
- Internet resources
- Tech corner

The content of APNIC Interactive is continually being revised and refined by its creators, APNIC staff members Chris Buckridge, Nurani Nimpuno, and Yun Jeong. the purpose of the project is to better meet the needs of APNIC community members, so all feedback is welcomed.

To obtain a copy of the CD, obtain more information, or provide feedback please contact secretariat@apnic.net.

▲ The updated APNIC Interactive CD, including a new sleeve design printed on recycled cardboard.

index

APNIC launches eLearning

Training has been a central concern of APNIC for many years, and APNIC staff have conducted face-to-face training sessions in locations throughout the Asia Pacific. While face-to-face sessions have many benefits, however, they have restricted the number of people who could participate in APNIC training. A new initiative of the APNIC training department, eLearning, hopes to change that.

eLearning is a training delivery method which offers an alternative to traditional face-to-face learning. Using electronic delivery systems (focused primarily around the web browser), eLearning can provide a diverse learning experience catering to a wide variety of learners via forum discussions, web-casting, web seminars, live chats and other media.

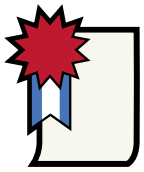
The value of eLearning is that it allows for an interactive learning experience regardless of geographical distance and differing time zones. The training department will continue to provide traditional face-to-face sessions, but it will mean that there is a viable alternative for those members of the community who are unable to attend in person. As an ongoing part of the training program, eLearning will integrate with other activities, including external training sessions and APNIC meeting tutorials.

The APNIC eLearning program is being launched at the APNIC 22 meeting in Kaohsiung, Taiwan, from 4-8 September. Related meeting activities will include a Birds of a Feather (BoF) session on training and education. The session will discuss, among other things, the integration of eLearning into the broader APNIC training program. There will also be an eLearning corner where meeting attendees can learn more about eLearning, try it for themselves, and a competition for those who register and use the eLearning computers.

For more information on the APNIC eLearning program, visit:

www.apnic.net/training/elearning

Certification of IP resources



As APNIC continues to lead the development of a future IP resource certification service, one of the key developers, Geoff Huston, discusses the motivations behind the project and fundamentals of the how the service could work.

The Internet has presented us with some novel challenges as it undertakes the role of a global communications platform. These challenges include creating applications that support new communication paradigms, as well as encountering an entirely new realm of security considerations. It is in this latter area, and in particular the aspect of network infrastructure security, that resource certification can play a critically important role.

One of the common vulnerabilities for the Internet lies in the routing subsystem. If it is possible to inject false information into the routing system, then a number of forms of hostile attack are enabled. In this case there is no need to compromise the proper operation of any particular application, nor is there any need to create a drone army through the assembly of captured end systems. By being able to manipulate the network's routing state it is possible to redirect user traffic, and perform traffic inspection, alteration, or subversion, all without the user even being aware of the attack.

Through deliberate subversion of routing, services can be hijacked or blocked, and entire networks can be black-holed. Why is the Internet's routing system – the integrity of which appears to be so critical to the proper functioning of all forms of Internet services – such a point of vulnerability?

The answer lies in the nature of the Internet.

A more historical model of network service provision was that of a small number of qualified network service providers and an associated set of network clients. The trust model within such a framework spans across the network service providers, and explicitly excludes the client base. Examples of such a framework include the international postal system, or the public switched telephone system.

The Internet has a broader model of a network service provider that includes various forms of networks that would normally be considered as clients rather than peer network service providers, and the ensuing trust domain is both very broad and very diverse. Indeed it is so diverse as to make the term 'trust' inapplicable.

In such an environment, networks interconnect by means of exchange of routing information relating to address prefixes. So, when a client network requests its ISP to accept a routing advertisement for a particular address prefix, how can the service provider establish whether the request is valid and the addresses are indeed ones that properly can be associated with the client network? When two ISPs enter into a peering arrangement at a local exchange how can each ISP tell whether all the route advertisements from the other ISP are valid?

This task of establishing validity of routing requests and routing advertisements is one that has serious repercussions for getting the wrong answer, particularly if the ISP admits a malicious route into the routing fabric.

There are various information resources available today that can assist in validating a routing request, including whois database queries and Internet Routing Registries (IRRs), but such resources have some problems with the currency, accuracy, completeness, and validity of the information they present. Validating a routing request or a routing advertisement can quickly become an exercise in data mining across a rather diverse set of potentially conflicting information sources. Such a validation task can be complex, expensive to undertake, and with outcomes that are not totally trustworthy. In an industry of low margins and cost constraint, it is not surprising that route validation, particularly in complex cases, is often performed in a haphazard fashion, leading to a continual series of incidents of attack via deliberate subversion of the route admission process, and in consequence, deliberate subversion of the routing system.

Can we improve this situation? Is it possible to both improve the level of accuracy of validation, while at the same time making validation fast, efficient, accurate, and cheap?

One possible approach to this is through the use of public key cryptography, coupled with a public key certificate infrastructure. In such a framework, IP resource holders (address and AS numbers) hold a private key that is associated with their resource holdings. The corresponding public key is certified by the resource issuer, where the public certificate lists both the matching public key and the resource holdings. This certificate is signed by the issuer's private key. Any document signed with the resource holder's private key can be readily validated against the issued certificate, and if the document contains a reference to an IP resource, this resource can be compared to that listed in the certificate.

In effect, the certificate represents a form of 'right-of-use' of an IP resource, granted by the resource issuer. For example, if an entity has been assigned the IP address block 192.0.2.0/24 and wishes an ISP to route that address prefix on its behalf, it would sign a route request with its private signature and attach the associated resource certificate. The recipient of the route request could validate the signature against the certificate, and check that the address block in the certificate encompasses the address block 192.0.2.0/24. This certificate is then validated in the context of a Resource Certificate Public Key Infrastructure (PKI). If the certificate is validated, then there is a high degree of confidence that the routing request is legitimate, in that it came from the current holder of the resource and the resource itself is validly assigned to that entity for its use.

To validate these resource certificates, a Resource Certificate PKI is proposed. In this case, a hierarchical PKI model is appropriate rather than a 'web of trust' model. In a hierarchical PKI model validation entails not only validation of the certificate, but also validation of the issuer's signature in the certificate. This, in turn, requires validation of the parent certificate that certifies the issuer's public key, and so on. This validation path terminates when a self-signed 'trust anchor' certificate is encountered.

The approach proposed in this resource certificate model is for the RIRs to undertake the role of trust anchors for IP resources; a certificate is valid if there exists a sequence of valid certificates from an RIR trust anchor to the certificate being validated. The certificate validation path follows the existing resource allocation path; when an RIR performs a resource allocation it would also issue an associated certificate to the resource recipient with the allocated resources listed in the certificate. If the recipient is functioning as a redistribution point (such as a Local Internet Registry) then it too would issue certificates corresponding to resource sub-allocations that it performs, and so on.

Validation of a resource certificate is then directly analogous to unraveling and validating a sequence of whois resource allocation records from the RIR to the target entity, although in this case the path is deterministic and the information model being used is consistent along the entire certificate path.

How can such resource certificates be used to improve the situation with respect to routing security?

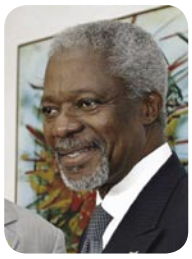
This resource certificate framework can also be used as the supporting infrastructure for security-related refinements in inter-domain routing protocols. One approach, sBGP, proposes adding digital signatures to BGP update messages, allowing a BGP peer to validate the authenticity of the address prefix being advertised, as well as allowing for validation that the update message itself

has traversed the same network path as that asserted in the AS PATH attribute of the update message. Another approach, soBGP, proposes the use of digital signatures to flood inter-AS topology information across the network. This, when coupled with signed origination of address prefixes, allows the receiver of the update to validate the address prefix and determine if the AS PATH attribute is a plausible one in terms of network topology.

While it is likely that it will take some time to achieve complete deployment of a secure inter-domain routing infrastructure, there is considerable value in being able to simply improve the trust model in the current environment of use routing requests, IRRs and WHOIS databases. Within such a framework digital objects, such as routing requests, IRR objects or WHOIS entries could be signed by the resource holder. This allows third parties to validate the information, validate the implied currency of 'right-of-use' of the resource, and validate the resource itself in an automated fashion. This makes the exercise of confirming the accuracy and validity of routing information and routing requests one that can be performed with a high degree of accuracy, as well as quickly and efficiently.

There are a number of current activities associated with resource certificates and the effort to improve the security properties of the Internet's inter-domain routing system. APNIC, in cooperation with the other RIRs, has embarked on a trial of resource certification. The effort includes an open source toolkit and associated documentation as well as an exercise in prototyping the integration of certificate management into the resource management framework. Within the Internet Engineering Task Force, the Secure Inter-Domain Routing Working Group (SIDR) has been chartered to develop standards relating to securing inter-domain routing protocols.

IGF program begins to take shape



▲ United Nations Secretary-General Kofi Annan

Source: Ricardo Stuckert/ ABr 14 Nov 2003 ©

▲ Adiel Akplogan, CEO of AfriNIC

▲ Raúl Echeberría, Executive Director of LACNIC.

United Nations Secretary-General, Kofi Annan recently announced that the inaugural meeting of the Internet Governance Forum (IGF) will be held in Athens, Greece, from 30 October to 2 November 2006.

The IGF is one of the products of the World Summit on the Information Society (WSIS), a two-year process of international dialogue to establish the foundations of an Information Society which benefits all nations and people. Throughout that process, discussions of Internet governance were prominent and often controversial.

In announcing the first IGF meeting, Mr Annan explained that "Two rounds of consultations open to all stakeholders … have contributed towards a common understanding with regard to the format and content of the first IGF meeting. I have also appointed an Advisory Group with the task of assisting me in preparing the IGF meeting".

The RIR community is represented on the 46-member Advisory Group by Raúl Echeberría, Executive Director of LACNIC and Adiel Akplogan, CEO of AfriNIC. Other members are drawn from governments, the private sector and civil society.

As RIR heads, both Echeberría and Akplogan are members of the Executive Council of the NRO, which has noted that these appointments signify "the important contribution the NRO plays in the Internet community and also reflects the integral role of the Regional Internet Registry system in Internet operations".

Following the recommendations of the Advisory Group, Mr Annan has announced that the overall theme of the meeting will be "Internet Governance for Development" and that the agenda will be structured along the following broad themes:

- Openness - Freedom of expression, free flow of information, ideas, and knowledge
- Security - Creating trust and confidence through collaboration
- Diversity - Promoting multilingualism and local content
- Access - Internet connectivity: Policy and cost

Cutting across all themes will be a priority on capacity building.

"WSIS saw the beginning of a dialogue between two different cultures: the non-governmental Internet community, with its traditions of informal, bottom-up decision-making; and the more formal, structured world of governments and intergovernmental organisations," said Mr Annan.

"It is my hope that the IGF will deepen this dialogue and contribute to a better understanding of how we can make full use of the potential the Internet has to offer for all people in the world".

Rather than seeking to produce negotiated decisions or formal resolutions, the outcome of the IGF is to intended to be a report of the individual sessions and the meeting as a whole. All material used as input for the IGF will remain archived on the IGF web site.

However, the IGF has also noted that another possible outcome will be so-called "dynamic coalitions", described on the IGF web site as "a group of institutions or people who agree to pursue an initiative started at the inaugural IGF meeting". Exactly what shape such coalitions may take remains to be seen.

More details about the IGF, including program information, archived submissions and contributions, and a full list of the Advisory Group members, are available at:

http://www.intgovforum.org

A greener APNIC

Over the past year, environmental concerns have moved into the world spotlight like never before. Issues like global warming and the price of oil have inspired governments, businesses, and individuals to examine their relationships to the natural environment. The discouraging news is that many of our standard practices, learned over decades, waste precious resources, often with little or no economic benefit.

The issues being raised by the scientific community are of particular concern in the Asia Pacific region. If predictions of rising sea levels are correct, many AP communities, particularly the low-lying Pacific island nations, will bear the brunt of the changes. Meanwhile the continuing economic growth of China and India means that the region's demand for energy will increase dramatically over the coming years.

The business community bears a great deal of responsibility for pollution and the creation of greenhouse gases. However, this is not restricted to the obvious industries, such as manufacturing or transportation. Even an office involved in a business like Internet services can waste a surprising amount of energy and resources.

With that fact in mind, the APNIC Secretariat recently launched Eco-APNIC, a staff-driven project aimed at reducing the "ecological footprint", or environmental impact, of APNIC work practices.

The Eco-APNIC working group has examined the day-to-day operations of the Secretariat. We have identified a variety of ways in which APNIC and its staff can be more environmentally friendly, without compromising the services that we provide to members and the Internet community. It is hoped that by doing this, APNIC will not only reduce our own impact on the environment, but will also set an example for other businesses and organisations around the region to follow.

Described below are some of the steps that APNIC plans to take to reduce our ecological footprint. These may include options also relevant to your organisation.

Travel

Long distance travel is an important part of the APNIC Secretariat's work, whether it be for Open Policy Meetings, regional training events, or outreach and liaison activities. Air travel, however, is a major contributor to global warming, with aircraft producing carbon dioxide, water vapour, and nitrogen oxides, all of which contribute to the formation of high altitude cloud formation, and destroy ozone.

One way for businesses and individuals to neutralise this impact is "carbon offsetting". Organisations like:

- Climate Friendly (www.climatefriendly.com)
- Climate Care (www.co2.org), or
- Sustainable Travel International (www.sustainabletravelinternational.org)

make it is possible to offset your greenhouse gas production by paying a certain price per tonne of greenhouse gas. This money is used to fund projects which will save or re-absorb an equivalent amount of carbon dioxide, such as renewable energy production or reforestation. APNIC is currently investigating options for offsetting the carbon dioxide which staff travel produces.

- On a local scale, staff have begun to organise car pooling for travel to and from work, reducing the number of cars being driven to the office and the amount of greenhouse gas produced, as well as saving money on fuel.

Recycling and office supplies

Paper is perhaps one of the most common areas of office wastage, but it is also one of the most easily addressed. A preliminary audit found that the APNIC office used just over 200 reams of paper during the first half of 2006.

- Small changes in individuals' office practices can make a significant impact on this, however, by defaulting to double-sided printing and printer settings like "draft", which save on toner.

Because an office will always rely on paper and printed material to some extent, it is also vital that paper use practices be as environmentally responsible as possible.

- Recycling (separating waste paper for recycling and, just as importantly, buying recycled paper) is the key strategy here, and its impact is significant.

US conservation group Conservatree has estimated that one ton of uncoated, non-recycled office paper uses 24 trees. Not only does recycled paper destroy fewer trees, but its manufacture also uses up to 90% less water and 50% less energy than conventional paper manufacturing.

While recycling paper is relatively easy for many offices, recycling is about more than just paper or plastic. Computer parts, printer cartridges, and other used electrical items are also a major problem. This "e-waste" is, in many ways, far more dangerous than paper waste. Many electrical components contain materials such as lead, cadmium, mercury, and arsenic, all of which leach into the environment when they are dumped. This is of particular concern in the Asia Pacific region; with western nations exporting e-waste to economies including China, Vietnam, India, the Philippines, and Indonesia, this waste disposal has raised numerous environmental concerns [DOT-COM Activity: Asia & Near East Computer Recycling Study].

- The APNIC Secretariat has identified a number of local options for recycling computer and electrical equipment. For other economies around the region, many of the larger computer companies, including Dell Asia Pacific, Apple, and Sony, run recycling programs for their customers.

Using energy efficiently

Between heating, cooling, lighting, and computer operation, the energy use of an average office can be surprisingly high. An important first step in the Eco-APNIC project has been to identify areas where the APNIC office could save on energy. One major area, naturally, is computers.

Energy usage varies dramatically between computers. Laptops use far less power than desktop models, LCD displays use less energy than CRT monitors. Perhaps the most significant factor, though, is simply leaving our computers switched on. People leave computers turned on overnight for a range of reasons, including the mistaken, but widespread, belief that the "power surge" created by turning a computer on or off uses more power than leaving the computer in "sleep" mode.

- In reality, the average computer uses 49 watts when fully on, 29 watts when "asleep", and 2 watts when switched off; the "power surge" on start-up uses the equivalent energy of a few seconds average running time.

eco APNIC

- Similarly, many people use a screensaver when away from their computer screen, when switching off the monitor will use 90% less energy.

Seemingly small changes such as these, when multiplied by each person in the office, each day of the year, add up to significant energy savings, which translates to money saved, and a decreased environmental impact.

Promoting greener businesses

A regular section in Apster will keep you up to date on Eco-APNIC activities, as well as showcasing environmental initiatives that other APNIC community members are taking. It will also feature tips on ways your organisation can be more eco-friendly. There will also be a presence on the APNIC website, and at events such as APNIC meetings.

- APNIC Open Policy Meetings will now provide an opportunity to recycle meeting paraphernalia, such as lanyards and paper documentation – look for recycling stations at the registration desk or APNIC Helpdesk.

Chris Buckridge

Resources

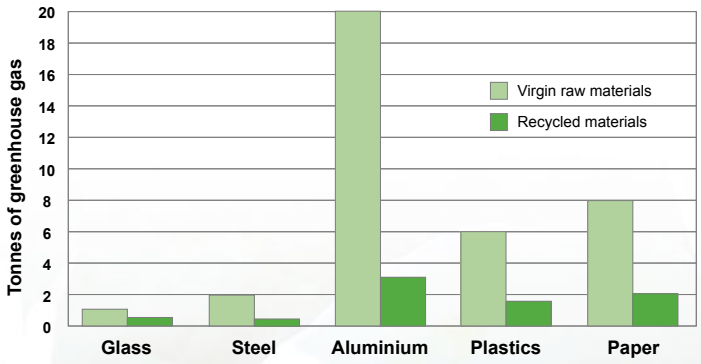
DOT-COM Activity: Asia & Near East Computer Recycling Study, October 2004

http://www.dot-com-alliance.org/activities/activitydetails.php?activity_id=97

http://www.conservatree.org

Green Office Guide

http://www.deh.gov.au/settlements/publications/government/purchasing/green-office-guide



▲ This graph shows how many tonnes of greenhouse gas are produced as a by-product of manufacturing one tonne of various products, starting from either raw or recycled materials. It demonstrates the impact that can be made by buying recycled products. Source: Green Office Guide

Things that your organisation can do for the environment!

And finally, here are just a few tips that you and your organisation might look at employing to reduce your "ecological footprint"!

Transportation

- Carpool
- Ride your bike or walk
- Investigate carbon offsetting programs

Around the office

- Print or copy on both sides of the paper
- Recycle office and computer paper, cardboard, etc.
- Buy recycled paper
- Use scrap paper for informal notes to yourself and others
- Recycle/refill printer cartridges
- Use compact fluorescent bulbs - they last up to 13 times longer than regular bulbs and use 75% less energy
- Reduce water waste
- Cut your vampire power! Turn off monitors and computers when not at your desk

For more tips, visit these websites:

http://environment.about.com/od/globalwarming/tp/globalwarmtips.htm

http://events.yahoo.com/earthday06

http://www.justgive.org/html/guide/50waysenvironment.html

http://www.everydayactivist.com/ways_to_help/2/at_work

http://www.climatecrisis.net

eco APNIC
This issue of *Apster* is printed on ONYX recycled paper.

Eco-APNIC by numbers

17 Number of trees saved by recycling a ton of paper	260 Number of kilograms of fossil fuels used in the manufacture of a single computer	70% Percentage of hazardous waste made up by electrical components
100 Number of centimetres the sea is predicted to rise this century due to global warming	3 Number of hours you could run a television for with the energy saved by recycling just one aluminium can	700 million Number of tonnes of CO_2 produced by commercial aviation annually

Current security practices by large ISPs:

Secure device management, secure software upgrade, and configuration integrity

▲ Security expert Merike Kaeo will deliver workshops on host and network security at APNIC 22.

Merike Kaeo is founder and chief network security architect of Double Shot Security. She is a recognised global expert in information security, was the lead member of Cisco's first security initiative in 1997, and is the author of **'Designing Network Security'**. Merike is a frequent speaker and instructor on security issues and solutions at conferences and ISP forums around the world including RSA, NANOG, RIPE, APRICOT, and SANOG. At APNIC 22, Merike will deliver workshops on host-based and network security. Here, she reviews the current approaches to security by large ISPs.

Introduction

While every network user and ISP is keenly aware that security measures must be used to protect the critical devices that make up their network infrastructures and the data traversing these networks, there always exists the trade-off between mitigating security risks and having operational efficiency. What are the security measures that make sense without causing too many operational headaches? This article discusses the security measures used to secure device management and software upgrade and configuration integrity, as revealed by a recent survey of the current security practices used by large ISPs (draft-ietf-opsec-current-practices-06.txt, 2006).

What are we protecting?

Invariably, the security goal is to protect electronic communication from malicious individuals and applications that are determined to spoof, corrupt, alter, or destroy the data or render critical services unavailable. Protection is required by every device that is participating in networked communication and all information that is either stored on a device, is in transit between communicating devices, or is processed by the devices. Security measures must incorporate mitigation techniques which decrease the risk of both deliberate attacks or unintentional events (such as a mis-configured device); the difference between an 'attack' and a 'mistake' is one of intent, and an effective security system should protect effectively against either.

What do we need to consider?

The mechanisms to provide the security measures can take many forms, but essentially all forms pertain to the preservation of confidentiality, integrity, accountability, and availability.

- **Confidentiality** is the property by which access to information is restricted to those who are privileged to see it. Examples of violations of confidentiality include bypassing access control rules or having the capability to read unauthorised information while it is in transit from sender to the recipient.
- **Integrity** can pertain to the data as well as the communicating parties. Data integrity is having trust that the information has not been altered during its transit from source to destination. Host/user integrity is having trust that the sender and/or recipient of the information is who it is supposed to be. Data integrity can be compromised when information has been corrupted – willfully or accidentally – before it is read by its intended recipient. Host/user integrity is compromised when an imposter 'spoofs' a sender's identity and supplies incorrect information to a recipient.
- **Accountability** is synonymous with non-repudiation, which refers to the property that you cannot deny having done something.
- **Availability** is the property that the information or resources are accessible when required within a reasonable period of time.

Usually, there exist a variety of technologies and/or device features which can be used to implement these security characteristics. The following services are primarily used to implement the properties of confidentiality, integrity, accountability, and availability:

- **Authentication** – the process of verifying the claimed identity of a device, user and/or application trying to access the resources.
- **Authorisation** – the rights and permissions granted to a user or application that enables them the access to network or computing resources.
- **Access control** – the means by which an authorised user has access to resources.
- **Encryption** – the mechanism by which information is kept confidential from unauthorised users.
- **Auditing** is the process that keeps track of what an authorised or unauthorised user or application is doing.

In many instances, a specific protocol will offer a combination of these services. While much attention is paid to filtering and network traffic auditing procedures, network devices and upgrades to software and configurations also require diligent security measures.

Secure device management

'In-band management' is generally considered to be device access where the control traffic takes the same data path as the data which traverses the network. 'Out-of-band (OOB) management' is generally considered to be device access where the control traffic takes a separate path to the data which traverses the network. In many environments, device management for layer 2 and layer 3 infrastructure devices is deployed as part of an out-of-band management infrastructure, although there are some instances where it is deployed in-band as well. Note that while many of the security concerns and practices are the same for OOB management and in-band management, most ISPs prefer an OOB management system since access to the devices which make up this management network are more vigilantly protected and considered to be less susceptible to malicious activity.

Controlling device access

Console access is always architected via an OOB network. The OOB management system is designed via a terminal server at each location and SSH is used to access the terminal servers to ensure encrypted communication. Dial-in access is deployed as a backup; however, it is common to use dial-back, encrypting modems, or one-time-password (OTP) modems to avoid the security weaknesses of plain dial-in access.

Other access mechanisms used for either in-band management or OOB management are via virtual terminal access (such as Telnet or SSH), SNMP, or HTTP. In all large ISPs that were interviewed, HTTP management is never used and is explicitly disabled.

Note that specific filters are often used to specify which IP addresses or subnets are allowed to communicate to the devices via Telnet, SSH, or SNMP.

Device access authentication

All access to layer 2 and layer 3 devices is authenticated. The user authentication and authorisation is typically controlled by a AAA server (such as RADIUS and/or TACACS+). Credentials used to determine the identity of the user vary from static username/password to one-time username/password scheme such as Secure-ID. Static username/passwords are expired after a specified period of time, usually 30 days. Every authenticated entity via AAA is an individual user for greater granularity of control. In some deployments, the AAA servers used for device management authentication/authorisation/accounting are on separate networks to provide a demarcation for any other authentication functions.

For backup purposes, there is often a single local database entry for authentication which is known to a very limited set of key personnel. It is usually the highest privilege level username/password combination, which in most cases is the same across all devices. This local device password is routinely regenerated once every 2-3 months and is also regenerated immediately after an employee who had access to that password leaves the company or is no longer authorised to have knowledge of that password.

Device access authorisation

Each individual user in the AAA database is configured with specific authorisation capability. Specific commands are either individually denied or permitted depending on the capability of the device to be accessed. Multiple privilege levels are deployed. Most individuals are authorised with basic authorisation to perform a minimal set of commands while a subset of individuals are authorised to perform more privileged commands. Securing the AAA server is imperative and access to the AAA server itself is strictly controlled. When an individual leaves the company, his/her AAA account is immediately deleted and the TACACS/RADIUS shared secret is reset for all devices.

Encrypted access

IPsec is considered too difficult to deploy and the common protocol to provide for confidential management access is SSH. There are exceptions for using SSH due to equipment limitations since SSH may not be supported on legacy equipment. In some cases changing the hostname of a device requires an SSH re-key event since the key is based on some combination of host name, MAC address, and time. Also, in the case where the SSH key is stored on a route processor card, a re-keying of SSH would be required whenever the route processor card needs to be swapped. Some providers feel that this operational impact exceeds the security necessary and instead use Telnet from trusted inside hosts (called 'jumphosts' or 'bastion hosts') to manage those devices. An individual would first SSH to the jumphost and then Telnet from the jumphost to the actual infrastructure device, fully understanding that any passwords will be sent in the clear between the jumphost and the device it is connecting to. All authentication and authorisation is still carried out using AAA servers.

In instances where Telnet access is used, the logs on the AAA servers are more verbose and more attention is paid to them to detect any abnormal behavior. The jumphosts themselves are carefully controlled machines and usually have limited access. Note that Telnet is **never** allowed to an infrastructure device except from specific jumphosts (for example, packet filters are used at the console server or infrastructure device to ensure that Telnet is only allowed from specific IP addresses).

SNMP management

If SNMP is used for management, it is for read queries only and restricted to specific hosts. If possible, the view is also restricted to only send the information that the management station needs rather than expose the entire configuration file with the read only SNMP community. The community strings are carefully chosen to be difficult to crack and there are procedures in place to change these community strings between 30-90 days. If systems support two SNMP community strings, the old string is replaced by first configuring a second newer community string and then migrating over from the currently used string to the newer one. Most large ISPs have multiple SNMP systems accessing their routers, so it takes more then one maintenance period to get all the strings fixed in all the right systems. SNMP RW is not used and is disabled by configuration.

In instances where SNMP is used, some legacy devices only support SNMPv1 which then requires the provider to mandate its use across all infrastructure devices for operational simplicity. SNMPv2 is primarily deployed since it is easier to set up than SNMPv3.

Device access auditing/logging

All device management access is audited and any violations trigger alarms which initiate automated email, pager, or telephone notifications. AAA servers keep track of the authenticated entity, as well as all the commands that were carried out on a specific device. Additionally, the device itself logs any access control violations (for example, if an SSH request comes in from an IP address which is not explicitly permitted, that event is logged so that the offending IP address can be tracked down and investigations made as to why it was trying to access a particular infrastructure device).

Secure software upgrade and configuration integrity

Software upgrades and configuration changes are usually performed as part of either in-band or OOB management functions. However, there are additional considerations to be taken into account which are enumerated in this section.

Controlling software and image access

Images and configurations are stored on specific hosts which have limited access. Filters are used to limit access to uploading/downloading configuration files and system images to specific IP addresses and protocols.

All access and activity relating to the hosts that are used to upload and download software images and/or configuration files are authenticated and logged via AAA services. When uploaded/downloading any system software or configuration files, either TFTP, FTP, or SCP can be used. Where possible, SCP is used to secure the data transfer and FTP is generally never used. All SCP access is username/password authenticated but since this requires an interactive shell, most ISPs will use shared key authentication to avoid the interactive shell. While TFTP access does not have any security measures, it is still widely used especially in OOB management scenarios. Some ISPs implement IP-based restriction on the TFTP server while some custom written TFTP servers will support MAC-based authentication. The MAC-based authentication is more common when using TFTP to bootstrap routers remotely using TFTP.

Integrity checking

In most environments scripts are used for maintaining the images and configurations of a large number of routers. To ensure the integrity of the configurations, every hour the configuration files are polled and compared to the previously polled version to find discrepancies. In at least one environment these tools are Kerberised to take advantage of automated authentication (not confidentiality). Rancid is one popular publicly available tool for detecting configuration and system changes.

P 10

The software images perform CRC-checks and the system binaries use the MD5 algorithm to validate integrity. In the survey, many ISPs expressed interest in having software image integrity validation based on the MD5 algorithm for enhanced security. Where the MD5 algorithm is not used to perform data integrity checking of software images and configuration files, ISPs have expressed an interest in having this functionality. IPsec is considered too cumbersome and operationally difficult to use for data integrity.

Dealing with passwords in configuration files

In all configuration files, most passwords are stored in an encrypted format. Note that the encryption techniques used in different products can vary and that some weaker encryption schemes may be subject to off-line dictionary attacks. This includes passwords for user authentication, MD5-authentication shared secrets, AAA server shared secrets, NTP shared secrets, and so on. For older software, which may not support this functionality, configuration files may contain some passwords in readable format. Most ISPs mitigate any risk of password compromise by either storing these configuration files without the password lines or by requiring authenticated and authorised access to the configuration files which are stored on protected OOB management devices.

Validating configurations

Automated security validation is performed on infrastructure devices using nmap and nessus to ensure valid configuration against many of the well-known attacks.

Summary

It is critical to ensure the security of all devices which make up the core ISP infrastructure. This requires adequate measures for authenticating and authorising device access and effectively auditing against any unauthorised access. Ensuring that software upgrades and configuration files have effective security measures is also important. However, these are only a subset of the operational functions that are needed to securely deploy and operate a network. For more information on current work that is being done in the IETF, refer to the operation security working group at:

http://www.ietf.org/html.charters/opsec-charter.html

Further reading

Kaeo, M. 'Operational Security Current Practices' (work in progress) July 2006

http://www3.ietf.org/internet-drafts/draft-ietf-opsec-current-practices-06.txt

ICANN contracted to perform IANA function until 2011

The United States Department of Commerce (DoC) has executed a new contract with ICANN. The five-year contract (with yearly options) means that ICANN retains the IANA function it has been contracted to perform since 1998.

The IANA function includes IP address space allocation, protocol identifier assignment, generic (gTLD) and country code Top-Level Domain (ccTLD) name system management, as well as root server system management functions.

On 21 February 2006, the DoC's National Telecommunications and Information Administration (NTIA) issued a Request for Information, inviting other organisations to provide evidence that they were qualified to perform the IANA function.

ICANN President and CEO, Dr Paul Twomey said "In executing this contract the Department of Commerce has confirmed that ICANN is uniquely positioned to perform this function."

The present contract expires on 30 September 2006, and the new contract will become effective on 1 October 2006.

A copy of the contract is available at:

http://www.icann.org/general/iana-contract-14aug06.pdf

More information about the NTIA's Request for Information:

http://www.ntia.doc.gov/ntiahome/press/2006/icanncontract_081406.htm

Daniel Karrenberg to Chair ISOC Board of Trustees

▲ RIPE NCC's Chief Scientist, Daniel Karrenberg

The RIPE NCC's Chief Scientist, Daniel Karrenberg, has been elected as the new Chair of the Internet Society's (ISOC's) Board of Trustees. Karrenberg was elected during ISOC's Annual General Meeting (AGM) which was held recently in Marrakesh, Morocco.

"The Internet Society has much to contribute to the continued success of the Internet," said Karrenberg.

"The diligent work of my predecessors, the Trustees, and the staff has put the society in a very sound position. Building on this foundation we will intensify our work in the areas of public policy and education. We will ensure that the IETF has the administrative support it needs to continue its exemplary standardisation work. We will continue to build a healthy network of chapters for local activities close to the Internet users. All this will help us to realise our motto 'The Internet is for Everyone'".

Karrenberg is a pioneer member of ISOC and has been actively involved with the development of many of the society's educational initiatives. He taught tutorials at early INET conferences, supported networking workshops, and has written ISOC member briefings about Internet operations and coordination. In 2001 he was awarded the Jon Postel service award in recognition of two decades of extraordinary dedication to the development of networking in Europe and around the world. A regular IETF participant since 1992, Daniel has co-authored several RFCs.

New staff

Finance Department

Alvin Goh, Senior Finance Officer

Alvin Goh joined the Finance team in August in the newly created role of Senior Finance Officer. Alvin holds a Bachelor of Commerce and is a Member of the Australia Institute of Management (AIMM), and he has worked in the past as an Accounts Manager with Majans Pty Ltd and Group Accountant with InterTax Holdings Pty Ltd. Alvin is fluent in Mandarin, Malay, Cantonese, Hokkien, and Teow Cheow. His responsibilities at APNIC will include supervising general accounts keeping, and assisting with the various accounts administration, reporting, and analysis functions of the Finance Department.

Deirdre Phayre, Accounts Officer

Deirdre Phayre joined the Finance team in August as an Accounts Officer. Her experience to date includes working as an accounts clerk and office administrator with a retail organisation. Her responsibilities at APNIC include general accounts keeping, billing related queries, and other administrative tasks within the Finance Department.

Resource Services Department

Anuttara (Annie) Tallents, Internet Resource Analyst

Anuttara Tallents joined APNIC as an Internet Resource Analyst, or Hostmaster, in August. Annie has a Bachelors degree in Computer Science, and has worked in IT, networking, and testing for the Queensland government. She is fluent in Thai. Annie's responsibilities at APNIC will include processing requests for IP address space and AS number allocations within the Asia Pacific region.

Training schedule

2006

September

4 - 8	Kaohsiung, Taiwan (In conjunction with APNIC 22)
27 - 29	Ulaan Baatar, Mongolia

October

2 - 3	Hong Kong

November

6 - 10	Bangkok, Thailand
13 - 17	Manila, Philippines
27 - 30	Kuala Lumpur, Malaysia

December

4 - 7	Singapore

The APNIC training schedule is provisional and subject to change. Please check the web site for regular updates at:

http://www.apnic.net/training

If your organisation is interested in sponsoring APNIC training sessions, please contact us at:

training@apnic.net

New-look ICONS site launched

Many readers will be familiar with APNIC's ICONS (Internet Community of Online Networking Specialists) web site. A new and improved version of this interactive site, which provides a forum for members to communicate about Internet and networking topics, was launched on 1 August.

Existing ICONS members provided APNIC with valuable feedback in recent months, leading to improvements in structure, navigation, and user features. To support these new features, ICONS has been upgraded from Mambo to the Joomla platform. Members can submit blog entries, user guides, tools and technical glossary terms, access a variety of news feeds, and find out about technical events in the Asia Pacific.

Membership is still free, and is open to anyone. We encourage all members of the Internet community to explore the new site.

Existing member details have been migrated over to the new site, but some content from the old site (such as the forum area) was not transferred. If you had posted to the forums in the past and you think that information would still be useful, then please feel free to upload it to the new site as a fresh blog entry.

For more information, visit:
http://www.icons.apnic.net

▲ The new-look ICONS web site was launched on 1 August, 2006.

Calendar

APNIC 22

4-8 September 2006
Kaohsiung, Taiwan
http://www.apnic.net/meetings/22/

U-connect

12-13 September 2006
Almaty, Kazakhstan

RIPE 53

2-6 October 2006
Amsterdam, Netherlands
http://ripe.net/ripe/meetings/ripe-53

ARIN XVIII/NANOG 38

8-13 October 2006
St. Louis, USA
http://arin.net/ARIN-XVIII/

First Internet Governance Forum meeting

30 October - 2 November 2006
Athens, Greece
http://www.igfgreece2006.gr/

67th IETF

5-10 November 2006
San Diego,, USA
http://www.ietf.org/meetings/67-IETF.html

ITU Plenipotentiary Conference

6-24 November 2006
Antalya, Turkey
http://www.itu.int/plenipotentiary/2006

Asia IPv6 Summit

7-8 November 2006
Makati, Philippines
http://www.asiaipv6.com/

CNNIC Open Policy Meeting

16-17 November 2006
Hangzhou, China
http://www.cnnic.net.cn/en/index

Asian Internet Engineering Conference (AINTEC) 2006

28-30 November 2006
Bangkok, Thailand
http://www.interlab.ait.ac.th/aintec06/

AfriNIC 5

31 November - 1 December 2006
Port Louis, Mauritius
http://www.afrinic.net/meeting/index.htm

ICANN meeting

2-8 December 2006
Sao Paulo, Brazil
http://www.icann.org/meetings/

Global IPv6 Summit in Australia

4-6 December 2006
Canberra, Australia
http://www.isoc-au.org.au/ipv6summit

ITU Telecom World 2006

4-8 December 2006
Hong Kong
http://www.itu.int/WORLD2006/

APRICOT 2007/APNIC 23

21 February - 2 March 2007
Bali, Indonesia
http://www.apnic.net/meetings/upcoming

How to contact APNIC

Street address	Level 1, 33 Park Road, Milton, Brisbane, QLD 4064, Australia
Postal address	PO Box 2131, Milton QLD 4064, Australia
Phone	+61-7-3858-3100
SIP	info@voip.apnic.net
Fax	+61-7-3858-3199
Web site	www.apnic.net
General enquiries	info@apnic.net
Hostmaster (filtered)	hostmaster@apnic.net
Helpdesk	helpdesk@apnic.net
Training	training@apnic.net
Webmaster	webmaster@apnic.net
Apster	apster@apnic.net

Member Services Helpdesk

The Member Services Helpdesk provides APNIC members and clients with direct access to APNIC Hostmasters.

www.apnic.net/helpdesk

helpdesk@voip.apnic.net

helpdesk@apnic.net

+61 7 3858 3188

Helpdesk Hours: 9:00 am to 7:00 pm (UTC + 10 hours) Monday - Friday

Communicate with APNIC via MyAPNIC

APNIC members can use MyAPNIC to:

- view APNIC resources held by their organisation
- monitor the amount of address space assigned to customers
- view current and past membership payments
- view current tickets open in the APNIC email ticketing system
- view staff attendance at APNIC training and meetings
- vote online

For more information on MyAPNIC's features, see:

www.apnic.net/services/myapnic

eco APNIC
This issue of *Apster* is printed on ONYX recycled paper.