

Issue 44

Publication date: 17/08/07

Contents

- Third Consultation on RMC Policy Review
- Government Must Act Now to Maintain Confidence in the Internet
- UNIX & Linux Security Checklist v3.0
- The Yin & Yang of Internet Security Research
- Wireless Network Security for IEEE 802.11a/b/g & Bluetooth
- The Evolution of Networks Beyond IP
- Shared SCADA WAN: Enterprise, Surveillance & VoIP
- The Physical Layer

CCIP Contact Details:

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

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

Third Consultation on RMC Policy Review

Office of the Domain Name Commissioner

InternetNZ, through the Domain Name Commission (DNC), is currently reviewing the Registering, Managing and Cancelling Domain Names policy. An initial call for comments on the policy review resulted in four submissions being received. These can be seen at <http://dnc.org.nz/rmc-review>. A second call for comments on some of the proposals raised as a result of the initial consultation was undertaken. Nine submissions were received as a result of that and these, together with the consultation paper, can be seen at <http://dnc.org.nz/rmc-2ndconsult>.

Source: <http://www.dnc.org.nz/>

Government Must Act Now to Maintain Confidence in the Internet

Lords Science & Technology Committee (UK)

The House of Lords Science and Technology Committee have today highlighted the threat to the future of the Internet posed by e-crime, and have argued that the Government must do more to protect individual Internet users.

The Committee argue that the laissez-faire attitude taken to Internet security by a range of stakeholders including Government, Internet Service Providers, hardware and software manufacturers and others risks undermining public confidence in the Internet and contributes to a 'wild west' culture where the end user alone is responsible for ensuring they are protected from criminal attacks online.

The Internet, while still a powerful force for good, has increasingly become the playground for criminals. Today's e-criminals are highly skilled, organised, and motivated by financial gain. Individual Internet users are increasingly victimised - yet instead of acting to protect individuals, or providing incentives for the private sector to act, Government continues to insist that individuals are ultimately responsible for their own security. The Committee describe this approach as "inefficient and unrealistic".

Source: <http://www.parliament.uk/>

The report & evidence: <http://www.publications.parliament.uk/>

UNIX & Linux Security Checklist v3.0

AusCERT

This document aims to assist system administrators in organisations of all sizes by providing a concise guide to running UNIX and Linux systems securely.

In version 3.0, the checklist has been fully updated, and is structured to follow the lifecycle of the system, covering the steps to be considered at each stage from initial planning to maintenance.

Source: <http://www.auscert.org.au/>

The Yin & Yang of Internet Security Research

Washington Post

A law that makes it a crime to host, online or otherwise, software that could be used in cyber attacks went into effect in Germany this month. While the reaction from Germany's hacker culture has been somewhat muted, the measure is already prompting changes within one of the world's most active computer security research and hacking communities.

Source: <http://blog.washingtonpost.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)

Wireless Network Security for IEEE 802.11a/b/g & Bluetooth

National Institute of Standards & Technology

SP 800-48 Revision 1 provides an overview of wireless networking technologies and gives detailed information on two standards commonly used in office environments and by mobile workforces: Institute of Electrical and Electronics Engineers (IEEE) 802.11a/b/g and IEEE 802.15.1, better known as Bluetooth. The publication seeks to assist organizations in reducing the risks associated with these forms of wireless networking. SP 800-48 Revision 1 updates the original version of SP 800-48, which was released in November 2002. SP 800-48 Revision 1 complements, and does not replace, SP 800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i. People seeking information on IEEE 802.11i should consult SP 800-97.

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

The Evolution of Networks Beyond IP

International Engineering Consortium

To understand how networks are evolving beyond Internet protocol (IP), we must begin by looking at the trends and challenges faced by the primary consumers of network connectivity, which are the array of enterprise and consumer applications and services that sit just outside the network edge. The message coming from C-level executives at the enterprises, traditional service providers, and content providers that manage these applications and services is the same—networks need to better understand the content and context of the data they carry. Today's solution of using content infrastructure software does not deliver the results desired.

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

Shared SCADA WAN: Enterprise, Surveillance & 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. Increasingly we hear that IP cameras and VoIP phones will be installed at the field sites and potentially traveling over the physical SCADA WAN. Is this an issue?

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

The Physical Layer

Maarten Van Horenbeeck, Internet Storm Center

About ten years or so ago, I was very much into a BBC television series called 'Bugs' which sketched the lives of a couple of skilled high tech crime investigators. It always dealt with spectacular physical machines (think radio guided cars & airplanes) controlled by computers, because this obviously makes the dry subject a bit more vivid.

Recent history proved them right that there is something more physical out there than OSI layer 1. In many cases, the data we as security professionals need to protect has an impact on the physical lives of others. Nowhere is this division as thin as with SCADA and DCS equipment.

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.