

## Issue 45

Publication date: 31/08/07

### Contents

- New Zealand 2007 Daylight Saving Changes
- Privacy Breach Guidelines
- Shared SCADA WAN: Enterprise, Surveillance and VoIP
- Know Your Enemy: Malicious Web Servers
- Old Threats Never Die
- Awareness and Training Surveys in EU and US
- Tackling Security at the National Level: A Resource for Leaders
- When your World is Hacked
- Foundations of Cryptography

### 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 Zealand 2007 Daylight Saving Changes

*Microsoft*

In April 2007 the New Zealand Government announced an update to the Time Act of 1974. This update changes the dates of both the start and end of daylight saving time (DST). When this law goes into effect in 2007, daylight savings time will start one week earlier (2:00 A.M. on the 30th September 2007) and will end two weeks later (3:00 A.M. on 6th April 2008) than past years.

A number of Microsoft® products require updates for the new daylight saving times.

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

## Privacy Breach Guidelines

*Privacy Commissioner*

Key steps for agencies responding to privacy breaches and privacy breach guidelines. The Commissioner welcomes feedback on the draft documents. Comments due by 28 September 2007.

Source: <http://privacy.org.nz/>

## Shared SCADA WAN: Enterprise, Surveillance and VoIP

*Digital Bond*

A few new fronts are emerging in the battle between physical and logical separation of SCADA WAN's. When we perform assessment and architecture projects we always ask if there are any new applications or changes expected in the near future. Increasing we hear that IP cameras and VoIP phones will be installed at the field sites and potentially travelling over the physical SCADA WAN. Is this an issue?

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

## Know Your Enemy: Malicious Web Servers

*The Honeynet Project & Research Alliance*

Today, many attackers are part of organized crime with the intent to defraud their victims. Their goal is to deploy malware on a victim's machine and to start collecting sensitive data, such as online account credentials and credit card numbers. Since attackers have a tendency to take the path of least resistance and many traditional attack paths are barred by a basic set of security measures, such as firewalls or anti-virus engines, the "black hats" are turning to easier, unprotected attack paths to place their malware onto the end user's machine. They are turning to client-side attacks.

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

## Old Threats Never Die

*IBM*

What kind of answer do you give if someone asks you "how long did it take before the slammer worm ceased to be a threat?" Slammer kicked off in the morning of January 24th, 2003, and within its first 10 minutes of propagation had managed to compromise an estimated 75,000 hosts running Microsoft's SQL Server engine. To most security professionals, it's "the worm that could – and did". So, when did it cease to be a threat?

Source: <http://blogs.iss.net/>

### 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)

## Awareness and Training Surveys in EU and US

*NoticeBored*

Two survey reports into information security awareness and training practices offer insights into the state of the art. The first report from the European Network and Information Security Agency ENISA is Information security awareness initiatives: current practice and the measurement of success. Although the survey and case studies are European in origin, I'm sure the general discussion and ideas on the thorny issue of measuring information security awareness programs, and in fact measuring information security as a whole, are broadly applicable. The second report from NASCIO (an organization representing chief information officers, information technology executives and managers from US state governments) is IT Security Awareness and Training: Changing the Culture of State Government. The authors promote security awareness as a preventive control that can help to avert major crises caused by serious information security incidents.

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

## Tackling Security at the National Level: A Resource for Leaders

*CERT/CC*

Not all information security incidents can be handled in-house. Some require coordination with third-party forensics firms or law enforcement personnel, others with external partners or suppliers, and still others with national or global organizations. In these latter types of incidents, the expertise of a national CSIRT (Computer Security Incident Response Team) can be a valuable resource for business leaders.

National CSIRTs deal with security at the macro level. They focus on large-scale incidents or incidents that can affect the economy, critical infrastructure, government operations, or national security. If they are dealing with a worldwide event, they can coordinate with national CSIRTs in other countries to establish communications and cooperation among those countries to deal with the incident.

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

## When your World is Hacked

*CIO Magazine*

The call to Bob Bailey, an IT executive with a major government contractor, came on an otherwise ordinary day in October 2003. "Why are you attacking us?" demanded the caller, an IT leader with a Silicon Valley manufacturer. He wanted to know why Bailey's company had launched a denial-of-service attack against his network.

Source: <http://cio.co.nz/>

## Foundations of Cryptography

*SecurityDocs.com*

Cryptography has been employed for keeping secrets since the time of Caesar. From the simplest ciphers of shifting letters, to mathematically provably secure ciphers of today, cryptography has progressed a long way. It also has widened to a number of uses and capabilities to fit an ever growing number of applications. Cryptography makes it possible to keep data secure over an insecure network. It also makes it possible to keep private data on your computer safe from prying eyes. Even car thieves can be foiled by crypto systems in your remote unlock system.

Source: <http://www.securitydocs.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.*