SIGMA
A PIVOT COMPANY

# SigmaUptime

volume 14 number 5

# Opening Up

Dell’s open-networking solutions reduce cost and complexity by giving customers the option to run open-source software on Dell switches.

# Technology services to help you streamline operations, reduce costs and improve business processes.

Companies today must align IT strategy with their corporate objectives, strategy and business model. Pivot has created a portfolio of operating companies and partners with a focus on helping you enhance and extend the capabilities of your technology assets.

Pivot provides technology services ranging from initial needs assessment and design, through procurement and implementation, to on-going support. As an adjunct to your IT team, we provide the resources that allow your team to offload some of the day-to-day operational challenges and focus on innovations that will drive business value and competitive advantage.

Contact us to learn more.

PIVOT
TECHNOLOGY SERVICES

www.pivotts.com 888-895-0495

# Contents

4

**Sigma Uptime**

**Editorial Correspondence:**

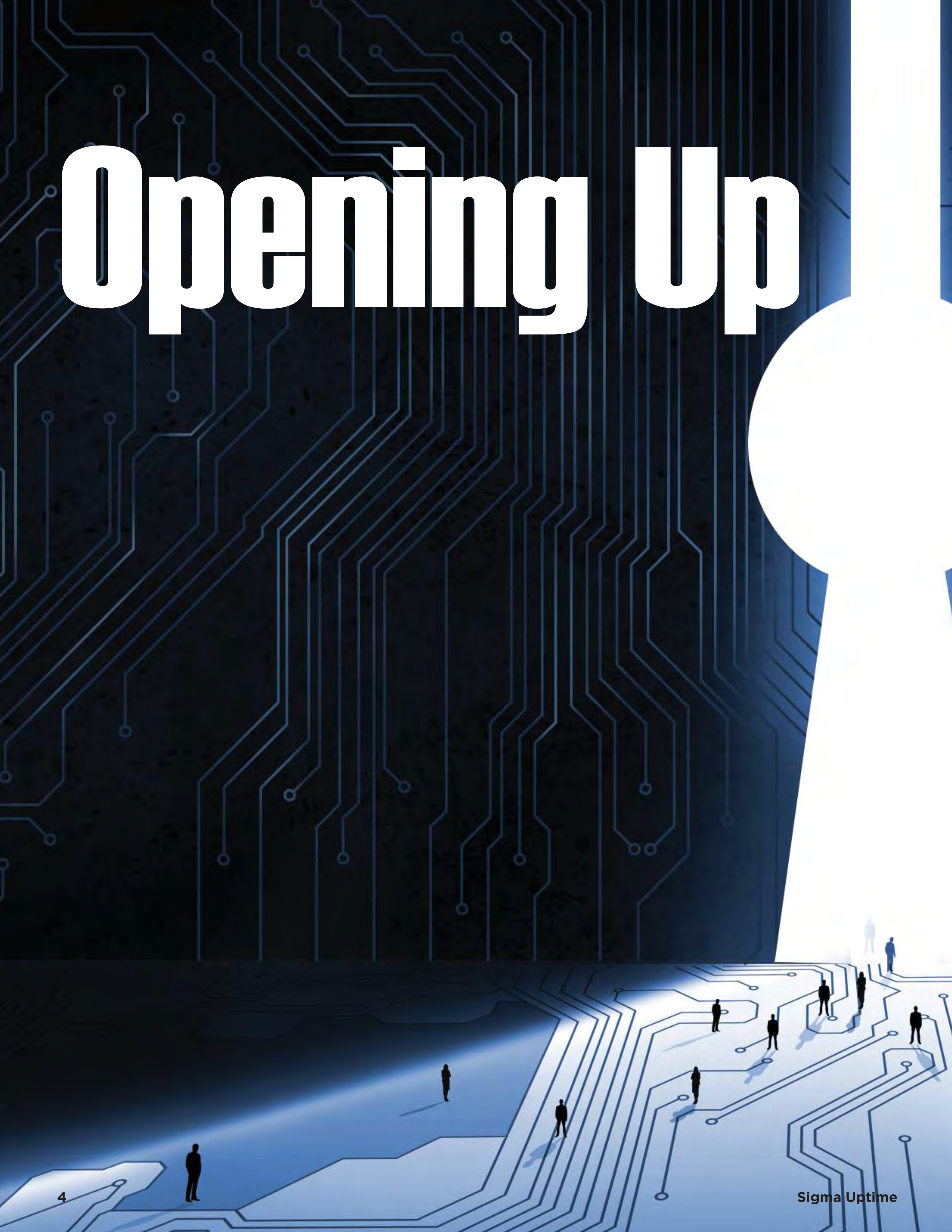
7360 East 38th Street, Tulsa, OK 74145

Phone (800) 726-7667 • Fax (918) 270-7134

Change of Address: Send corrected address label to the above address.

Sigma UPTIME is published bimonthly by CMS Special Interest Publications. Printed in the U.S.A. Product names may be trademarks of their respective companies.

# Opening Up



*Dell's open-networking solutions reduce cost and complexity by giving customers the option to run open-source software on Dell switches.*

Computing technology has changed dramatically since the days of the mainframe — and not just in terms of capacity and performance. Open-computing principles have allowed organizations to leverage commodity hardware and open-source software to drive down costs and enable innovation. The result is a more flexible, scalable and manageable data center infrastructure.

These concepts have been slow to reach the network environment. Traditionally, network architectures are built from proprietary devices that must be configured and managed using vendor-specific protocols — a time-consuming, resource-intensive process.

Software-defined networking (SDN) promises to relieve this bottleneck by separating control of the data plane from the physical network hardware. With SDN, administrators use centralized controllers to manage how applications and services are delivered across the network. SDN also enables the use of automation and orchestration to provision, configure and allocate network resources. Open-source standards such as OpenFlow help minimize vendor lock-in and make network design and operation simpler and more flexible.

Despite its promise, SDN has been hampered by a lack of consensus regarding standards. Incumbent networking vendors have introduced their own competing technologies, creating confusion as to the true definition of SDN.

"SDN was introduced by the Open Networking Foundation — but somewhere along the way, the con-

continued on page 6

cept of openness took a back seat to other issues," said Brad Moss, Solutions Architect, Sigma Solutions. "Protocols such as OpenFlow have helped to relieve vendor lock-in, but simply adding open standards to proprietary network switches doesn't get to the root cause of the problem.

"Dell is addressing this issue with its open-networking initiative. Dell has introduced a line of products that disaggregate network hardware and software, providing customers with the kind of flexibility and choice they're accustomed to with open computing."

## The 'Brite' Way

The open-networking concept arose in the hyperscale space, where Facebook, Google, Amazon and other large cloud service providers began deploying generic "white-box" switching and routing hardware to support open-source networking software. Open networking provides the levels of scalability and flexibility that are needed for the build-out of massive, web-scale data centers.

Although enterprises could also benefit from white-box switching, few have the ability to take advantage of it. Network engineers would have to procure generic equipment and integrate the networking software without the kind of support they're accustomed to with traditional gear. This has led to the development of so-called "brite-box" switches that offer the benefits of white-box switching in a branded component that is easier to buy and implement.

> "By allowing customers to run open-source software on Dell hardware, Dell can offer switches that are more open and less expensive than traditional network gear."

"Traditionally, network switching hardware comes tightly integrated with the vendor's network operating system and other software," Moss said. "Brite-box switches break this interdependence through hardware and software disaggregation, enabling customers to choose these components independently. A vendor's switching software can run on commodity hardware, or third-party software can run on the vendor's switches."

The primary advantages of brite-box switches are cost, simplicity and innovation. The development of open-source networking software requires that hardware specifications be shared and more standardized, which in turn drives down hardware prices and reduces compatibility problems. In turn, ongoing collaboration within the open-networking community has the potential to accelerate the pace of network innovation.

"By allowing customers to run open-source software on Dell hardware, Dell can offer switches that are more open and less expensive than traditional network gear. Dell's open-networking solutions are more expensive than white-box switches but are backed by the services and support of an industry-leading vendor," said Moss.

## Strong Commitment

Dell launched its open-networking initiative in January 2014 when it began offering Cumulus Networks' Linux operating system on Dell switches. Dell soon expanded the program to include open-source network virtualization software from Midokura and SDN products from Big Switch Networks.

In April 2015, Dell introduced 1/10GbE and 40GbE switches and a multi-rate 10/25/40/50/100GbE platform that offer low latency and high density with the flexibility of operating system choices. These solutions support the Open Network Install Environment (ONIE) to allow for a zero-touch install of all prequalified operating systems, including Dell Networking OS9 and third-party options. In September, Dell debuted the Dell Networking S6100-ON, combining multi-rate connectivity, chassis-level modularity and open networking to deliver unparalleled in-rack networking flexibility for data center operators.

"Dell was one of the first — if not the first — of the top-tier vendors to launch an open-networking initiative," Moss said. "Since then, Dell has shown its commitment to open networking by introducing products for a wide range of customers, from smaller organizations to large enterprises and service providers."

The dominance of proprietary hardware, software and operating systems in the networking sector has made it difficult for the open-networking concept to gain traction. However, a growing movement toward software-defined architectures has helped mobilize supporters of open networking, creating an influential community of vendors and customers who are committed to making the network more flexible and standardized.

"Legacy network architectures built from proprietary devices and software are ill-suited to today's highly dynamic IT environment. Organizations need the flexibility to run the networking software of their choice on any compatible switching hardware," said Moss. "Dell's open-networking initiative gives customers that flexibility and choice and paves the way for a more agile, software-defined environment."

The Dell Z9100-ON 10/25/40/50/100GbE network switch

# A new era in network flexibility.

Traditional chassis-based switches built before virtualization and cloud computing created vendor lock-in and left organizations with few choices about their network platforms. Dell is changing that with its family of Open Networking switches that can run operating systems from multiple vendors.

Based on our award-winning Z-Series and S-Series switch hardware and featuring a choice of third-party OS and software options, these solutions give you the power to transform your network and accelerate data-center innovation with simplified, high-capacity network fabrics. Designed to ease orchestration and automation, Dell Open Networking switches provide a clear path to software-defined networking (SDN).

Contact your Sigma representative to learn how Dell's Open Networking switches can dynamically change your IT environment by simplifying deployment and operations while reducing costs.

SIGMA
A PIVOT COMPANY

www.sigmasol.com 888.895.0495

# The Software-Defined WAN

*SDN principles improve the performance and reliability of branch network links.*

The need to connect countless objects, devices, people and applications is fundamentally changing the way workloads move through the network. Cloud computing, mobile access, federated applications and unified communications are among the services that have significantly increased network traffic and intensified connectivity demands.

These demands are particularly acute in organizations with multiple locations and distributed workforces. Remote sites require wide-area network (WAN) connectivity with the performance and reliability to support a full complement of mission-critical services and applications.

Industry analysts say applying the principles of software-defined networking (SDN) to the network edge can bring new levels of reliability and functionality to the WAN. The software-defined WAN (SD-WAN) enables IT organizations to dynamically mix and match connectivity options to optimize traffic, improve application performance and control expenses.

"SD-WAN is a new and transformational way to architect, deploy and operate corporate WANs, as it provides a dramatically simplified way of deploying and managing remote branch office connectivity in a cost-effective manner," Gartner analysts Andrew Lerner and Neil Rickard wrote in their July 2015 technology overview.

## Connectivity Choices

SD-WAN allows an organization to blend transport types such as MPLS and broadband to suit their specific needs. While Internet broadband circuits deliver more cost-effective bandwidth than a service provider's dedicated MPLS connection, MPLS offers more functionality and security, making it ideal for mission-critical and sensitive data.

In a traditional WAN environment, the manual configurations required to differentiate and segment traffic are complex and time-consuming. These configurations need to be updated regularly as application profiles and business needs change, which would require IT to visit each location for every update. As users and organizations demand greater flexibility and agility, and computing continues to shift to mobile and the cloud, the cost and complexity of traditional WAN models are becoming unsustainable.

SD-WAN enables organizations to centrally manage and automate configurations of WAN edge routers. Rather than having a single active network and a backup connection, all connections are active, and traffic routing is automated across a hybrid network that includes public broadband, private MPLS, Internet VPNs and LTE.

## Cost Efficiency

SD-WAN reduces costs by making it possible for organizations to rely more upon broadband and less upon more expensive, private MPLS links. SD-WAN is intelligent enough to know when broadband won't provide an adequate connection and reroutes traffic to MPLS on an "as needed" basis. Complex configurations that were previously manual are automated through the SD-WAN application. IT only has to define and prioritize various types of traffic and routing policies instead of constantly reconfiguring devices. Routing is based upon the current state of the network, providing the flexibility to adapt to changing network conditions.

SD-WAN also provides network functions virtualization, which virtualizes all network services. Rather than requiring IT to manage a number of appliances to provide WAN functions, SD-WAN brings these functions to one device where they can be centrally managed and deployed on demand.

SD-WAN appears to be catching on. A recent IHS Infonectics survey of 150 businesses in North America found that 45 percent intend to increase spending on SD-WAN over the next two years.

"Within the data center, raw speed with support for software-defined networking and virtualized workloads are the top requirements for fabrics," said Cliff Grossner, IHS research director. "Meanwhile, outside the data center, SDN-led transformation is taking hold in the WAN optimization market. There's a shift from optimizing application traffic flows over a single point-to-point WAN link to automated and dynamic load balancing of application traffic over multiple link types — MPLS, broadband, Internet, cellular, et cetera."

## WAN Study Shows Demand Spiking

The ongoing migration of applications to the cloud, the limitations of the public Internet over long distances and the impact of networking problems on application performance are among the key factors driving the evolution of the enterprise WAN, according to a new report.

Network optimization provider Aryaka's 2015 State of the Enterprise WAN report notes that these trends are contributing to a sharp rise in enterprise bandwidth demand and the need to improve last-mile access. The report says the emergence of software-defined WAN solutions will help resolve some of these issues.

Following are some of the key points in the report:

- Global enterprise bandwidth demand grew at a mean rate of 236 percent last year.

- The software vertical saw the highest growth in bandwidth demand, with demand more than doubling over last year. Manufacturing, computer hardware and financial services companies also saw a huge surge in bandwidth demand.

- Regional Internet bandwidth is improving globally, with 67 percent of those surveyed reporting they use a high-speed Internet link (greater than or equal to 10Mbps) for their last mile.

- HTTP traffic continues to dominate, pointing toward heavy cloud adoption rates. The firm said 88 percent of enterprise organizations send HTTP traffic over the WAN, while 80 percent send HTTPS.

- Many protocols, including CIFS, HTTP, IMAP and MSSQL, can see bandwidth usage savings of 50 percent or more with the right optimization technologies in place. Data reduction can help enterprises keep up with skyrocketing bandwidth demands, at least in the short term. In the longer term, more advanced, unified approaches will be needed.

- Enterprises typically see less than 0.25 percent packet loss over the last-mile link, even in places such as China and India. The global median packet loss is a mere 0.04 percent. However, this is only for last-mile links. Over longer distances, the public Internet is far from business-grade, since network problems in the middle mile tend to kill application performance.

# Changing of the Guard

*Once-formidable SSL 3.0 encryption protocol is showing its age as security flaws are exposed.*

In 1996, Janet Jackson became the highest-paid musician of all time, Beanie Babies were "must-have" Christmas presents, AOL ruled the Internet and the Macarena was the most popular dance in the world.

Things change.

Version 3.0 of the Secure Sockets Layer (SSL) protocol became an indispensable element of network security when it was released back in '96 to protect data being sent across the Internet by providing encryption and authentication between servers and applications. Compared to other developments of the day, it has had spectacular longevity — it's still supported by as much as 98 percent of the world's most popular web sites, by some accounts.

It's had a good run, but just like the "Rachel" haircut and Hootie and the Blowfish, SSL 3.0 is past its prime.

Several recently uncovered flaws have essentially made the protocol too vulnerable to be of any practical value. The POODLE, FREAK and Logjam attacks all are designed to exploit SSL 3.0 vulnerabilities through "man-in-the-middle" attacks that will force security downgrades and make encrypted information easier to crack. The Google researchers who uncovered the POODLE attack say SSL 3.0 is "an obsolete and insecure protocol."

## The 'Downgrade Dance'

SSL 3.0 actually was replaced with an improved protocol — Transport Layer Security (TLS) version 1.0 — back in 2011. TLS 1.0 was based upon SSL 3.0 and is considered only marginally more secure. Versions 1.1 and 1.2 of TLS are significantly more secure and fix many of the vulnerabilities in SSL 3.0 and TLS 1.0. In April 2014, the National Institute of Standards and Technology (NIST) issued guidelines recommending that government agencies use TLS 1.1 and 1.2.

However, most TLS implementations include provisions for backward compatibility with SSL 3.0 to interoperate with legacy systems and ensure a smooth user experience. A protocol "handshake" process negotiates the latest protocol version common to both the client (browser) and the server (website), and then implements that version for authentication.

A team of Google researchers announced last fall that they had uncovered a significant flaw they termed POODLE, which stands for "Padding Oracle on Downgraded Legacy Encryption." In a POODLE attack, the attacker interferes with the protocol handshake process and forces browsers and websites to accept SSL 3.0. In a process Google calls the "protocol downgrade dance," the attacker simply interrupts secure connections, forcing the browser to retry with the next-lower protocol. Once the downgrade process has moved through all versions of TLS to SSL 3.0, the attacker can exploit known vulnerabilities to decrypt secure HTTP cookies, which could let them steal information or take control of the victim's online accounts.

## Freak Show

FREAK is another man-in-the-middle attack designed to force a downgrade in security measures. The flaw, which stands for "Factoring RSA Export Keys," was announced in March by a group of cryptographers who discovered a weakness in the SSL/TLS protocols that had actually been introduced on purpose decades earlier for compliance with U.S. security regulations.

This flaw allows an attacker to force secure connections to a lower level of encryption — 512 bit — which can be read and attacked with relative ease. It is an artifact of 1990s U.S. security policy requiring software being exported out of the country to be limited to "export-grade" encryption with key pairs of 512 bits or less. The idea was to make it easier for the U.S. to break the codes of any foreign adversaries.

"The 512-bit export grade encryption was a compromise between dumb and dumber," cryptographer Matthew Green of Johns Hopkins University wrote in a blog post explaining the vulnerability. "In theory it was designed to ensure that the NSA would have the ability to 'access' communications, while allegedly providing crypto that was still 'good enough' for commercial use."

The group that uncovered the flaw discovered that support for this weaker "export-grade" encryption was still baked in to numerous Web servers, browsers and other SSL implementations. The bug affects SSL/TLS servers and clients, and Microsoft, Google, Apple and Mozilla all have patches in the works.

## Shutting It Down

In May, a second group of cryptographers announced they'd found another flaw based on cryptographic export restrictions. Unlike a FREAK attack, which tricks both ends of a conversation into accepting downgraded security, a Logjam attack exploits a vulnerability in the key exchange to make both believe they are running stronger keys than they actually are. The middleman in the attack can then eavesdrop or actually insert data into the communication path.

In response to this rash of flaws, Microsoft, Apple, Google and Mozilla have all issued patches for these vulnerabilities and are working to make their browsers more secure. Mozilla disabled SSL 3.0 in Firefox 34, as did Google with Chrome 40 and Microsoft with Internet Explorer 11. Apple has not gone that far yet, but it did block Safari's use of vulnerable cryptographic ciphers and has stopped using SSL 3.0 for its push notifications service.

In the long run, organizations likely will work to reconfigure web servers to address the SSL issue at its root. In the meantime, security experts say organizations and users should take a proactive approach to the vulnerability by updating to the latest version of their chosen web browser, or turn off support for SSL 3.0. A comprehensive guide for turning off SSL support in a variety of browsers is located at https://zmap.io/sslv3/browsers.html.

When it was introduced, SSL 3.0 represented a quantum leap in Internet security, and it was the de facto standard for cryptography for the better part of two decades. By providing an authentication process that ensured data confidentiality and integrity, it allowed millions of websites to protect online transactions with customers. However, POODLE and other exploits have now exposed critical flaws in the protocol, and there's no room for nostalgia in data security.

## New PCI-DSS Standard Addresses SSL Flaw

To address vulnerabilities within the Secure Sockets Layer (SSL) encryption protocol that can put payment card data at risk, the PCI Security Standards Council published an updated version of the PCI Data Security Standard (DSS) on April 15. Version 3.1 went into effect immediately, with version 3.0 retired on June 30.

The move comes in response to word from Google researchers about a serious SSL flaw called POODLE (Padding Oracle on Downgraded Legacy Encryption) that enables hackers to obtain passwords and other confidential information that can be used to access a user's private account on a website. Upgrading to a current, secure version of TLS is the only known way to remediate the vulnerabilities that have been exploited by POODLE.

To address this risk, PCI DSS 3.1 removes all references to SSL and early versions of TLS from requirements 2.2.3, 2.3 and 4.1 of the standard. Although the revisions are effective immediately, impacted requirements have a sunset date to allow for organizations with affected systems to implement the changes:

- SSL and early TLS cannot be used as security controls to protect payment data after June 30, 2016. However, existing implementations that use SSL and/or early TLS must have a formal risk mitigation and migration plan in place prior to this date.

- Effective immediately, new implementations must not use SSL or early TLS. New implementations are those that have no existing dependency on the use of the vulnerable protocols.

- Point-of-sale (POS) devices that can be verified as not being susceptible to any known exploits of SSL and early TLS may continue using these protocols as a security control after June 30, 2016.

PCI 3.0 became mandatory on January 1, and brought sweeping changes to the rules organizations must follow in securing payment data. Chief among these is a new mindset that encourages a "continuous compliance" approach to data protection. Although PCI 3.0 was published in 2013, many organizations are still struggling to adapt to the new requirements. Version 3.1 adds a new layer of complexity.