The STRATEGIC NEWS SERVICE®
N E W S L E T T E R

SNS
NEXT YEAR'S NEWS
THIS WEEK
www.stratnews.com

The most accurate predictive letter in computing and telecommunications, read by industry leaders worldwide.

SNS Subscriber Edition Volume 14, Issue 24 Week of July 4, 2011

SNS
SPECIAL LETTER: SOLVING THE GREATEST ENTERPRISE SECURITY THREAT

"This was my first time at FiRe, and I think it's one of the best conferences I've ever been to." – *Gregory McRae, Executive Director, Morgan Stanley*

"What [FiRe] means to me most is really smart people, getting together and changing the world --- Best conference yet: good attendance, focused themes --- Great job!" – *Michael Pfeffer, Managing Partner, Kolohala Ventures*

Sign up now for FiRe 2012: www.futureinreview.com

IN THIS ISSUE

Publisher's Note: About five years ago, Ray Ozzie, then newly anointed chief software architect at Microsoft, described the world he saw, from a security perspective, and the vision was daunting. He maintained then, and it surely is true today, that the primary challenge for the enterprise operating system would be to allow trusted computing for a new "universe of devices."

Today that challenge, often referred to as the "consumerization" of enterprise IT tools, represents the greatest security risk chief information officers must face. Do you allow any Android (or, for that matter, Windows) phone onto your network just because Bob or Jill brought it to work?

The first answer is No. Android hacks are already legion, and the efforts have just begun. Not that anyone else in the business – perhaps outside of BlackBerry – has really locked down their phones.

In this week's special issue, Wave Systems' CEO Steven Sprague explains a simple, pervasive, low-cost, and effective solution to at least providing security down to the device – the solution most needed by CIOs yesterday – and then down to the user, as well. Why this has not been implemented yet is a separate question, but I will suggest that this technology (or one just like it) will be in full force within five years for securing all of our devices. – mra.

___

SOLVING THE GREATEST ENTERPRISE SECURITY THREAT

By Steven Sprague

The users have left the building.

You've heard it before: we've entered the age of the mobile workforce. Today's employees aren't confined to a physical office building, nor are they restricted to working on a corporate-issued PC. Workers are armed with laptops, smartphones, and other computing devices that are increasingly important to their jobs, empowering them with the resources and information they need to perform their work while beyond the office walls – and beyond the safety of the firewall and traditional IT security.

These new mobile employees fall into a range of categories, according to the research firm IDC [International Data Corp.]. IDC classifies *on-site movers* as those who move around many locations but within a single site – for example, IT technicians. *Yo-yos* are those employees who work from a fixed location but have jobs that require business travel. Next come *nomads*, who work in a number of different places – e.g., sales reps; *pendulums*, who work at two primary locations; and *carriers*, who must work while in motion.

Whatever the category or label for the mobile worker in your organization, their existence beyond the firewall is one trend that's transforming the way business is conducted. And this has now led to a second major phenomenon posing security challenges:

The applications are leaving the building.

Cloud Computing has been at the center of a lot of handwringing and analysis by pundits. Most enterprises are beyond the awareness stage, and have identified opportunities where Cloud Computing can be a business driver for their organizations. Yet implementers are struggling to understand how they should leverage the opportunities, while addressing the new challenges presented by all things Cloud – ensuring privacy, security, and reliability. But the significant benefits that the Cloud offers, from cost savings to flexibility, show us that this is not a passing phenomenon.

The consensus is that it's here to stay, the rightful successor to a previous generation's mainframe-client-server network computing model.

Take a look at the growing number of business applications that have already moved to the Cloud. Today, you can log into a customer-relationship management application such as SalesForce.com, or alter your tax withholdings and check on your 401(k), all in the Cloud.

There are still private Cloud applications. Our company, for example, still hasn't traded in its corporate email system for Gmail, nor do I predict that will happen anytime soon. But the migration has started; the user base is comfortable from their own consumer interactions with iTunes and photo sharing sites, and this evolution – much like the rise of the mobile worker – is transforming the cyber security landscape.

So if the users have left the building, and the apps have left the building, then what's the role of the corporate network?

What does the network look like when there is far less reliance on the LAN? Will the LAN go away? Or will we see it occupy a more peripheral role in corporate culture? And how do we implement robust security that takes these new realities into account?

The current authentication paradigm of username and password isn't working. And with the recent breach involving RSA, more sophisticated proprietary authentication, such as tokens, isn't fully adequate either. Let's start with a new idea: we need a new identity-centric model for networking, where the *identity of the device* determines access.

We start with the premise that only *known* devices are granted access to the collection of services that are one's own services – *my services*. Imagine a company where every device has a known identity, and only those devices that have been granted permission can access the organization's Sales Force Cloud application. Fundamentally, this means I've built a network, and that network is an identity-based network, in which all of the computing devices and their identities become the foundation for how my company exists in cyberspace. It is the nexus of the virtual corporation.

➢ Credentials Held Securely in the PC or Smartphone

The underpinning of this new security paradigm is the requirement that identity credentials must be held inside every device, in a place resistant to tampering. Otherwise, if those credentials were exposed and the identity of the device could be stolen, it would have the same impact as theft of a person's identity. If someone can steal the device credential, they can break into the network.

The industry came up with a remarkable way to securely house device credentials and, unbeknownst to many, it actually happened about a decade ago. It's a micro controller security chip encapsulated in the motherboard of the PC. It's called a Trusted Platform Module (TPM), and despite its low cost and ubiquity, it has significantly advanced the computing industry's security capabilities.

At the highest level, the TPM safely secures information – keys, passwords, and digital certificates. Because it is made from hardware, it's immune from external software attacks and resistant to physical tampering.

The standards for the TPM were created by the Trusted Computing Group (TCG), a consortium of the leading PC companies united by a common cause: recognition that enterprise security could be vastly improved through the application of hardware security conforming to open standards. With Trusted Computing, the TPM chip acts as the hardware root of trust, ensuring that systems behave in specific ways and those behaviors are enforced by hardware and software, when the owners of those systems enable these technologies.

The TCG has been unwavering in its commitment to open standards. Equally important is that it has acted on its commitment to ship them in scale – a commitment which has helped us evolve beyond the realm of the theoretical. Examples of precedents on the impact of standards on technology over the last two decades include RJ45 as the standard for Ethernet jacks, Wi-Fi, and CD-ROM. These were not features that businesses asked for or purchased; they were bundled into the platform and became available for widespread use. These features, which we take for granted today, have had a profound effect on our business environment. That's the power of standards.

The old axiom of the '90s comes to mind: *Standards are built by shipping*. That's where we are today with Trusted Computing. Approximately half a billion platforms have been shipped with the TPM, and the projected shipment rate is 100 million devices per year. This standard is here to stay, and provides us with the infrastructure that will allow us to change the very fabric of the enterprise network.

➢ The Trusted Platform Module As Credential Vault

The TPM has unique and sophisticated security features, far beyond the scope of this letter. Dense books have covered its capability for "remote attestation" or "assured cryptographic operations" or as a "trusted key store." But one of the easiest ways to think of it is as a "credential vault" – a container affixed to the motherboard of the computer that can hold identities. And those identities can be used to log me into a specific service, give my machine a specific identity, and assert the integrity of the device to specific services.

Now the TPM is capable of much more than creating a device ID. That's a narrow depiction of its functionality. The TPM can also fully represent a user's credential. The difference between a device credential and a user credential is a PIN number, or some other second factor that only the user possesses. The user types this information in, and that effectively binds the user identity to a set of keys. *This binding of the person's identity then allows those keys to log into networks or services as known and trusted devices.*

Think of the TPM then as a mini vault for credentials inside the PC. It can be provisioned by any public key infrastructure (PKI), which refers to the use of public-key and private-key pairing for authentication. This infrastructure benefits organization by ascertaining the quality of information sent and received, and by assuring the source and destination of that information. Using PKI, IT can provide keys that are bound to specific services.

It starts with a PC or laptop issued by your organization. IT then provisions the PC with dozens of keys that can log the user into his or her individual services – the business-enabling applications your corporation uses, from HR systems to productions systems or those accessed by sales and marketing. Each device contains this multitude of keys for these applications that the user is subscribed to.

Think about the implications: employees can now physically leave the office and, from anywhere in the world, connect to those services securely. Only the computing device has the credentials to assert that it is a known and authorized device. In this way, my traveling sales rep can log into her PC, and the PC then remembers how to log her into her services for which the company has authorized access. This is a dramatically simpler model – yet it is vastly more secure than the one we follow today. Users love it: our sales rep logs into her laptop, and that device manages the connection to her applications. It's that seamless and easy. And secure.

By creating a network of known devices, IT can assure that only trusted computers are accessing confidential information and applications. And likewise, the TPM in our PCs assures end users that the server on the other end of our connection is the proper, known server as well. It validates that we're connecting to a known corporate network that we intended to access and to communicate with.

We're already familiar with this model. We see it every day when accessing corporate email via BlackBerry smartphones, for example. A simple PIN unlocks the BlackBerry, which has a credential vault for strong authentication to enterprise email. In order for this to work, I had to register the device and enroll my credentials into the device.

Using a BlackBerry and accessing corporate email via an enterprise server is a familiar experience to many of us. IT sends you a code and you use it to enroll in the corporate server. Once you've performed this registration, you never have to remember your enterprise password for your email again, because you only have a simple PIN that unlocks your BlackBerry, and the BlackBerry remembers how to log you into the enterprise server.

Now imagine that model for all Cloud services.

Registration can be automated so that once I, the administrator, have bound the keys and registered the user's device, then I can deliver not only her keys for her email account, but also the keys for all the different services that belong within the corporation – or for only specific applications that you need access to for her job. This

is the identity-centric model of networking. Only known devices and only known users can access my services. That's the goal IT has today.

But what happens when we have multiple devices?

You may already possess a smartphone, a tablet, and a laptop. There's no reason why each of these devices shouldn't have a similar credential vault containing all the same keys that log you into your services. Think about the synchronization of the Amazon Kindle. I can begin reading the latest best-seller first on my Kindle and continue reading it on my iPad or on my PC. No matter which device I choose to read the book on, it knows where I left off.

This is possible with an identity-centric model for computing, in that my PC, or my tablet, or my smartphone, can all house credentials to the different services that I subscribe to and assign ownership to each of my devices. For the first time, I can begin a transaction on my PC and complete it on either my smartphone or my tablet, because both are able to assert that they are *known* and *trusted* devices, and that I'm in the middle of a continuing session or transaction with my online service.

There's been a debate about whether tablet computers will one day replace laptops as the standard-issue workplace computer. It's a debate that the top tablet and phone manufacturers have welcomed, and the concept may be a logical transition for some companies.

But this discussion assumes that we'll need to build in tablet-friendly functionality for apps in the Cloud or customize applications used mostly on the laptop to the tablet. *These discussions miss a larger point: We really want all of these devices, and for others to be secure and trusted devices that we can work on.*

And we want all of these devices to have the same set of capabilities for accessing the different services to which we subscribe, or to which we need access. This model provides the best end-user experience, because at any given moment wherever you happen to be – you'll have access to one of your devices. We all know the experience of trying to edit a spreadsheet on our BlackBerry. It's not a pretty sight. But if that's all you're carrying at the time, it's a viable, and perhaps necessary, option.

I would liken this experience to another that most of us would recognize: using the company phone when a perfectly good cellphone is sitting nearby.

Whether due to cost, convenience, or power, there's a reason we sometimes choose our land-line or voice-over-IP phone over our cellphone. Or we might choose a personal cellphone, with its limited minutes, over a work phone because of the advantage of a pre-saved contacts list. That's applicable to computing devices as well.

With a network consisting of only known devices, *what about the capability of the device*? The service itself can recognize the device that's accessing it, as websites do today when recognizing that you're visiting on a smartphone that runs better with a

streamlined page, optimized for mobile browsing. For example, the service could ask, "Does the device I'm talking to actually have the capability of storing, retaining, and managing sensitive content?"

If a Web-based service allows access to 10,000 Social Security numbers, how will the device receive and store those Social Security numbers? If the service is sending them to a laptop, and the laptop has client-side encryption installed, there's no problem. But if I should access a website with my Android phone, and if I have no data protection in place, then the service may query the device to verify if it has the ability to protect that sensitive data. And if no encryption is in place, the service can prevent access.

➢ Empowering Applications and Services

With a network that allows only known devices, the next step is to empower the services themselves, to know the function of the endpoint. This is a powerful new set of capabilities for the corporate network, as it means that I no longer have to have a consistent policy for my devices. By incorporating more agility at the service level, the service can verify whether appropriate policies are in place for the transaction to transpire. This is a seismic shift from the current corporate thinking, which is: "How do I get a monolithic desktop image on every desktop and a unified set of policies for each machine?"

That mindset is obsolete in an age in which we're bringing iPads, smartphones, and laptops to work. There's simply no way they're going to have the same policy capabilities. And it sets the stage for bringing your personal devices into the office security zone.

The Trusted Platform Module protects the credentials for users to log onto the services they've been provided access to. Trusted or known computing has created a foundation for an identity-centric model for networking, built upon a tamper-proof foundation of hardware security.

This is a proven security play. Think about the big cellular companies – T-Mobile, Verizon, AT&T – it's virtually impossible to access the AT&T network, for example, from an unregistered (thereby unknown) device. Registering the device to the network is simple to do and has provided great security for the phone carriers, and the consumer, for almost 20 years. It's a network that scaled to use by billions of devices.

Because of this security model that allows only known devices on the network, the concept of cloning a phone is no longer a concern for today's consumers. When we get our cellphone bill, we don't expect to see someone else's calls, texts, or app purchases on it. Concern about identity theft – in this example, for stolen minutes – has been a nonfactor for consumers.

The tools for enabling this security model for today's network are here, allowing me to bind only known devices to the enterprise network. It is one of the single most powerful steps to combat cyber security.

It's a security model that could substantially reduce cyber fraud.

Think about the impact of the reduction in fraud seen in the cellular industry with the transition from analog to digital, or with the cable industry's switch from analog cable boxes, with weak security, to today's more-effective cable boxes. Do you need to log on with a password to access each of your premium movie channels?

There are technologies built on industry standards that offer these capabilities for the PC today, that ultimately will support the smartphones, tablets, and other computing devices of tomorrow. The industry is evaluating the right technology for incorporating a credential vault for every app developer, from payment to access control. The BlackBerry already has this, and it's a step in the right direction. We need the same capability that consumers experience in Apple devices, Android, and Nokia products.

Trusted Computing provides industry standards and technology framework for a stronger and more secure network of the future, based upon the premise of known devices. Mobile trust module specification, another standard from the TCG, is a solid formation to enable this common security paradigm – not only for the PC, but also for all handsets and mobile devices.

Organizations need to begin taking the next steps with Trusted Computing adoptions. It all starts with known devices ensuring a hardware-level of assurance for every device we have, whether it's a tablet, a phone, a PC, a smart television, or the multimedia console or Internet hotspot in your car. We have the right set of specifications and tools to enable these capabilities today, strengthening identity and access control.

As we embrace and adopt new opportunities emanating from the Cloud, Trusted Computing is helping organizations to evolve their network infrastructure securely, by building upon a hardware security foundation.

With further awareness and, ultimately, broad implementation, this security model stands to benefit organizations, users, and consumers alike.

About the Author

Steven Sprague is the president and CEO of Wave Systems Corp., a leading provider of client and server software for hardware-based security, enabling organizations to know who is connecting to their IT infrastructure, to protect corporate data, and to strengthen the boundaries of their networks.

Since taking the helm as CEO, Steven has played an integral role driving the industry transition to embed stronger, hardware-based security into the PC. He has guided Wave to a position of market leadership in enterprise management of self-encrypting hard drives and Trusted Platform Module security chips.

As a popular speaker and IT security thought leader, Steven speaks at dozens of conferences and events each year – educating global audiences about the latest PC hardware security advancements and industry standards (both on behalf of Wave and in his leadership role with the Trusted Computing Group). His expertise lies in leveraging advancements in hardware security for strong authentication, data protection, advanced password management, enterprise-wide trust management services, and more.

Steven's background is built upon more than 20 years of executive and technology developer experience in computer security and e-commerce – with a primary focus on addressing critical security issues facing businesses and government today.

Before being named president and CEO, Steven was vice president of Wave from 1992 to 1995, involved in technology development and marketing. In June 1995, he founded Wave Interactive Network, a division of Wave, to pursue opportunities in the multimedia marketplace. Prior to Wave, Steven's management experience included positions as president of Tech Support Inc., and vice president of Engineering for Krofta Inc.

Steven received his Bachelor of Science degree in Mechanical Engineering from Cornell University.

I would like to thank Steven for presenting the case for implementing the Trusted Computing Platform now, with all of its obvious benefits for administrators and users alike. This would be important even if there were no such thing as an Economic Cyberwar raging around all IP-related companies. But in a time when nation-states, and their well-trained proxies, are mounting ongoing sets of Advanced Persistent Threat attacks against anyone with useful Intellectual Property, the stakes are much greater.

I hope your company will, as Steven recommends, consider implementing TCP now, to keep the few remaining horses that have not yet left the barn, inside. Or, as Jon Evans, head of MI5, put it in a letter to 300 British CEOs a few years ago: assume that all of your IP has been compromised, and act accordingly in the future.

Your comments are always welcome.

Sincerely,

Mark Anderson,
writing from the Accenture CIO Conference on Economic Cyberwar, London.

CEO
Strategic News Service LLC Tel. 360-378-3431
P.O. Box 1969 Fax. 360-378-7041
Friday Harbor, WA 98250 USA Email: sns@tapsns.com

—

To arrange for a speech by Mark Anderson on subjects in technology and economics, or to schedule *a strategic review* of your company, email mark@stratnews.com.

For inquiries about **Sponsorship Opportunities** and/or SNS Events, please contact Sharon Anderson-Morris ("SAM"), SNS Programs Director, at sam@stratnews.com or 435-649-3645.

If SNS is a competitive weapon, shouldn't all of your employees have it? Email David Morris at david@stratnews.com for **details on SNS Site Licenses.**

UPCOMING SNS EVENTS & MEDIA LINKS

Registration is now open for the annual **New York Predictions Dinner, December 8, 2011**, at the historic Waldorf=Astoria Hotel:

www.stratnews.com/newyork/2011

Register now for the 10th annual Future in Review conference, May 22-25, 2012, at the Montage Laguna Beach Hotel, California:

www.futureinreview.com

➢ SNS Media

- **SNS Interactive News™**

"SNS iNews is a terrific idea."
– Peter Petre, Author and Past Sr. Editor, *FORTUNE* magazine

Are you an AORTA (Always On RealTime Access) member of SNS? Use SNS iNews™ to stay in touch, in real time, with what your fellow members and FiRe Thought Leaders are achieving – and then help them get there.

Click here for the current iNews digest: www.snsinews.com

(For ID and password assistance, email scott@stratnews.com)

- **FiRe 2011 Photo Gallery:** See over 2,000 photos from FiRe 2011, at http://futureinreview.smugmug.com/FiRe-2010 – linked to galleries from FiRe conferences since 2007.

- **FiReGlobal : West Coast 2010 Photo Gallery:** Hundreds of photos of sessions and attendees at FiReGlobal 2010 in Seattle, taken by Dan Lamont: http://futureinreview.smugmug.com/FiReGlobal/Seattle-2010.

- **SNS Members' Book Lists:** SNS Library 2.0 – Here are your favorite books, including who has proposed them, whether they're fiction or nonfiction, and ready clicks to Amazon: www.tapsns.com/members/books.php

- **SNS TV on YouTube:** www.youtube.com/user/stratnews
- **FiRe TV on YouTube:** www.youtube.com/futureinreview
- **SNS in the News:** Announcements, press, and A/V links: www.tapsns.com/news.php
- **FiRe in the News:** www.futureinreview.com/press.php
- **SNS Blog, "A Bright Fire":** Join Mark in this SNS forum and add your own comments: www.abrightfire.com. If you're a blogger, you're welcome to email sally@stratnews.com if you'd like to be added to our blogroll.
- **SNS Media Page:** www.tapsns.com/media.php

IN OTHER HOUSE NEWS…

➢ SNS Positions Open

Site Sales by Commission. This person (or company) will join a team that continues our nearly 100% success rate in offering site licenses for the SNS newsletter to large companies. Current license holders include: Deloitte, Accenture, Deutsche Telekom, Internode Pty, Accenture's Global CIO Forum, and Adobe. Generous commissions available. Please send a cover letter and bio/resume to Sharon Anderson-Morris at sam@stratnews.com.

➢ How to Subscribe

(All rates $USD)

If you are not currently an SNS subscriber, the SNS newsletter has been sent to you for a one-month trial. If you would like a one-year subscription to SNS, the current rate is $595, which includes approximately 48 issues per year, plus special industry alerts and related materials. Premium Subscriptions, which include passworded access to additional materials on the SNS website, are $895 per year. Subscriptions can be purchased, upgraded, or renewed at our secure website, at www.stratnews.com. Contact Scott Schramke, scott@stratnews.com, for subscription assistance.

UPGRADE YOUR SUBSCRIPTION TO PREMIUM LEVEL for $300 per year, and enjoy email access to our FiRe Conference speakers through our new service, SNS Interactive News (SNS iNews™), along with other Premium benefits. After logging in to your Account, go to: www.tapsns.com/orders/?page=account.

VOLUME CORPORATE SUBSCRIPTION RATES: More than half-price savings, for up to 10 members: $2950. Additional members: $295.

SMALL COMPANY SITE LICENSE (for companies with fewer than 10 employees): Deep discount (far less than half price), for up to 10 members: $1495. Additional members: $295.

TEACHERS' GROUP RATE (five teachers): $295.

STUDENT and INDEPENDENT JOURNALIST RATE: $295 per year.

➢ May I Share This Newsletter?

If you are aware of others who would like to receive this service, please forward this message to them, with a cc: to Mark Anderson at sns@stratnews.com; they will automatically receive a free one-month pilot subscription.

➢ About the Strategic News Service

SNS is the most accurate predictive letter covering the computer and telecom industries. It is personally read by the top managers at companies such as Intel, Microsoft, Dell, HP, Cisco, Sun, Google, Yahoo!, Ericsson, Telstra, and China Mobile, as well as by leading financial analysts at the world's top investment banks and venture capital funds, including Goldman Sachs, Merrill Lynch, Kleiner Perkins, Venrock, Warburg Pincus, and 3i. It is regularly quoted in top industry publications such as *BusinessWeek*, *WIRED*, *Barron's*, *Fortune*, *PC Magazine*, ZDNet, Business 2.0, the *Financial Times*, the *New York Times*, the *Wall Street Journal*, and elsewhere.

Email sent to SNS may be reprinted, unless you indicate that it is not to be.

➢ About the Publisher

Mark Anderson is CEO of the Strategic News Service. He is the founder of two software companies and of the Washington Technology Industry Association "Fast Pitch" Forum, Washington's premier software investment conference; and has participated in the launch of many software startups. He regularly appears on the *CNN World News*, CNBC and CNBC Europe, Reuters TV, the BBC, Wall Street Review/KSDO, and National Public Radio programs. He is a member of the Merrill Lynch Technology Advisory Board, and is an advisor and/or investor in OVP Ventures, Ignition Partners, Mohr Davidow Ventures, the UCSD Calit2 Laboratory, the Global

Advisory Council of the mPedigree Network (Ghana), SwedeTrade, The Family Circle (Europe), and the Australian American Leadership Dialogue.

Mark serves as chair of the Future in Review Conferences, SNS Project Inkwell, The Foresight Foundation, and Orca Relief Citizens Alliance.

➢ Where's Mark?

• On July 7 and 8, Mark will be leading the **Accenture C-Suite Network Summit** section, CIO Circle Cyber Security Summit, in London, on the subject of "Economic Cyberwar." • On November 7-9, he will be speaking at the **Accenture** Annual meeting in Berlin, on Economic Cyberwar and Valuing Intellectual Property. • Save the date now for the **SNS Annual Predictions Dinner at the Waldorf=Astoria**, New York, December 8th, 2011, where Mark will share his views on the economic landscape, and technology predictions for the coming year, and host a general discussion on what 2012 has in store. Registration is now open at www.stratnews.com/newyork/2011. • On May 22-25, 2012, he will be be hosting the **10th annual FiRe conference**, at the Montage Laguna Beach. You really should sign up now, at www.futureinreview.com.

ISSN 1093-8494