

## Issue 46

Publication date: 14/09/07

### Contents

- CIS Benchmark for securing Virtual Machines
- Sanity Check: is perimeter security dead and is protecting the data all that matters?
- The Security of Web Services as Software
- Sensitive Information Requires Extra-Care to Prevent Industrial Espionage
- Guide to Secure Web Services
- Dual Perspectives: A CIO's and CISO's Take on Security
- Understanding Windows Vista Service Hardening
- New Computer Security Guides Available

### 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/>

## CIS Benchmark for securing Virtual Machines

*Center for Internet Security*

This white paper addresses security concerns that apply generally to Virtual Machine technologies. The recommendations contained within are vendor neutral and should apply to most virtualization deployments. Recommendations are based on a variety of public sources and input from members of the Center for Internet Security (CIS).

Source: <http://www.cisecurity.org/> (registration required)

## Sanity Check: is perimeter security dead and is protecting the data all that matters?

*TechRepublic*

The primary method of corporate computer security over the past three decades has been focused around the network. It's been about allowing those inside the network to have privileged access to corporate resources and building impenetrable walls to keep outsiders out. Unfortunately, this model is rapidly losing its effectiveness because the borders of networks are becoming much more fluid and dynamic with the advent of VPN, Web mail, push e-mail on smartphones, telecommuters, and a geographically dispersed and mobile workforce.

Source: <http://blogs.techrepublic.com.com/>

## The Security of Web Services as Software

*Booz Allen Hamilton*

To help creators of Web services and Service-Oriented Architectures (SOAs) understand and address the security challenges that confront them, the National Institute of Standards and Technology (NIST) is getting ready to publish a new Special Publication (SP) 800-95, Guide to Secure Web Services. This SP describes Web service security standards and explains how to develop Web services and SOA portals using technologies based on those standards. However, neither SP 800-95 nor the standards it describes address a critical challenge: the security of Web services as software. Without considering software security, developers cannot create Web services that are truly trustworthy. This article describes both the content of SP 800-95 and highlights its critical omissions in terms of measures needed to produce Web service software that is in and of itself secure.

Source: <http://www.stsc.hill.af.mil/>

## Sensitive Information Requires Extra-Care to Prevent Industrial Espionage

*IT Security Portal*

If the news is to be believed, it seems that an employee at Ferrari just could not resist it and helped himself to a few secrets. Not only that, but according to the news an employee at a competitor couldn't resist the temptation when offered the chance to gain some inside info. After all what man in his right mind could resist the temptation of getting the inside gossip. We're all curious and live in a world where we daily try to steal a lead on our competitors and every little bit of info helps. So there we have it a court battle ensues between McLaren and Ferrari!

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

### 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

The Internet Safety Group (NZ)

CCIP Security Tips

National Cyber Alert System (USA)

AusCERT National Information Technology Alert Service (AUS)

IT Security Awareness For Everyone (UK)

National Alerting Service (Netherlands)

## Guide to Secure Web Services

*National Institute of Standards and Technology*

SP 800-95 seeks to assist organizations in understanding the challenges in integrating information security practices into Service Oriented Architecture (SOA) design and development based on Web services. The publication also provides practical, real-world guidance on current and emerging standards applicable to Web services, as well as background information on the most common security threats to SOAs based on Web services.

Source: <http://csrc.nist.gov/>

## Dual Perspectives: A CIO's and CISO's Take on Security

*CERT Coordination Center®*

In this podcast, Motorola CIO Patty Morrison and CISO Bill Boni share their experiences in their respective roles and offer advice for listeners who are faced with building a security program or strengthening their current one.

Podcast: <http://www.cert.org/podcast/show/morrisonboni.html>

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

## Understanding Windows Vista Service Hardening

*ZDNet UK*

Microsoft has been touting Windows Vista as the most secure Windows ever. Backing up that claim, Microsoft has included a number of new security features in the operating system. These new features are designed to address some of the common vectors by which previous versions of Windows have fallen to anonymous miscreants and other criminals.

Source: <http://resources.zdnet.co.uk/>

## New Computer Security Guides Available

*Government Computer News (US)*

The National Institute of Standards and Technology has updated its security guidelines for dealing with active content, providing an overview for active content and mobile code in use today and laying out a framework for making security decisions about its use within an organization.

A draft of Special Publication 800-28 Revision 2, titled "Guidelines on Active Content and Mobile Code," has been released for public comment.

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

## Boards Lack Real Understanding of IT Risks Facing Their Companies

*PricewaterhouseCoopers LLP*

Technology-related risks figure higher on the agenda of UK company boards than ever before but new research questions whether board members really have sufficient understanding of their organisation's IT risks to address them adequately.

Source: <http://www.ukmediacentre.pwc.com/>



*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.*