



AGAINST CYBER THREATS

CCIP e-Bulletin

CENTRE for CRITICAL INFRASTRUCTURE PROTECTION

Issue 35

Publication date: 16/03/07

Contents

- IEEE 802.11 Wireless LAN Security with Microsoft Windows
- Avoid Wasting Money on Penetration Testing
- Introduction to Windows Integrity Control
- Drive-By Pharming
- Password Malpractice: Are You Guilty?
- Read RSS, Get Hacked
- Introduction to Security Governance
- Improving the Intelligence of Your Gateway Security
- Independent Comparatives of Anti-Virus Software

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/>

IEEE 802.11 Wireless LAN Security with Microsoft Windows

Microsoft

Although wireless LAN networks provide freedom of movement, they also require you to address security issues that are not as prevalent on a private cabling system for a wired LAN technology such as Ethernet. The main security issues are the authentication of wireless clients and the encryption and data integrity of wireless LAN frames. This paper discusses the security issues of IEEE 802.11 wireless networks and shows how Microsoft Windows operating systems can be used to make 802.11 wireless networks as secure as the current set of 802.11-related technologies allow.

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

Avoid Wasting Money on Penetration Testing

IT-Observer

Penetration Testing is the final word in proving that technical compliance and good security practices are in place - or so it should be. But how do you know if you're getting a good service or not? What if the consultant performing the test is inexperienced? What is the impact on quality if the consultant is overworked? What if the consultant is an expert 'hacker', but terrible at report writing?

The trouble with asking questions like these is that there's no tick box to check when choosing your supplier. An easier method is to ask if someone has CHECK or PCI accreditation. However, neither of these is a guarantee of quality.

<http://www.it-observer.com/>

Introduction to Windows Integrity Control

SecurityFocus

This article takes a look at the Windows Integrity Control (WIC) capabilities in Windows Vista by examining how it protects objects such as files and folders on Vista computers, the different levels of protection offered, and how administrators can control WIC using the ICACLS command-line tool. WIC is intended to protect a system from malware and user error by helping to establish different levels of trust on objects.

<http://www.securityfocus.com/>

Drive-By Pharming

Indiana University Department of Computer Science

Inexpensive broadband routers are a popular way for people to create an internal, and sometimes wireless, network in their homes. By purchasing such a router and plugging it in, they can have a network set up in seconds. Unfortunately, by visiting a malicious web page, a person can inadvertently open up his router for attack; settings on the router can be changed, including the DNS servers used by the members of this small, quickly erected internal network. In this paper, we describe how a web site can attack home routers from the inside and mount sophisticated pharming attacks that may result in denial of service, malware infection, or identity theft among other things. Our attacks do not exploit any vulnerabilities in the user's browser. Instead, all they require is that the browser run JavaScript and Java Applets. We also propose countermeasures to defeat this type of malware -- new methods that must be used since the traditional technique of employing client-side security software to prevent malware, is not sufficient to stop our proposed attacks.

<http://www.cs.indiana.edu/>

Information Security Links

National Infrastructure Security Co-ordination Centre (NISCC)

Public Safety and Emergency Preparedness Canada (PSEPC)

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)

Password Malpractice: Are You Guilty?

IT-Observer

The explosion of passwords in today's enterprise has created a sea of holes in the security infrastructure. Some CIOs have responded to the challenge by bringing in the lifeboats, figuratively speaking, but in many cases the password-related security risk remains largely unchecked and even ignored.

Whether out of denial, inertia or sheer work overload, many IT managers simply look the other way when it comes to ensuring password security. The upshot, in effect, is password malpractice. Thousands of points of possible network infiltration are left open to determined hackers and even disgruntled employees. One cracked or stolen password can undo all other security measures combined.

<http://www.it-observer.com/>

Read RSS, Get Hacked

Computerworld

Users of Web feed services such as Real Simple Syndication (RSS) and Atom might want to make doubly sure they are not downloading malicious code along with their favorite Web content.

That's because the growing use of Web feed readers and the proliferation of content-aggregation sites are giving hackers a really simple way to deliver keystroke loggers, Trojan horses and other malware onto their computers, security analysts warn.

<http://www.computerworld.com/>

Introduction to Security Governance

SearchSecurity.com

Security governance is very similar in nature to corporate and IT governance because there is overlapping functionality and goals between the three. All three work within an organizational structure of a company and have the same goals of helping to ensure that the company will survive and thrive – they just each have different focuses.

<http://searchsecurity.techtarget.com/>

Improving the Intelligence of Your Gateway Security

Microsoft

If you want to build a comprehensive SSL-secured access platform that will help you extend and manage the reach of your information systems, check out these resources and get in-depth guidance on edge solutions, including Microsoft Internet Security and Acceleration (ISA) Server 2006 and the Whale Intelligent Application Gateway (IAG).

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

Independent Comparatives of Anti-Virus Software

av-comparatives.org

On this site you will find independent comparatives of Anti-Virus software. All products listed in our comparatives are already a selection of some very good anti-virus products. In order to get tested by us, companies must fulfill various conditions and minimum requirements.

<http://www.av-comparatives.org/>



AGAINST CYBER THREATS

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.