Backgrounder

Questions & Answers

What is DNS? Humans prefer locating Internet servers using easy-to-remember names (such as www.pch.net), but behind the scenes the Domain Name System, or DNS, acts as a “phone book” for the Internet, matching each name to a unique numeric address that computers can use to find the server the user was trying to reach, in much the same way that a street address or telephone number allow a person to be located in the postal or telephone systems.

What is DNSSEC? DNSSEC (DNS Security Extensions) is a set of protocols that are currently being deployed to secure the DNS. DNSSEC adds security to the DNS by incorporating public key cryptography into the DNS hierarchy, resulting in a single, open, global Public Key Infrastructure (PKI) for domain names. It is the result of over a decade of community-based, open-standards development.

Why DNSSEC now? Since the signing of the DNS root servers, the top of the Internet’s addressing structure, in June, 2010, DNSSEC is gradually being adopted by both generic top-level domains (gTLDs) and country-code top-level domains (ccTLDs) to form a continuous, secured chain of trust within the DNS. Many ccTLDs and gTLDs have secured their own domains (70 at present) by generating their own cryptographic keys, which are used sign and authenticate their domains on the Internet. It is unreasonable or financially impractical for many ccTLDs to establish and maintain their own secure key signing facilities. The Singapore facility is part of a service offered at no cost by PCH to administrators of such ccTLDs to make their domains DNSSEC compliant.

To the broader question of why DNSSEC is important now after over a decade of development in the IETF, the answer lies in not only the ever increasing attacks on the Internet combined with our global reliance on the Internet but the demonstration by Dan Kaminsky in 2008 of improved attacks which could be used to redirect users en masse to rogue sites. This discovery made clear the need to solve the cache poisoning problem in short order with the accelerated deployment of DNSSEC.

How does DNSSEC improve Internet security?
DNSSEC was developed to prevent hacking and cyber-attacks that utilize forged DNS information to misdirect people to fake websites. This is commonly done in “phishing” and other kinds of attacks that involve identity theft and theft of online banking credentials, and sophisticated espionage and cyber-warfare attacks against nation-states are also possible.

Over the past fifteen years**,** the function of securing and authenticating Internet identities has been handled by certificate authorities (CAs), which issue certificates for individual machines that attest to the authenticity of their ownership. Under this system, CAs can issue certificates for any machine in any domain, so the trustworthiness of this certificate is only as good as the CA that issued it. Some CAs and types of certificates, such as Extended Validation Certificates, have thus far appeared reliable. But other CAs have been compromised and are no longer secure. Unfortunately, there is no way in the CA system for end users to distinguish which CA they are relying on.

Unlike the CA system, a DNSSEC signed top-level domain allows the owners and operators of zones within that domain (the addresses for specific websites) to also authenticate themselves as the true owners of their own domains and the hosts within them, as vouched for by the top-level domain administrators. The extension of DNSSEC to top-level domains makes possible a unified authentication and privacy mechanism that is based on the hierarchy of the DNS. This system allows anyone to secure their own domain and its online contents, without relying upon an ever-growing collection of compromised third-party CAs.

How does this impact third-party certificate authorities? As the standards for authenticating websites are improved, organizations that issue traditional X.509 certificates will have smaller roles. This will certainly have a negative business impact on some large organizations that benefit from the current system, but the new standard is of great benefit to users, online businesses, and the Internet as a whole.

What does PCH add to the DNSSEC program? Because the Internet is universal, a weak link anywhere in the net threatens everyone. Criminals can falsify domain information and create fake websites from anywhere, and the traps they lay can reach end users anywhere. Countries with a long history of Internet participation and infrastructure building tend to also have well-developed regulatory oversight and cyber-crime laws. Many of these same countries also have the financial strength to secure their own ccTLDs and deploy DNSSEC, as 70 have already done. On the other hand, countries with developing economies and nascent regulatory environments are easier to exploit by cyber-criminals. Some of these states have not yet adopted the Council of Europe Convention on Cybercrime and therefore have limited ability to apprehend and successfully prosecute online criminals. Many of these same states have pressing society-building problems that take up their limited financial resources. They have neither the resources nor the public demand to build and maintain a facility such as this new one in Singapore.

In this state of imbalance among countries, the wealthier states tend to secure their own ccTLDs with their own facilities, while the less able countries cannot and do not. Cyber-criminals will naturally migrate to and set up in the unsecured countries, where they have less to fear from prosecution. Thus, the problem simply moves from one location to another—and from there it can still reach the whole Internet world.

The PCH DNSSEC service being inaugurated in Singpore counters this imbalance by offering countries an alternative to securing their own domains from their own resources. Through funding from more developed countries, along with the generous hosting services of Singapore, this PCH service secures the participating countries' TLDs at no cost to those countries. Prioritizing DNSSEC deployment for the ccTLDs of these states will effectively force perpetrators of online crimes into countries where cyber-crime legislation is more thoroughly developed and criminals are more likely to be convicted—or else it will force these criminals out of business altogether. The benefit is to Internet users everywhere.

Why Singapore? Singapore's stability and commitment to political neutrality have been demonstrated over the course of several decades, demonstrating its reliability as a host able to provide high security to the project. One of the four Asian Tigers, it is the world's fourth leading financial center and has a strong governmental interest in advancing the development of the Internet and ICT for business. A founding member of ASEAN and host of the APEC Secretariat, Singapore is experienced in the diplomatic interchanges needed to bring other countries into the DNSSEC program.

What are the details of the project facilities?
The exact locations of the facilities will not be disclosed to the public as part of their security. The Singapore facility is hosted by the National University of Singapore, on behalf of the Singaporean Infocomm Development Agency (IDA). The Swiss facility is hosted in Zurich by SWITCH, the Swiss national research and education network. The U.S. facility is hosted by Equinix in San Jose.

Each facility is highly protected against natural disasters and intrusion. Each facility utilizes "defense in depth" and "layered defense." Each defensive layer is progressively more difficult to penetrate than the last. The datacenter itself is the outside layer. Within each facility is a room that has been hardened against intrusion and made tamper-evident by such features as expanded steel mesh in the walls and wire mesh in the windows. The security of the datacenter and the approach to this room are the responsibility of the datacenter operator (NUS, for the Singapore facility). Responsibility for access to the room rests with PCH's Security Controllers. Within each room there is a Sensitive Compartmented Information Facility (SCIF), which requires two of the three Security Controllers to open. The SCIF uses Videx CyberLocks. The SCIF contains an IPS safe, which has a Kaba-Maas combination lock. The IPS contains a hardware-signing module, an AEP Keyper.

http://en.wikipedia.org/wiki/Defense_in_depth_(computing)
http://en.wikipedia.org/wiki/Layered_security
http://www.nsa.gov/ia/_files/support/defenseindepth.pdf
http://www.videx.com/CyberLock/CyberLock_Overview.html

Each of these layers is certified to the highest available standard, the same standards applied by ICANN to protect the root of the DNS.

All components of the system were selected to have a low power draw, and the system as a whole is being designed to be both energy-neutral and carbon-neutral, through tree planting and solar power generation.

What is the size and cost of each facility? The three facilities are identically constructed; each is 2m x 3m in size, and each costs less than USD $1M to construct. The net present value of the donated facilities is about USD $55M, and the operational costs of the system are about USD $2M per year.

How does DNSSEC deployment affect regular Internet end users? Although DNSSEC makes the Internet far more secure, it will be some time before its effects are seen by all Internet users. However, the implications of DNSSEC deployment for the Internet as a whole can already be seen. Internet browsers already integrate the client side of the DNSSEC protocol, validating domain signatures to allow users to see if a site they visit is authentic. As more top-level domains implement DNSSEC, sites that cannot show the same chain of authentication will be inherently less trustworthy and fade from use. The adoption and promotion of DNSSEC by operators of the Internet's core infrastructure, like top-level domains, will eventually make the secure and authenticated domains a fundamental feature of the Internet.

Why is PCH employing U.S. standards for physical security? Although PCH is an international organization, and this service is fundamentally international in nature, PCH is also following ICANN's lead in replicating the security processes, mechanisms, and standards employed in securing the root of the DNS. ICANN is overseen by the National Telecommunications and Information Administration (NTIA), an agency of the U.S. Department of Commerce. As part of ICANN's responsibility to NTIA, ICANN implemented U.S. government recognized standards for physical security, and PCH has therefore followed the same standards, notably:

- Federal Information Processing Standards 140-2, Level 4 Hardware Security Module
- Government Services Administration AA-C-2867, Class 5 Information Processing Systems Container
- Director of Central Intelligence Directive 6/9, Physical Security Standards for Sensitive Compartmented Information Facilities
- Telecommunications Industry Association Standard 942, Tier 4 Data Center

Each of these is the highest or most stringent specification in its class.

PCH deviates from ICANN's model only by diversifying the locations of the secure sites. ICANN signs the root at two locations both within the United States. PCH signs country-code domains in three different countries: Singapore, Switzerland, and the United States, and compares the result of every signature across the three sites to ensure consistency and validity. This improves the political and legal security of the system without compromising the physical and process security, which remain identical to that of the root of the DNS. By maintaining the same set of security standards as the root, we relieve national domain registries' auditors of the burden of understanding and evaluating needless multiple regimes and begin to establish a set of commonly agreed upon best practices.

Additional Resources

The hosts of this event are available to answer any questions leading up to the press event on June 22, as well as afterwards. We are also open to questions submitted in advance for more detailed responses during the event, particularly if you'd like us to prepare additional resources like photographs or diagrams.

Subject-Matter Experts:

A number of subject-matter experts have agreed to make themselves available for direct contact by members of the press:

Rick Lamb, DNSSEC Program Manager, ICANN
richard.lamb@icann.org, +1 310 301 3891
Rick is the DNSSEC expert who designed the signing systems used by ICANN for the root of the DNS, and by PCH for the country-code Top Level Domains.

Marcel Schneider, Manager of Special Operations, SWITCH
marcel.schneider@switch.ch, +41 44 253 98 07
Marcel is hosting the DNSSEC facility under construction in Zurich, one of the two counterparts to the Singapore facility that was announced today. SWITCH is also the administrator of the .ch and .li ccTLDs for Switzerland and Liechtenstein, both of which are DNSSEC-protected.

Patrik Fältström, Senior Consulting Engineer, Cisco Systems
paf@cisco.com, +46 706059051
Patrik is Cisco Systems' authority on DNSSEC, and is the author of a number of pieces of DNSSEC software. He is an independent authority, without any connection to PCH or any of the other sponsoring organizations.

Olaf Kolkman, Director, NLNet Labs
olaf@NLnetLabs.nl
Olaf runs the Dutch government's networking research labs, which publish of one of the two commonly-used pieces of DNSSEC server software, and Olaf recently retired from chairing the Internet Architecture Board, which oversaw development of the DNSSEC standard under his watch. He is an independent authority, without any connection to PCH or any of the other sponsoring organizations.

Stephan Somogyi, Crypto Officer
somogyi@gyroscope.net, +1 415 666 3270
Stephan is one of the seven holders of the cryptographic keys that enable the DNSSEC key-generation process, and is a respected independent cryptographic security consultant.

Steve Feldman, Crypto Officer
feldman@twincreeks.net, +1 925 997 2379
Steve is one of the seven holders of the cryptographic keys that enable the DNSSEC key-generation process, and is the chairman of the board of PCH, as well as the chairman of the board of NANOG, the North American Network Operators Group.

Links:

Wikipedia article on DNSSEC: http://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions

The IETF DNSSEC protocol definitions: http://www.ietf.org/rfc/rfc4033.txt, http://www.ietf.org/rfc/rfc4034.txt, http://www.ietf.org/rfc/rfc4035.txt

The IETF DANE working group: http://tools.ietf.org/wg/dane

Bio Statements

Bill WOODCOCK, Research Director, PCH

Bill Woodcock has operated international Internet service provision and content delivery networks since 1989 and currently divides his time between building Internet exchanges in developing countries and researching efficiency and stability in the operations of critical Internet infrastructure. In addition to PCH, he serves on the boards of directors of the American Registry for Internet Numbers, the Internet Capacity Development Consortium, the Technology Policy Institute, and several for-profit ventures in the communications and information security sectors. He has also served on the program committees of NANOG, APRICOT, SANOG, and PAM and has published a book and numerous articles in networking publications.

Rick LAMB, DNSSEC Program Manager, ICANN

Rick Lamb has over 25 years of Internet experience as engineer, entrepreneur, and policy expert. Currently responsible for DNSSEC efforts at ICANN, he was the technical and policy architect for ICANN's root DNSSEC deployment and is a driving force behind DNSSEC's deployment as a cross-organizational, transnational platform for Internet security innovation and opportunity. Previously he was Director of Global IT Policy at the U.S. Department of State, where he worked to bridge technology and policy across a wide range of agencies and issues. Before this he founded a number of networking startups, the last being acquired by Microsoft. His years in the networking field have included implementation and commercialization of a wide range of communication protocols (UUCP, MEP2, BiSYNC, SDLC, X.25, DECNET, Q.921/931, H.323, IPX, TCP/IP). Rick received a Ph.D. from MIT in 1987.

Kim DAVIES, ccTLD Liaison, ICANN

Kim Davies is IANA Technical Liaison at ICANN, where his primary responsibilities are management of the DNS root zone and other aspects of IANA's work related to domain names. He was previously Technical Policy Advisor to CENTR, the Council of European National TLD Registries. His role on the CENTR secretariat, and his representation of European country code managers in international fora, brought additional knowledge and expertise to ICANN as ICANN continues to strengthen its service to IANA customers, particularly TLD managers. Prior to his appointment at CENTR, Kim held appointments concerned with domain and ISP management, including as Head of Web Services for iiNet, an Internet access company. He was also on the board of the .au domain manager auDA from its founding through to 2005 and was responsible for commissioning and operating a key Australian Internet exchange point. Kim was also the principal of Cynosure Innovation, an Internet consulting business.

Steve FELDMAN, Chairman of the Board of Directors, PCH

Steve Feldman is a network engineer for CNET Networks. He has been involved in computer networking since 1978, providing software development and network engineering for Tymnet and MFS/Worldcom, where he was the principal architect for the MAE Internet exchanges, working on several startups, and acting as an independent consultant. Steve received B.S. and M.S. degrees in computer science from the University of California at Berkeley. He has chaired the NANOG Program Committee since February 2005.

Jonny MARTIN, Internet Analyst, PCH

Jonny Martin, an Internet Analyst at Packet Clearing House, is responsible for INOC-DBA operations and technical development and supports the day-to-day operations of the PCH anycast DNS network. He has previously held senior network engineering roles with national service and critical infrastructure providers in New Zealand. Besides PCH, he serves as a Councillor for Internet New Zealand, on the board of directors for the Asia and Pacific Internet Association, and on the program and organizing committees of NZNOG and APRICOT.

Michael SINATRA, Network Engineer, Energy Sciences Network

Michael Sinatra's mission with ESnet's Network Engineering Group is to help the transition to IPv6, work on ESnet's DNS and DNSSEC extensions, as well as perform general network engineering duties. For the past eleven years he has been working as principal network engineer at the University of California, Berkeley. He has held a variety of technical jobs, in 1999 joining the UC Berkeley central campus networking department, where he was appointed to the Security Working Group. He developed IPv6 and DNSSEC services at UC Berkeley, which have attracted national attention to the university for its pioneering efforts in this area. Sinatra has lectured on sustainable network development and is interested in issues involving workable solutions for green network development. He is active in the North American Network Operators Group (NANOG), Internet2, the American Registry for Internet Numbers (ARIN), and other network engineering groups.

Stephan SOMOGYI, Principal, Gyroscope

Stephan Somogyi is an expert in productizing security and privacy technologies. He is the principal of Gyroscope, a consultancy that has provided services to the Cloud Security Alliance, VMware, and Infineon, among others. He is also the principal partner in dotFIN LLC, a startup developing a high-assurance gTLD for global financial services. From 2002 to 2007 he was Director of Products at the PGP Corporation. He has also contributed to *The Economist*, *Wired*, and the *Financial Times*, and takes a particular interest in privacy, security, and risk challenges that span national boundaries.

Gaurab Raj UPADHAYA, Network Architect, Limelight

Gaurab Raj Upadhaya is Network Architect on the backbone engineering team of Limelight Networks (LLNW), Singapore office, supporting Limelight's high-speed backbone in Asia, Europe, and North America. He previously worked for Packet Clearing House as Senior Internet Analyst (2002-2010) and ran PCH's global anycast DNS platform. Gaurab has a long record of volunteerism and commitment to the Asia Pacific Internet community. He has served on the Asia-Pacific Internet Association (APIA) Board of Directors since 2004, and as Chair from 2006 through 2009. He has served on the APRICOT Program Committee continuously since 2004, and as Chair from 2007 to 2009. Additionally, in 2003 he was the founder of the South Asian Network Operators Group (SANOG). Gaurab is one of the fourteen global Trusted Community Representatives who cryptographically sign the root of the domain name system in ICANN Root DNSSEC Key ceremonies. In 2001 he founded the Nepal Internet Exchange (NPIX), the first Internet exchange in the South-Asian region, and still serves as its CEO. In 2007 he worked with local colleagues to build the Nepal Research and Education Network (NREN) and continues to serve as its Technical Director.

James KILABA, Deputy Director, Tanzania Communications Regulatory Authority
James Kilaba is Deputy Director of Information and Communication Technologies at the Tanzania Communications Regulatory Authority. He has a Masters degree in Telecommunications and Information Systems and is a Senior Member of the Institution of Engineers in Tanzania and is a Member of the Institute of Electrical and Electronics Engineers of fourteen years standing. Mr. Kilaba has represented Tanzania in the GAC and ICANN activities since 2002 and has been a member of the board of the Tanzania Network Information Centre (tzNIC) since 2007.

LIM Choon Sai, General Manager, Singapore Network Information Centre
Mr. Lim is the General Manager of the Singapore Network Information Centre (SGNIC) Pte Ltd which administers the registry function of .sg domain names. Mr Lim is also a Director in the Infocomm Development Authority of Singapore (IDA) which is the regulatory authority for telecommunications. He is responsible for the resource management and telecommunication standardisation. His responsibility includes frequency spectrum management, telephone network numbering/code management, network and equipment standards. Mr Lim holds a B Eng and MBA.

Jeff MOSS, VP & CSO, ICANN
Jeff Moss, founder of DEF CON, the world's largest hacker conference, and Black Hat, a global technical security conference, was named earlier this year as the Vice President and Chief Security Officer of the Internet Corporation for Assigned Names and Numbers (ICANN), the multinational non-profit organization working for a secure, stable and unified global Internet. Moss has organized technical security conferences around the globe, in locations such as the Netherlands, Spain, the United Arab Emirates, Japan, and Singapore. Prior to his work with Black Hat and DEF CON, he was a Director at the Secure Computing Corporation, where he established the professional services department in Asia, Australia and the United States. He also worked in the information system security division of Ernst & Young, LLP.

Marcel SCHNEIDER, Manager of Special Operations and International Relations, SWITCH

Marcel Schneider was born 1.4.1949 in Winterthur, Switzerland; basic education as dipl. El. Ing. FH/STV/EUR-ING. From 1973 to 1980 working for Swiss Broadcasting Corporation, technical department. From 1980 to 1990 at Willi Studer AG as project manager for the development of the first open reel digital tape recorders and as assistant to the chief development manager. January 1991 to today: Foundation SWITCH, first as network engineer, currently as manager special operations and international relations. Studies newer history at University of Zurich. Holds two patents and is co-author of a book on Internet domain names, published 1996.