

Issue 10 – June 2005

# News from .aero

the domain of aviation

[www.information.aero](http://www.information.aero)

## In this issue...

02



DNS security breach,  
a CNN headline?

06



.aero online directory

07



.aero moving forward  
in the IP world

08



Can airlines cut out  
the middleman?

## Welcome

A special welcome to the June 2005 edition of the newsletter that keeps you posted on developments at .aero – the world's first industry-specific top level domain, reserved exclusively for aviation.

We deal with some weighty issues in this edition – not least the role that .aero is playing in reducing the cost of travel, as well as the urgent issue of combatting potentially serious Internet attacks. A great many reports are constantly published that deal with the structure of the Internet, but we recommend the report that is being published by the Washington DC-based National Academies Research Council (see page 2). It's thorough, timely and reports the conclusions of an assessment of the current state and the future prospects of the domain name system (DNS) and its interactions with Internet navigation.

We introduce the .aero directory, although in its early development stage, we are sure you will agree with us that it will become a rather useful service from .aero. You can find more details about the directory and how to be listed at [www.information.aero](http://www.information.aero) – the only place to go for anything to do with the air transport community's own domain.

Lastly, we check out the new sponsored top level domains, including .travel. How does it compare in its aims with .aero? And are you blogging yet? Some 10 million people and companies are – and they may be talking about you...this is your newsletter, for your domain. Keep in touch and we hope you enjoy this edition.

sponsored by  
**SITA**

[.aero team, SITA](#)

# Should we wait for CNN headlines about DNS insecurity before taking action?

Most Internet users rely on the domain name system (DNS) and navigation to find the resources they seek or to attract users to the resources they provide.



The system has worked well for over two decades but a number of security and governance challenges need to be addressed if it is to meet future challenges from hackers and be capable of accommodating Internet growth, according to a new report to be published by the Washington DC-based National Academies Research Council\*. In this article, we have a closer look at some of the security challenges addressed in the report.

A number of recent attacks against DNS suggest that hackers are increasingly targeting the Internet infrastructure rather than individual services. These often serve as a precursor to other violations, such as security theft, installation of spyware or adware on unsuspecting PCs connected to the net etc. As an example, take the technique call pharming, which, although known for many years, only recently made its debut in the media. It will serve to illustrate the value of DNS security.

"Pairing that data with Webroot's findings that the average PC scanned with the company's software has 2.5 adware programs suggests that adware firms garner nearly US\$ 2bn in annual revenue, or about 20 per cent of the more traditional online advertising market."

Richard Stiennon – Vice President, Webroot Software

### Pharming works like this

The DNS is hierarchical. When a browser looks up a Web page, [www.sita.aero](http://www.sita.aero) for example, it needs the IP address associated with the URL. If the local server does not have up to date information, it will ask one of the Internet root servers for a pointer. This will be a name server which the root knows runs .aero. Then, one of the .aero servers will provide a pointer to servers which, .aero knows, run the 'sita.aero domain' and so on. Ultimately, the requestor will receive back an IP address corresponding to [www.sita.aero](http://www.sita.aero).

Anywhere along that path, you could be given misinformation by a badly configured system, or an intruder. As a result, traffic will be directed to a different site. This might mean a hacker can intercept and read your e-mail, Web browser requests, or any other Internet traffic that uses domain names to locate servers. For example, you could find yourself on a Web page that looks like the Web page of your bank, behaves just like the Web page of your bank and asks you for the same credentials information as your bank would but... it is actually a front put up by a hacker luring you to provide this information or trying to gain access to you computer.

Why would anyone attack you? Money is the primary motive, according to Richard Stiennon, vice president of threat research for Webroot Software, an anti-spyware software maker quoted in the online publication Channel Register.

"Data from adware firms indicate that each PC installed with the software accounts for about US\$ 2.40 in annual revenue", he said. "Pairing that data with Webroot's findings that the average PC scanned with the company's software has 2.5 adware programs suggests that adware firms garner nearly US\$ 2bn in annual revenue, or about 20 per cent of the more traditional online advertising market."

### How DNSSEC can solve the problem?

To some extent, this problem can be addressed today with the correct deployment of digital certificates. However, this will only address part of the problem and due to inefficiencies with this process, many users view certificate warnings as an annoyance and accept them as a matter of course.

To fight pharming and provide tools for the user to improve internet security in general, the NARC report calls for the wide deployment of a security protocol called DNS Security Extensions (DNSSEC).

DNSSEC digitally signs and verifies every DNS mapping using cryptographic keys. At each stage of the DNS lookup, the response can be authenticated using a cryptographic key. A DNS entry relating to 'name.aero' would be authenticated by the .aero servers, and the response from .aero servers would be authenticated by the root. The root would be authenticated using a public key. As a user, you would know that

the response you receive is complete and authentic. And you would know that the website you arrived at is the website you wanted.

It is important to consider what DNSSEC actually can accomplish. It will make certain attacks in the DNS visible. However, the user will always remain responsible for deciding what to do when this happens. It will raise significantly the level of protection against the falsification of DNS data and help in deterring identity-related theft and SPAM problems.

On the other hand, because DNSSEC introduces cryptographic material in the DNS and allows for the addition of other (non-DNS) keys, some interesting possibilities emerge. Many technologies on the Internet need some kind of simple key distribution mechanism in place, such as SSH and IPSec. What DNSSEC promises is a system in which we can validate a key from an unknown host with only one key. If the validation is successful, we can be quite certain that the host key comes from the host from which it claims to come. We get this without any extra effort or cost (from a client's perspective at least). The possibilities are probably endless and DNSSEC provides a basis to build trust on the Internet to support higher level protocols facilitating IP telephony and web services.

### When can we expect DNSSEC deployment ?

The DNSSEC deployment project is under way. Internet root server operators and a number of registries already have pilots in place and they are preparing the technology for implementation. Several governments are also interested in improving Internet security by provide funding and support for deployment projects.

For live deployment however, registries and registrars will have to balance the technical need with the actual market demand. Most of them need to satisfy commercial objectives set by their shareholders and there is no clear business model yet in place. For the consumer to enjoy the benefits, Web browser developers will also need to upgrade browsers.

Deployment will be gradual and slow, starting with the users and community that can benefit most. But as we know from similar events in the past, this slow

pace can all change in a matter of days as soon as there are CNN headline news reporting a major breach of DNS security.

While waiting for DNSSEC, as a user there is much you can do to protect yourself. After all, on the Internet, every user has a duty of care.

- For domain registrations, choose a registrar with a good track record. Keep your records up-to-date, to ensure that the registrar can actually contact you if necessary. Always remember to renew your domain.
- Stay on top of all security upgrades and patches be, it for an individual PC or the entire enterprise infrastructure.
- Think carefully before deciding to ignore 'certificate warnings' displayed by your browser. They may be flagged simply as a result of the system's inefficiencies (for example, if your Web browser does not have the certificate of the issuer installed) but they may well indicate a bigger problem.

The NARC Report (still in pre-publication form as this newsletter went to press) will make a helpful contribution to a debate whose time is now. So let them have the last word: "While the introduction of DNSSEC imposes significant costs and does not eliminate all Internet Security concerns nor address all Internet Threats, its implementation would represent considerable progress in improving the security of the DNS."

### Resources

*"Signposts in Cyberspace: The Domain Name System and Internet Navigation"* published by the National Academies Press, 2005. See [www7.nationalacademies.org/cstb/pub\\_dns.html](http://www7.nationalacademies.org/cstb/pub_dns.html).

*"DNS attacks attempt to mislead consumers"* from Channel Register 8 April 2005. See [http://www.channelregister.co.uk/2005/04/08/dns\\_attacks\\_attempt\\_to\\_mislead\\_consumers](http://www.channelregister.co.uk/2005/04/08/dns_attacks_attempt_to_mislead_consumers).

For general technical reading about the DNSSEC programme, see <http://dnssec.net>.

"While the introduction of DNSSEC imposes significant costs and does not eliminate all Internet Security concerns nor address all Internet threats, its implementation would represent considerable progress in improving the security of the DNS."



# Sponsored TLDs boost the Internet

Last year ICANN, the global Internet coordination body, initiated a process of selection of additional sponsored Top level Domains (sTLD) and recently announced signed agreements for .travel and .jobs to go alongside .aero, .museum and .coop.



Another three from the original eleven applications have already been selected and are preparing their agreements with ICANN: .mobi, .post and .cat. Still being evaluated are five more possible sponsored domains, – including .asia, .mail, .xxx, and two separate proposals to develop .tel.

## What does this mean for .aero?

This is good news. More sponsored TLDs on the Internet means more choice and a greater awareness of top level domains other than .com. It should also inspire more innovation, since each TLD will have its own distinct objectives and clearly defined community to serve.

It is perhaps worth looking in more detail at the .travel domain. Following an initial and unsuccessful application by IATA in 2000, the initiative was passed to the Tralliance Corporation, now designated by ICANN as the registry for the .travel top level domain. It is intended as the online community for a broadly defined travel and tourism industry – including travel agents, tour operators, hotels, car rental companies cruise lines, airlines, bus companies, ferries, rail lines, theme parks, convention bureaus, and national tourism offices.

The focus of .aero, on the other hand, is firmly concentrated on delivering TLD benefits exclusively to the aviation community. The initiative is creating a structured, open and constantly evolving Internet naming architecture to help the community integrate systems and services, and streamline communications. The .aero domain is the uniting factor that addresses the key issues of technology development that impact on e-commerce and Internet security, all on a not-for-profit basis.

Similarities do and should exist between sponsored domains and their goals. The community they both address is defined and segmented with little or no overlap. Companies will be drawn to register their domain name in the Internet space most relevant to their business focus – or according to the different services the domain operator can provide. Above all, companies will register their business entities in the most appropriate space that will match buyers to sellers. The rise in sponsored domains unclutters the Internet space, for the benefit of all.

- .travel – the domain is intended as the online community for the travel and tourism industry
- .jobs – a space devoted to posting and recruiting job opportunities
- .post – for post offices, sponsored by the Universal Postal Union
- .mobi – sponsored by the mobile phone industry
- .cat – for the Catalan language community

# .aero online directory – undevelopment

With the launch of the new .aero website, we've included a new service into the site that will enhance the visibility of the aviation community on the Internet.

The .aero domain offers every registrant with an active .aero website a listing in the complementary .aero directory\*. Companies and organizations that register in the directory will all be found in one location, creating a large and comprehensive network of aviation business.

Today, the directory is segmented by industry focus and alphabetically. It features key products and services, contact details and a link to registered domains' home pages.

## Submit your listing today

In the future, as we develop the directory services, users should be able to search from a detailed listing of categories covering all facets of the aviation community.



The .aero directory will become a global online source of aviation products and services. With further development planned, it will allow users to search from a number of categories to locate precise and detailed information about aviation services and products more efficiently. It will also encourage users to confidently contact and conduct business with other .aero domain name holders they may not know.

## Submit your listing today

If you are a registered .aero domain and are not listed in the directory – then visit .aero's information website, click on 'Directory' and submit your details, using the online form.

\* A free-of-charge service from .aero, open to revision.

# .aero moving forward in the IP world

Traditionally the air transport community has had rigid standards for inter-system communications pinned to the underlying centralized network. However with advent of IP communications over the Internet fast becoming the de facto standards for business to business transactions and as the community begins to embrace this new technology, the absence of well defined standards restricts the flexibility and scalability of the solution.

Many air transport companies, airlines and airports are having to establish bilateral or multilateral mechanisms to connect their systems over IP networks and increasingly rely on a small number of hubs to gateway between their systems. The end result being a different number of solutions to the same problem but each achieved independently.

Work is being carried out in .aero to develop a framework for intra-industry communications using DNS as means to simplify addressing in IP network environment. Airlines in particular will benefit from this work, for examples while most airlines have moved to an IP, some still rely on legacy networks. From a community perspective, development or standardization of messaging formats, naming schemes or communication mechanisms taking advantage of the Internet should also provide for transition from and translation to legacy messaging.

At the same time, this level of future planning should avoid the expensive 'two transitions' trap of simply migrating old formats and ways of doing things to the new environment, only to be faced



with a later redesign to take advantage of the other special properties and strengths of the Internet.

.aero's approach to the deployment of this new technology and its related standards will not only help close the technology gap that exists in some areas between small and big airlines and airports – to the benefit of the community as a whole by reducing implementation costs and enhancing operational effectiveness.

# Can airlines cut out the middleman?

It costs the average airline as much as US\$ 12.75 per ticket in distribution fees to use the global distribution systems. In the days of the Internet, when everyone can access any information at the other side of globe in a matter of seconds, why do airlines need a middleman? Or do they?

This article is a vision into the near-future, showing how airlines can remove the middleman and, by using open common standards, create an Internet environment open to all elements of the distribution chain, with the help of .aero. It is up to the airlines and the air transport community at large to decide how far they want to take this vision.

## What do airlines need?

Low cost. At times of rising oil prices and increased competition, no-one wants to fund excessive spending anywhere, including on information technology.

Flexibility and scalability. A solution which on a small scale may bring immediate incremental cost savings may prove to be very costly when deployed on a large scale for lack of planning at the requisite scale in the first place. This is an abiding issue with deployment of 1-1 connections.

Happier customers and opportunities to provide better services. This is the most important element in the equation. In the rush to drive down costs, the air transport industry must not forget that service and accessibility of service is central to delivering to the customer.

One of the principles often cited in relation to networks, Metcalfe's Law, states that the usefulness, or utility, of a network equals the square of the number of users.



**So what role can the Internet play in driving out cost?**

Airlines increasingly recognize that adding new systems onto the existing communications infrastructure, or patching new business partner connections individually, is of restricted value. It may be effective at the outset, but the scalability of such solutions and their flexibility in accommodating changes in business relationships or the technologies used is limited.

From an individual airline's perspective, the approach to minimize such risk lies in engaging an experienced network design professional (in house or on a consultancy basis) who will ensure that, as far as this airline can go, the connectivity solutions the airline deploys will stand the test of time.

One of the principles often cited in relation to networks, Metcalfe's Law, states that the usefulness, or utility, of a network equals the square of the number of users. For example, the telephone is of no use by itself. It is of very limited use if only you and your best friend have one. If a whole town is on the system, it becomes more useful, and if every person in the world can be reached, the benefits are enormous. In the same manner, and from a community perspective, a low cost secure connection to a couple of your key business partners is important – but an individual connection through to each of your business partners will deliver far greater value.



**Only connect – it's simple?**

This is where open standards and naming conventions become critical. It is of little value having a 'connection' to a network if you do not know how to find your business partners, if you do not have the right protocol to allow you to communicate with them or if you cannot authenticate them, without having to reach individual agreement on each issue with each individual partner. This is exactly where the .aero initiative comes in. Ongoing development work is creating a deterministic framework for locating services and applications within the air transport community without the need for restrictive coding of IP addresses.

The DNS can serve as a useful convergence tool and a platform to store various industry identifiers, as well as their relationship to underlying systems.

## Special feature continued...

If you know who you want to talk to and what you want to do, you need to be able to determine what system to talk to and where in the IP world it is located. You also need to know the protocol required so that can the system talk to you, and last but not least how to obtain the correct certification in order to validate the authenticity of the information you are being proffered.

All of this can be obtained by using the DNS as a locator service, as a means of agreeing on communication and authentication standards. Some of them will relate specifically to the DNS but the scope must be wider. However, the DNS can serve as a useful convergence tool and a platform to store various industry identifiers, we well as their relationship to underlying systems.

For example, a single domain name corresponding to a ticket number (PNR), could be used by travel agent's application to identify a database of the validating carrier, confirm the ticket or modify the route. Similarly, RFID tags are becoming identifiers mapped to domain names to facilitate location of business applications that know the identity of the transactions related to the tag. By using the domain name/PNR, a passenger could make a phone call to check in, or send an e-mail to obtain the status of an associated flight. All in a matter of seconds.

### Applying the lessons

What does it mean for the middleman? The travel agent's application can look up the airline's own system and conduct all transactions without having to pass through a middleman. The middleman

is only needed if he provides some genuine value in the chain. He is – and should be – under constant pressure to prove that the service is needed. For example, there may be a need for transaction mediation – providing independent confirmation that a transaction has taken place or facilitating authentication of business partners, But there is no longer a need to store data with a middleman.

This is extremely important – the ability to change and scale up and down provides flexibility to the system participant. With flexibility comes the ability to adjust quickly to changing market conditions.

Examples from other industries show that the technology we use to set our location service is already used for similar purpose in other industries. Indications are that they will impact air transport anyway.

There is another crucial point. The telecommunications industry is beginning to transition the management of phone numbers to the Internet. In the framework of an initiative called 'enum' (see our last issue for details), telephone numbers, expressed as domain names, are becoming just another set of identifiers on the Net in the same way as VoIP telephone is 'just' another Internet application. Soon you will be able to decide how you wish to be reached on your phone number – including the ability to simply redirect your voice mail to your e-mail box as an attachment.



The ability to change and scale up and down provides flexibility to the system participant. With flexibility comes the ability to adjust quickly to changing market conditions.

### Secure all round

The Internet coordination body ICANN is moving steadily toward securing the root of the Internet, to support the expansion of the use of this key infrastructure element. Future opportunities are probably endless!

The Dot Aero Council recently received a report concerning the development of the .aero domain. It recommended the development of naming spaces for business applications and agreed that .aero must systemically prepare for deployment of the security blanket provided by DNSSEC.

With increased sophistication of online technologies, the air transport community is accelerating its move to Internet-based applications. While the migration of industry systems to Internet-style services seems inevitable, there is a real risk from the "two transitions" trap of simply migrating old formats and ways of doing things to the new environment, only to be faced with a later redesign to take advantage of the other special properties and strengths of the new environment.

The .aero initiative's aim is help industry avoid this trap by systemically pointing out new possibilities, demonstrating the advantages that are available to the industry, and facilitating adoption of the requisite standards. The end result will be of concern not only to the middleman, but also to travellers everywhere.

## DNSSEC – status update...

Perhaps the most extraordinary achievement of the founders of the Internet was the way they created a system that incontestably works.

The extent of that achievement is self-evident every time we use e-mail or communicate via the Web. Perhaps perversely, the success of the 'founding fathers' of the Internet can also be judged by noting the time it has taken to create DNSSEC – a set of security extensions to DNS, which provide: (a) origin authentication of DNS data, (b) data integrity, and (c) authenticated denial of existence.

Seven years after the domain name system (DNS\*) was invented, a security flaw was discovered. Five years later in 1995, research work on the flaw was made public when it became a topic within the Internet Engineering Task Force (IETF). This is a the loosely self-organized group of people who contribute to the engineering and evolution of Internet technologies. The IETF is the principal body engaged in the development of new Internet standard specifications. It is unusual in that it exists as a collection of happenings, but is not a corporation and has no board of directors, no members, and no dues.

The DNSSEC protocol, which addresses the security flaw, was finally approved by the IETF's steering group in October 2004 and as we go to print is still awaiting final publication. In February 2005, a roadmap for the introduction of DNSSEC was published, based on the experience of early adopters. This road map describes the basic goal for deployment; the current state of practice, gaps and barriers; a set of sequences and dependencies; and next steps.

Progress has been slow but real, including two pilot projects at two major registry operators, as well as education and training, including materials, curriculum and workshops. Clearly the issues are massively complex. But they also demonstrate the essential strengths of the Internet – simplicity, scalability and openness.

\*DNS is the Internet protocol that translates host names, such as www.aci.aero, into IP addresses, such as 195.74.129.66 – see dot aero newsletter Issue 8 October 2004.

### Are you blogging yet?

Remember the early days of the Internet, when month by month, the number of those online was a source of constant wonderment? Something similar is happening with the blogosphere, the space on the Internet occupied by online journals. So popular have they become that even the vice-chairman of General Motors has his own – and it's opening up new questions about the difference between editorial and advertising.

First, a definition. Wikipedia (the free-content encyclopedia) defines a blog "as a web application which contains periodic time-stamped posts on a common webpage... Blogs run from individual diaries to arms of political campaigns, media programs and corporations, and from the writing of one occasional author to the collaboration of a large community of writers. Many weblogs

enable visitors to leave public comments, which can lead to a community of readers centered around the blog; others are non-interactive."

In March 2003, according to Technorati, the real-time search engine that keeps track of what is going on in the blogosphere, there were 100,000 blogs. As this newsletter was going to press, that number had increased to almost 10 million – almost double the number at the end of 2004!

The mainstream media are getting variously excited, concerned or cynical about the growth and relevance of blogs. Business Week magazine led their 2 May edition with the headline "Blogs will change your business", but a week later Tom Zeller in the New York Times responded with an article headlined "A blogging revolution? Give me a break!"

As ever with the World Wide Web, it can be difficult to sort the wheat from the chaff. The best blogs are informative and engaging, allowing people to expand their own web of understanding, more akin to the original aims of the Web. Whatever the pundits think, blogging is now a massive fact of life – and companies need to be aware of it, not least when it can be used by customers and staff to voice grievances.

#### Resources

Business Week:

[www.businessweek.com/magazine/content/05\\_18/b3931001\\_mz001.htm](http://www.businessweek.com/magazine/content/05_18/b3931001_mz001.htm)

New York Times:

[www.ihf.com/articles/2005/05/08/business/blogs.php](http://www.ihf.com/articles/2005/05/08/business/blogs.php)

What's happening in the blogosphere:

[www.technorati.com](http://www.technorati.com)



### Industry events

#### NBAA 58th Annual Meeting & Convention 15-17 November 2005 – New Orleans, United States

The organizers describe this as the business aviation industry's largest and most efficient annual gathering of buyers and sellers. It is sometimes the only yearly opportunity to do direct, side-by-side comparisons of nearly every product and service available to company flight departments. For more information visit: <http://web.nbaa.org/public/cs/amc>.

#### Airport Council International World/Pacific Assemblies Conference & Exhibition 2005 6-9 November 2005 – Auckland, New Zealand

The 15th ACI World & Pacific events will join together for the annual conference in Auckland, hosted by Auckland International Airport in the largest city in New Zealand. For more information visit the dedicated ACI World Conference website, where online registration, the conference programme and all other relevant information is available. For more information, visit [www.airports.org](http://www.airports.org).

If you are a member of an aviation association and have an event you would like posted on the .aero events page, then please send the details to [www.aero.enquiries@sita.aero](mailto:www.aero.enquiries@sita.aero).

Online information and late breaking news are available at [www.information.aero](http://www.information.aero)  
e-mail enquiries to [aero.enquiries@sita.aero](mailto:aero.enquiries@sita.aero)

This newsletter is issued by SITA, the Sponsor of the .aero Top Level Domain. SITA also operates the official .aero web site [www.information.aero](http://www.information.aero) – providing information about domain registrations, policies and procedures and new developments in the .aero domain.

If you would like to comment on any of the articles in this issue or you would like more information, please contact our editor, Paola Piacentini, at [aero.enquiries@sita.aero](mailto:aero.enquiries@sita.aero)

#### News from.aero – the domain of aviation

For further information, please contact SITA:

##### Global Headquarters

26 Chemin de Joinville, B.P. 31, 1216 Cointrin,  
Geneva, Switzerland  
tel: +41 22 747 6000 fax: +41 22 747 6133  
e-mail: [aero.enquiries@sita.aero](mailto:aero.enquiries@sita.aero)

Design: Amarat Vekaria

Publisher: Marie Zitkova

Web Publisher: Paola Piacentini

Managing Editor: Paola Piacentini

Editorial: Gerald Oliver

Production Editor: Amber Harrison

Information is subject to change without notice.  
All trademarks acknowledged. © SITA 2005