



NEWSLETTER

CENTRE for
CRITICAL INFRASTRUCTURE
PROTECTION

Volume 3, Issue 7

October 2004

THE TIMES THEY ARE A-CHANGIN

Thank you Mr Dylan. These words are as true today as they were forty years ago when the album and title song were first released. And they are particularly relevant to the CCIP as we have relocated from the GCSB Head Office to St Paul's Square which also houses the Ministry of Education and Audit Office. All contact details remain the same.

It was also a big month for [Microsoft Updates](#). After the minimal patch release in September, there has been a deluge of advisories released this month. A total of three IMPORTANT and seven CRITICAL security bulletins were released for a number of operating system components and applications, including a cumulative security update for Internet Explorer. An update to [MS04-028: Buffer overrun in JPEG processing \(GDI+\) could allow code execution](#) was also released which affected Office XP, Visio 2002 and Project 2002.

Apple released several [security updates](#). Among which were applications such as ServerAdmin and QuickTime.

Several interesting reports have been released recently. The SANS Institute have released this year's list of the [Top 20 critical Internet threats facing organisations](#). "The Top-20 is a consensus list of vulnerabilities that require immediate remediation. It is the result of a process that brought together dozens of leading security experts. They come from the most security-conscious government agencies in the UK, US, and Singapore; the leading security software vendors and consulting firms; the top university-based security programs; many other user organizations; and the SANS Institute."

Symantec have also produced their half-year [Internet Security Threat Report](#). This report highlights five main issues affecting Internet users today:

1. The time to patch vulnerable systems is shorter.
2. Remotely controlled BOT networks are growing.
3. The IP space of 40% of Fortune 100 companies is compromised by worms.

4. e-Commerce is the most frequently targeted industry.
5. Attacks against application technologies are increasing.

Ernst & Young have released their [Global Information Security Survey for 2004](#). The main obstacle to effective information security, according to the respondents of the survey, is "lack of security awareness by users".

Finally, our sister organisation in the UK, the National Infrastructure Security Co-ordination Centre (NISCC) have published an excellent [Introduction to Vulnerability Assessment Tools](#) which is also well worth a read.

In this issue of the newsletter we provide a background to [Radio Frequency Identification \(RFID\) devices](#). This will be followed up in the next issue with a discussion on usage, applications and some security and privacy issues. But we kick off this month with a discussion around key loggers and the exfiltration of sensitive data from computer systems.

FROM THE CCIP FILES

CCIP is aware of a number of personal account login details that have been captured by keystroke logging malware, which usually includes userID and passwords. This data is then transmitted to a log server under the control of the hacker or originator of the malware attack. This is often described as exfiltration of data. Where we are aware of such cases, the log server has been shut down, and

the owners of the affected domains have been notified. The use of keystroke logging malware makes the strength of passwords irrelevant. While we encourage the use of a strong password, containing a combination of ASCII characters, any user ID and password system is vulnerable to keystroke logging. We have considered some ideas for protecting passwords from keystroke logging, and have the

following suggestions:

1. Cut and paste a password from a portion of a text document. (Probably not a good idea to have just the password sitting around in a text file on your PC).
2. Type password intermingled with some extra characters,

Continued on page 2

CONTENTS

<i>The Times They are A-Changin</i>	1
<i>From the CCIP Files</i>	1
<i>Radio Frequency Identification (RFID)</i>	3
<i>Virus Activity</i>	5
<i>Recent Significant Alerts & Advisories</i>	5

Communication regarding this newsletter should be addressed to: newsletter@ccip.govt.nz



Government
Communications
Security Bureau

CONTACT DETAILS

Ph: +64 4 498 7654

Fax: +64 4 498 7655

E-mail: info@ccip.govt.nz

Web: www.ccip.govt.nz

Mail: P.O. Box 12-209
Wellington
New Zealand

Be suspicious of any e-mail with urgent requests for personal financial information. Unless the e-mail is digitally signed, you have no assurance it wasn't forged or 'spoofed'.

From the CCIP Files

The US have been aggressive in cracking down on cyber-crime schemes. The recent success of the Joint FBI and US Department of Justice operation "Web Snare" has netted 150 individuals facing arrest or convictions.

From the CCIP Files

FROM THE CCIP FILES Continued

use the mouse to select the extra characters, then delete. (Ensure the extra characters are the same each time to avoid password discovery using letter frequency analysis).

In the case of keystroke logging, prevention is definitely better than the cure. Our message remains the same:

- Keep AV / spyware definitions up to date.
- Use a personal firewall that filters both ingress and egress network traffic to and from your machine.
- Browse the web in a safe manner.
- Keep up to date with verified software – especially browsers and e-mail clients.
- Avoid using the same password for multiple sites.

As a general rule, on line e-commerce is safe. However caution must be exercised before giving out personal financial information over the Internet. The [Anti-Phishing Working Group](#) has compiled the following list of recommendations:

1. Be suspicious of any e-mail with urgent requests for personal financial information. Unless the e-mail is [digitally signed](#), you have no assurance it wasn't forged or 'spoofed'. Typically phishing e-mails;
 - Include upsetting or exciting (but false) statements in their e-mails to get people to react immediately.
 - Ask for information such as user names, passwords, credit card numbers, etc.
 - Are NOT personalized, while valid messages from your bank or e-commerce company generally are.
2. Don't use the links in an e-mail to get to any web page,

if you suspect the message might not be authentic. Instead, call the company on the telephone, or log onto the website directly by typing in the Web address in your browser.

3. Avoid filling out forms in e-mail messages that ask for personal financial information. You should only communicate information such as credit card numbers or account information via a secure website or the telephone.
4. Always ensure that you're using a secure website when submitting credit card or other sensitive information via your Web browser. To make sure you're on a secure Web server, check the beginning of the Web address in your browsers URL address bar - it should be "https://" rather than just "http://". Consider installing a Web browser tool bar to help protect you from known phishing fraud websites, e.g. EarthLink ScamBlocker is part of a free browser tool bar that alerts you before you visit a page that's on Earthlink's list of known fraudulent phisher Web sites. Its free to all Internet users - download at [Earthlink.net](#).
5. Regularly log into your online accounts. Don't leave it for as long as a month before you check each account.
6. Regularly check your bank, credit and debit card statements to ensure that all transactions are legitimate if anything is suspicious, contact your bank and all card issuers.
7. Ensure that your browser is up to date and security patches applied.

8. Always report "phishing" or "spoofed" e-mails to the following groups:

- Forward the e-mail to reportphishing@antiphishing.com
- Forward the e-mail to the Federal Trade Commission at spam@uce.gov
- Forward the e-mail to the "abuse" e-mail address at the company that is being spoofed (e.g. "spoof@ebay.com").
- When forwarding spoofed messages, always include the entire original e-mail with its original header information intact.
- Notify the Internet Fraud Complaint Center of the FBI by filing a complaint on their website: www.ifccfbi.gov
Note: New Zealand Commerce Commission runs [ScamWatch](#), which monitor for scams.

The US have been aggressive in cracking down on cyber-crime schemes. The recent success of the Joint FBI and US Department of Justice operation "Web Snare" has netted 150 individuals facing arrest or convictions. Refer to the following links:

http://www.justice.gov/opa/pr/2004/August/04_crm_583.htm

<http://www.ifccfbi.gov/strategy/websnare.pdf>

In New Zealand The Internet safety Group run the [Netsafe](#) site which offers cybersafety education for all New Zealanders - children, parents, schools, community organisations and businesses.

If you suspect that you have been the victim of potentially fraudulent online banking activity, you should contact your own bank in the first instance for advice and guidance.

RADIO FREQUENCY IDENTIFICATION (RFID)

Introduction

RFID is an area of automatic identification that is gaining momentum and is considered by some to emerge as one of the most pervasive computing technologies in history. In its simplest form, RFID is a similar concept to bar coding. It is seen as a means of enhancing data processes and is complementary to existing technologies. It is a proven technology that has been in use since the 1970s.

A more complex description is an electromagnetic proximity identification and data transaction system. Using "RFID tags" on objects or assets, and "readers" to gather the tag information, RFID represents an improvement over bar codes in terms of non-optical proximity communication, information density, and two-way communication ability. Operational RFID systems involve tags and readers interacting with objects (assets) and database systems to provide an information and/or operational function.

RFID is used for a wide variety of applications ranging from the familiar building access control proximity cards to supply chain tracking, toll collection, vehicle parking access control, retail stock management, ski lift access, tracking library books, theft prevention, vehicle immobiliser systems and railway rolling stock identification and movement tracking.

While RFID systems can yield great productivity gains, they also expose new threats to the security and privacy of individuals and organisations.

A Brief History

One of the earliest papers exploring RFID is a landmark paper by Harry Stockman "Communication by Means of

Reflected Power" published in 1948. This came on the heels of the radar and radio research undertaken during the Second World War. There are also several technologies related to RFID, such as long range transponder systems of IFF (Identification Friend or Foe) systems for aircraft. It was, however, thirty years before technology caught up with the theory with the development of the integrated circuit, the microprocessor and changing business practices.

In the 1950's there was a theoretical exploration of RFID techniques with a number of pioneering research and scientific papers being published. In the 1960's various inventors and researchers developed prototype systems. Some commercial systems (for example, Sensormatic and Checkpoint) were launched with the electronic article surveillance (EAS) equipment used as an anti-theft device. These systems used 1-bit tags detecting the presence or absence of a tag and were used in retail stores attached to high value items and clothing. This proved an effective anti-theft measure and is arguably the first and most widespread commercial use of RFID.

In the 1970s there was a great deal of interest in RFID from researchers, developers and academic institutions including the Los Alamos Scientific Laboratory and the Swedish Microwave Institute Foundation. There was much development work in this period and such applications as animal tagging became commercially viable.

In the 1980s RFID applications extended into a number of areas. In Europe animal tracking systems became widespread and toll roads in Italy, France, Spain, Portugal and Norway were RFID equipped.

The 1990s were significant with the widespread adoption of electronic toll collection in the United States. In 1991 an electronic tolling system opened in Oklahoma where vehicles could pass toll collection points at highway speeds, (no toll booths). In Europe there was considerable interest in RFID applications including toll collections, rail applications and access control.

RFID Tolling and rail applications also appeared in many countries including Australia, China, Hong Kong, Argentina, Brazil, Mexico, Canada, Japan, Malaysia, Singapore, Thailand, New Zealand, South Korea, and South Africa.

Developments continued in the 1990s with integrated circuit development and size reduction until microwave RFID tags were reduced to a single integrated circuit.

Currently there is considerable work being undertaken in the rationalisation of frequency spectrum allocation between countries, development of standards and the introduction of many commercial applications. There are now over 350 patents registered with the US Patent Office, related to RFID and RFID applications.

What is RFID?

Today RFID is a generic term for technologies that use radio waves to automatically identify people or objects¹. There are several methods of identification, the most common of which is to associate the RFID tag unique identifier with an object or person.

An RFID system will typically comprise:

- An RFID device (tag);

While RFID systems can yield great productivity gains, they also expose new threats to the security and privacy of individuals and organisations.

Radio Frequency Identification

Today RFID is a generic term for technologies that use radio waves to automatically identify people or objects¹.

Radio Frequency Identification

Continued on page 4

ⁱ *RFID Journal Frequently Asked Questions, www.rfidjournal.com.*

RFID References

ⁱⁱ *Data from "Radio Frequency Identification - A Basic Primer", Association for Automatic Identification and Data Capture Technologies, August 2001 www.aimglobal.org and from Wikipedia Encyclopaedia, <http://en.wikipedia.org/wiki/RFID>.*

RFID References

RFID Continued

- A tag reader with an antenna and transceiver
- A host system or connection to an enterprise system.

Tags

RFID devices fall into two broad categories, those with a power supply (a battery) and those without. An RFID device that actively transmits to a reader is known as a transponder (TRANSMitter/resPONDER). Unpowered passive devices are known as "tags". More recently, common usage has described transponders as "active tags" and unpowered devices as "passive tags". Active tags are typically read/write devices while passive tags are generally read only.

Active tags are larger and more expensive than passive tags. The use of a battery places a limit on the life of the device, although with current battery technology this may be as much as ten years.

Passive tags have an unlimited life, are lighter, smaller and cheaper. The trade-off is limited data storage capability, a shorter read range and they require a higher-power reader. Performance is reduced in electromagnetically "noisy" environments.

There are also semi-passive tags where the battery runs the chip's circuitry but the device communicates by drawing power from the reader.

Tags are available in a wide variety of shapes, sizes and protective housings. Animal tracking tags, which are injected beneath the skin, are approximately 10mm long and 1mm in diameter. Some are encapsulated in credit card sized packages, typically building access cards. Others are for use in harsh environments such as container tracking applications and can measure 120x100x50mm.

Tag Data

Tags can incorporate read only memory (ROM), volatile read/write random access memory (RAM) or write once/read many memory (WORM). ROM is used to store security data, a unique device identifier and operating system instructions. RAM is used for data storage during transponder interrogation and response.

Data will comprise a unique identifier and may also include:

- Operating system;
- Data storage (volatile or non-volatile);
- Electronic product code (EPC - the successor to the bar-code).

Tag Operation

Passive tags draw their power from the transmission of the reader through inductive coupling. The passive tags will then respond to the enquiry. Inductive coupling requires close proximity.

Active tags usually communicate through propagation coupling and respond to the reader's transmission drawing on internal power to transmit.

Frequency Ranges

Frequency allocations are generally managed through legislation and regulation by individual governments. Internationally there are differences in frequencies allocated from RFID applications although standardisation through ISO and similar organisations is assisting in compatibility. For example, Europe uses 868 MHz for UHF and the US uses 915 MHz. Currently very few frequencies are consistently available on a global basis for RFID applications. Three frequency ranges are generally used for RFID applications:

In general, low-frequency passive tags have an effective range of 30cm, high frequency passive tags around a metre and UHF passive tags from 3 - 5 metres. Where longer range is needed, such as in container tracking and railway applications, active tags can boost the signal to a range of 100 metres. The smallest devices commercially available measure 0.4x0.4mm and are thinner than a sheet of paper.

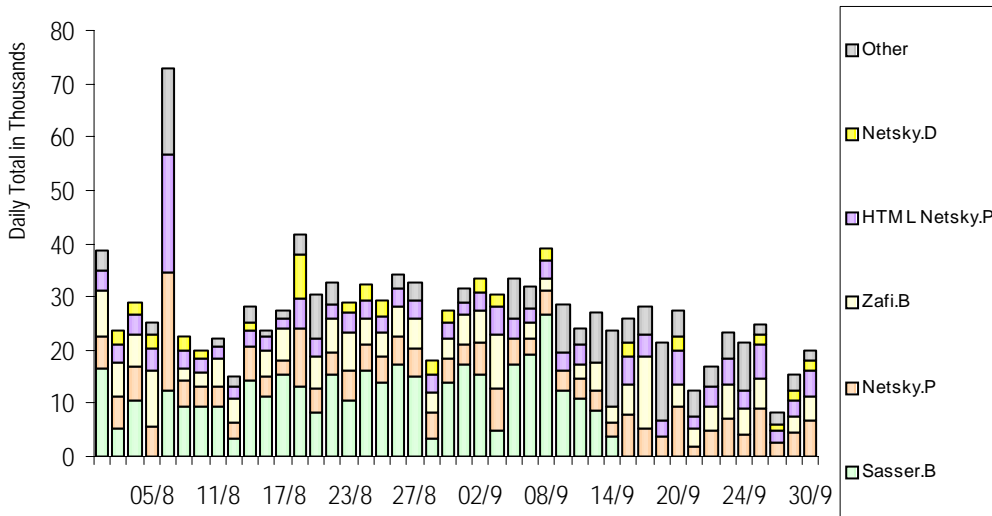
[See sidebar for references.](#)

Frequency Bands and Applicationsⁱⁱ

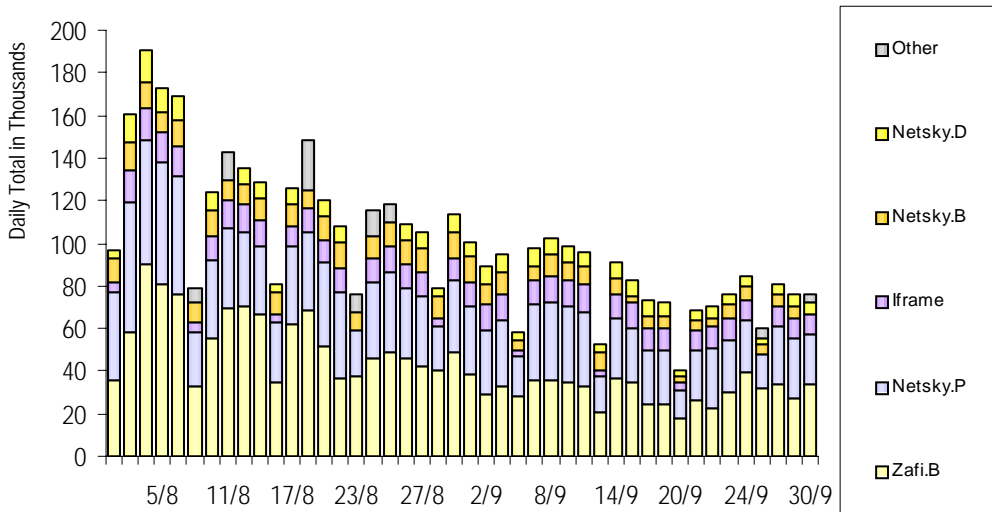
Frequency Band	Characteristics	Typical Applications
Low 100-500 kHz	<ul style="list-style-type: none"> • Short to medium read range. • Inexpensive low reading speed. 	<ul style="list-style-type: none"> • Access control. • Animal identification. • Inventory control. • Car immobiliser.
Intermediate 10-15 MHz	<ul style="list-style-type: none"> • Short to medium read range. • Potentially inexpensive medium - reading speed. 	<ul style="list-style-type: none"> • Access control. • Smart cards. • Library control.
High 850-950 MHz 2.4-5.8 GHz	<ul style="list-style-type: none"> • Long read range. • High reading speed. • Line of Sight required. • Expensive. 	<ul style="list-style-type: none"> • Railroad car monitoring. • Toll collection systems. • Pallet & container tracking. • Vehicle tracking.

VIRUS ACTIVITY

Daily Top Five: viruses captured worldwide by [TrendMicro](#) for August/September.



Daily Top Five: viruses captured worldwide by [RAV](#) for August/September.



RECENT SIGNIFICANT ALERTS & ADVISORIES

REFERENCE	DESCRIPTION	DATE
NISCC	An update to the vulnerability issues in implementations of the H.323 protocol	27/10
Redhat	Fraudulent e-mail & website puveying a trojaned redhat fileutils package	26/10
AusCERT	Multiple vulnerabilities in various tabbed web browsers	21/10
Secunia	Microsoft Internet Explorer two vulnerabilities	21/10
iDEFENCE	Multiple vendor anti-virus software detection evasion vulnerability	19/10
UNIRAS	Likely impact of vulnerabilities patched in Microsoft Security Bulletins MS04-29 and MS04-38	18/10
Microsoft	Buffer overrun in JPEG processing (GDI+) could allow code execution update	13/10
Microsoft	Cumulative security update for Internet Explorer	13/10

Please refer to the [CCIP website](#) for a complete list of alerts & advisories.

DISCLAIMER

While this newsletter 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 newsletter.

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 newsletter in any manner to any commercial product, process or service does not constitute or imply its endorsement or recommendation by CCIP. Views and opinions stressed herein may not be used for advertising or product endorsement purposes.

Please refer to the CCIP website for a list of recent alerts and advisories.



CONTACT DETAILS

Ph: +64 4 498 7654
 Fax: +64 4 498 7655
 E-mail: info@ccip.govt.nz
 Web: www.ccip.govt.nz
 Mail: P.O. Box 12-209
 Wellington
 New Zealand