

## Issue 90

Publication date: 27/11/2009

### Contents

- New ISO Standard for Effective Management of Risk
- ENISA Clears the Fog on Cloud Computing Security
- SPDY: An experimental Protocol for a Faster Web
- Draft: TLS & SSLv3 Renegotiation Vulnerability 2009
- Swine Flu Fears Makes Millions for Russian
- Virtually Here: The Age of Cyber Warfare
- Study Finds Majority of Security Products do not Perform as Intended
- Using a Cisco Router as a "Remote Collector" for tcpdump or Wireshark

### CCIP Contact Details:

T: +64 (0)4 498-7654  
F: +64 (0)4 498-7655  
E: [info@ccip.govt.nz](mailto:info@ccip.govt.nz)

<http://www.ccip.govt.nz/>

## New ISO Standard for Effective Management of Risk

International Standards Organisation

A new International Standard, ISO 31000:2009, Risk management – Principles and guidelines, will help organizations of all types and sizes to manage risk effectively. New ISO standard for effective management of risk ISO 31000 provides principles, framework and a process for managing any form of risk in a transparent, systematic and credible manner within any scope or context. At the same time, ISO is publishing ISO Guide 73:2009, Risk management vocabulary, which complements ISO 31000 by providing a collection of terms and definitions relating to the management of risk.

Source: <http://www.iso.org/>

## ENISA Clears the Fog on Cloud Computing Security

European Network and Information Security Agency

How can businesses and governments get the obvious benefits of cloud computing without putting their organisation at risk? The EU's 'cyber security' agency, ENISA (the European Network and Information Security Agency) answers this question in a comprehensive, new report on "Cloud Computing: Benefits, risks and recommendations for information security". It covers the technical, policy and legal implications and most importantly, makes concrete recommendations for how to address the risks and maximise the benefits for users.

Source: <http://www.enisa.europa.eu/>

## SPDY: An experimental Protocol for a Faster Web

Google

As part of the "Let's make the web faster" initiative, we are experimenting with alternative protocols to help reduce the latency of web pages. One of these experiments is SPDY (pronounced "SPeeDY"), an application-layer protocol for transporting content over the web, designed specifically for minimal latency. In addition to a specification of the protocol, we have developed a SPDY-enabled Google Chrome browser and open-source web server. In lab tests, we have compared the performance of these applications over HTTP and SPDY, and have observed up to 64% reductions in page load times in SPDY. We hope to engage the open source community to contribute ideas, feedback, code, and test results, to make SPDY the next-generation application protocol for a faster web.

Source: <http://dev.chromium.org/>

## Draft: TLS & SSLv3 Renegotiation Vulnerability 2009

G-SEC™

Around the 09/11/2009 Marsh Ray, Steve Dispensa and Martin Rex published details<sup>1</sup> about a vulnerability affecting the renegotiation phase of the TLS & SSLv3 protocol. The vulnerability is being tracked under CVE-2009-35552 | VU#1205413 and affects a multitude of platforms and protocols, the impact of this vulnerability varies from protocol to protocol and research into those is currently ongoing.

Source: <http://blog.g-sec.lu/>

### Information Security Links

Centre for the Protection of National Infrastructure (CPNI)

Canadian Cyber Incident Response Centre (CCIRC)

United States Computer Emergency Readiness Team (US-CERT)

CERT Coordination Center (CERT/CC)

Australian Computer Emergency Response Team (AusCERT)

Internet Storm Center (ISC)

US-CERT Cyber Security Bulletins

### Safe Computing Links

CCIP Security Guidelines

NetSafe

National Cyber Alert System (USA)

AusCERT National Information Technology Alert Service (AUS)

IT Security Awareness For Everyone (UK)

National Alerting Service (Netherlands)

## Swine Flu Fears Makes Millions for Russian

*Sophos*

As the number of reported swine flu cases in Britain climbs to an all-time high, IT security and data protection firm Sophos has added its voice to government warnings against buying Tamiflu over the internet. Panic-induced stockpiling by individuals who aren't officially classified as being at risk of contracting swine flu, and therefore anxious they won't receive Tamiflu from the NHS, will not only line cybercriminals' pockets with millions of pounds in cash but also grant them access to sensitive personal data to be used for other crimes. Sophos's indepth look at how these underground web affiliates, which form networks called the Partnerka, profit from online Tamiflu sales was revealed today in a whitepaper entitled "The Partnerka – what is it, and why should you care?"

Source: <http://www.sophos.com/>

## Virtually Here: The Age of Cyber Warfare

*McAfee*

Is the "Age of Cyber War" at hand? This year, the fifth annual McAfee Virtual Criminology Report contemplates this question and others prompted by the fact that nation-states are arming themselves for the cyberspace battlefield. Since our 2007 report, when we last discussed the growing cyber threat to national security, there have been increasing reports of cyber attacks and network infiltrations that appear to be linked to nation-states and political goals.

Source: <http://resources.mcafee.com/> (Registration required)

## Study Finds Majority of Security Products do not Perform as Intended

*ICSA Labs*

Are the security products your organization depends upon every day reliable? Do they consistently meet expectations and live up to their billing? Chances are they do not. This experience has resulted in the not-so-tongue-and-cheek postulation that new security products are created to compensate for the shortcomings and side effects of the existing ones. That's not to say there is never a legitimate need for new security solutions; new business models, new technologies, new threats, and new levels of global interconnectedness require us to continually adapt the products and practices we employ to protect information assets.

Source: <http://www.icsalabs.com/>

## Using a Cisco Router as a "Remote Collector" for tcpdump or Wireshark

*Internet Storm Center*

Have you ever thought about your routers. I mean - \*really\* thought about them? They think all day long, processing all of the packets in and out of your company's WAN or internet connection, and hardly ever complain. But can you get any useful information out of those packets? PC's with almost any operating system can be configured with tcpdump or windump (with wireshark or whatever gui you'd care to hang in front of it) to do packet capture and analysis. But if the traffic you are trying to capture is halfway across the world (or maybe closer but still too far to drive), can you use your router to capture packets in a standard libpcap format? As you've probably guessed, the answer is YES, or else there'd be no reason to write this article. Let's go through the steps, from start to finish.

Source: <http://isc.sans.org/>

*While this e-bulletin is accurate to the best of our knowledge, CCIP does not accept any responsibility for errors or omissions. If any of the vulnerabilities affects you, you are advised to ensure that you have the most current information available. CCIP will not be liable for any loss or damage howsoever caused, arising from or in connection with the use of information contained in this e-bulletin.*

*CCIP only issues those external alerts that we assess as serious and would affect a large number of New Zealand users. For notification of all discovered software vulnerabilities we recommend that you subscribe to a commercial Computer Emergency Response Team or to vendor alert lists.*

*Reference in this e-bulletin in any manner to any commercial product, process or service does not constitute or imply its endorsement or recommendation by CCIP. Views and opinions expressed herein may not be used for advertising or product endorsement purposes.*

