Edith Cowan University
Research Online

Australian Information Security Management Conference

Security Research Institute Conferences

2011

A longitudinal study of wi-fi access point security in the Perth central business district

Emil Jacobson
Edith Cowan University

Andrew Woodward
Edith Cowan University

Originally published in the Proceedings of the 9th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, 5th -7th December, 2011
This Conference Proceeding is posted at Research Online.
http://ro.ecu.edu.au/ism/118

A LONGITUDINAL STUDY OF WI-FI ACCESS POINT SECURITY IN THE PERTH CENTRAL BUSINESS DISTRICT

Emil Jacobson, Andrew Woodward
secau Security Resarch Centre, School of Computer and Security Sceince
Edith Cowan University, Perth, Western Australia
a.woodward@ecu.edu.au

Abstract

This study collected data in 2008 and 2011 in relation to the level of apparent security of wireless network access points in the Perth CBD. It also compared this data to a comparable study conducted in 2004. The aim was to determine whether businesses were using an appropriate level of encryption to protect their wireless networks. A pre-determined route was followed which traced the Perth CBD and the open source wireless network auditing tool Kismet was used to survey the wireless networks. In 2008, approximately 1300 access points were discovered in the Perth CBD, this number climbing to approximately 3400 in 2011. Of the 1400 discovered in 2008, approximately 30% were open, with 15% using WEP security, with these values falling to 8 and 4% respectively in 2011. In conclusion, the number of APs using WEP appears to have fallen in total and as a percentage of the total number of networks. The number of APs still using WEP and WPA TKIP is concerning, as the technology underlying these security methods is flawed and open to compromise. No significant finding can be drawn in relation to the open access points, due to not knowing whether a VPN or other upstream authentication mechanism was employed.

Keywords
Encryption, Wireless networks, WEP, WPA, Wi-Fi, WLAN

INTRODUCTION

Security issues with 802.11 based wireless networks, or Wi-Fi, have been extant for a number of years, and there really is no valid reason for a business to be operating an unsecured access point, unless it is for the purpose of public access. Open wireless access points (AP) represent a security risk on two fronts. Firstly, they can be used to commit or facilitate crime or even acts of terror. There are numerous examples in the literature of individuals who have used open wireless access points to commit illegal acts. For example, it was reported that open Wi-Fi was used to plan and execute the Ahmedabad and Delhi bombings in 2008. It is alleged that an email sent before the Ahmedabad blast was traced to an open AP belonging to a US resident living in Mumbai, and the email sent before the second blast being traced to a company in Chembur (Gadgil & D'Monte, 2009). Additionally, it is worth noting that subsequent to the bombings, Mumbai Police conducted a major exercise to locate and close down or secure open Wi-Fi access points after that event (Cox, 2009). Another risk factor in this category is of open APs being used to download illegal material. A man in Toronto was arrested in his car whilst downloading and viewing child pornography from an open Wi-Fi AP (Leyden, 2003). Along similar lines, an associated risk factor in this category is being incorrectly targeted as the perpetrator of a crime when an open AP is used for illegal purposes. A resident of Buffalo, in New York was wrongly accused of downloading child pornography, and had his house raided by police because his neighbour had used his open Wi-Fi AP (Thompson, 2011).

The second risk category is that the information exchanged over an open wireless access point is sent unencrypted, meaning that anyone within broadcast range can capture this traffic and use it to extract logon credentials (usernames and passwords), emails, and other personal or financial information. Whilst this may be a risk that most users of Wi-Fi networks are prepared to accept, it would be unacceptable for a business to operate an open Wi-Fi AP which was used to transmit business information. However, there might be some sort of other authentication present, and the purpose of this study was not to map this. Previous studies of the Perth CBD conducted in 2004 indicated that unsecured Wi-Fi was being used, as many APs were detected with company names used as the SSID.

It is not just open access points which are a security risk. There are numerous free, open source tools available which can be used to break WEP authentication / encryption within minutes (Aircrack, 2011). The last few years have also seen methods developed to allow for brute-forcing of WPA/TKIP protected networks, with the CoWPAtty tool being one such example (Wright, 2009). Whilst this is more time consuming, requiring the calculation of the keyspace to be calculated for individual SSIDs, the introduction of GPU based computing has considerably reduced the time taken to complete this task (Anon, 2011).

The aim of this research was to survey the Perth Central Business District to count the total number of access points, and to determine their level of encryption. The study was first conducted in 2008, and then a more comprehensive survey repeated in 2011. The data was analysed to determine the percentage of APs which were open, using WPA or using WPA2.

METHODOLOGY

2004 Survey

The data from the 2004 survey was collected and published by Webb (2004) according to the following procedure:

> **Equipment and Route Used**
> The laptop computer used for all scan rounds was an IBM ThinkPad 600E, 366MHz Pentium II running Mandrake Linux v9.0. The Wireless Network Interface Card (WNIC) was a Cabletron/Orinoco RoamAbout 802.11 DS PC Card. Attached to the WNIC was a directional antenna made from a tin can that gives an 8-10 Dbi gain. The software used to detect the presence of WLANs was Kismet v. 2.6.0. The same route was taken during each scan, travelling approximately 40 kilometres (25 miles) through the CBD of Perth, Western Australia. The CBD occupies an area of approximately 8.75 square kilometres (3.38 square miles) and has an estimated day-time population of 100,000 people (City of Perth, 2004). Each scan took approximately one and a half hours to complete. Limitation of the study include: WPA based equipment was not yet in use at the time of this scanning, and as such, security data is classified as either open or WEP

2008 Survey

The survey conducted in 2008 utilised a Lenovo X61 Tablet running Backtrack 4R2 and used the onboard wireless NIC. Kismet was used to collect the data on total number of access points, and also to determine what type of security was being used by each Access Point operator. This survey was performed in Perth CBD. Limitations of the study include: Data captured by Kismet provided security data as either open, WEP, WEP/WPA or WPA. No further information in relation to encryption method being used is available

2011 Survey

Since the location of this study is the Perth CBD, CAT buses have been used as means of transportation. The stops used were Yellow 21, 23, 25, 28, Red 10, 22. The researcher walked between Yellow 28 and Red 10, and between Red 22 and Yellow 21.

This survey has been carried out using a Dell INSPIRON Mini 1018 netbook, it's built-in network adapter, the operating system Ubuntu 11.04, and a built-in wireless sniffer called Kismet. The scans have been performed on Thursdays, every other week from August 4th, until October 13th between 12pm and 3pm. The results have been recorded using Kismets own log files, and these files have been analysed using Microsoft Excel 2010. The networks in this study have not been connected to, Kismet is a passive tool. No information about the networks other than their encryption will be published, and the log files from the scans will be deleted on publication of this report.

Limitations:

- Since the CAT buses run at a certain speed, this might cause some access points to be missed by the scan.
- Geographical limitations: Only Perth CBD will be scanned. Havelock St to the West, Wellington St to the North, Bennett St to the east and Hay St to the South. For a more detailed map, see Appendix A.

RESULTS

The total number of access points detected in the Perth CBD between 2004, to 2008 to 2011 is presented in Figure 2. It can be seen that there is an upward trend in terms of total number of access points from 2004 to the most recent scans. Another observation is that although the number of open APs appeared to increase between 2004 and 2008, the number of both WEP and open devices fell as a percentage of the total over this time.

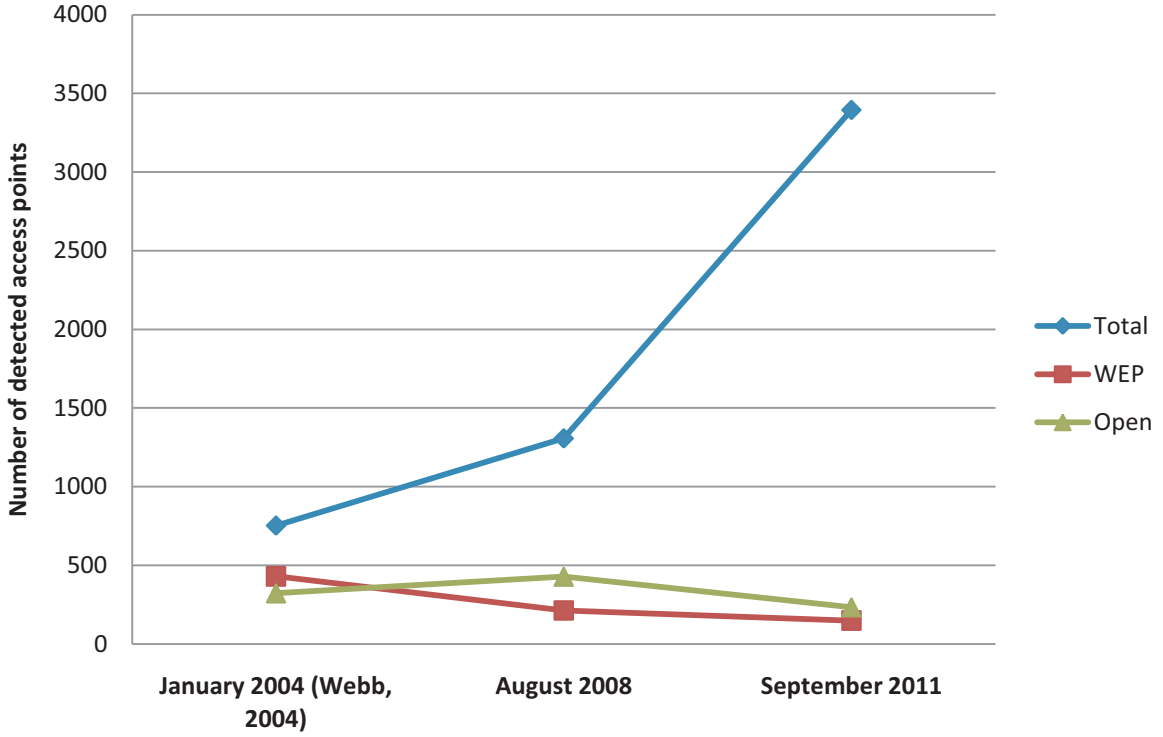

Figure 2: Total number of detected access point in the Perth CBD as surveyed in 2004, 2008 and 2011. These numbers may not be truly representative as paths followed varied slightly between each scan year

The percentage breakdown in terms of Wi-Fi AP security is shown in Figure 3. This indicates that the number of open access points and WEP protected networks has fallen significantly over time, whilst the number of WPA protected networks as a percentage increased from 2008 to 2011. WPA was not introduced until later in 2004, and thus is not represented in the chart.

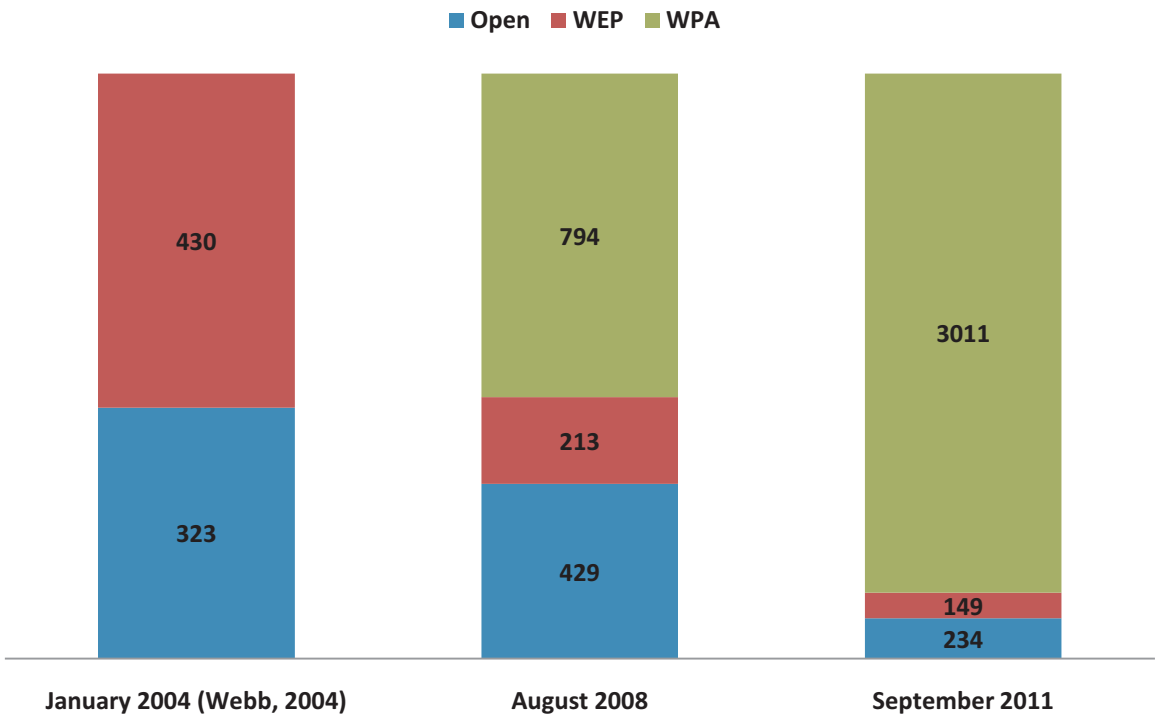

Figure 3: Breakdown of numbers as a percentage of total of Wi-Fi access point security type employed by users of Wi-Fi in the Perth CBD between 2004 and 2011. WPA was not introduced until later in 2004.

The specific type of encryption (as opposed to authentication) in use by Wi-Fi APs measured over an eight week period is given in Figure 4. Data presented is the average of six scans. This illustrates the individual security mode employed with greater granularity. It can be seen that there while there are some APs which are open, and there are relatively few devices using WEP. Of significance here is that although a large number of devices are using WPA, they are using PSK/TKIP mode which is vulnerable to attack. Although some reasonable numbers of devices are using AES-CCMP for encryption, it is not known whether any of these devices are using 802.1x / EAP authentication, which is a more secure mode of operation. The last two columns, WPA+PSK and WPA+TKIP could effectively be grouped together as they are using the flawed four-way handshake method of protection.

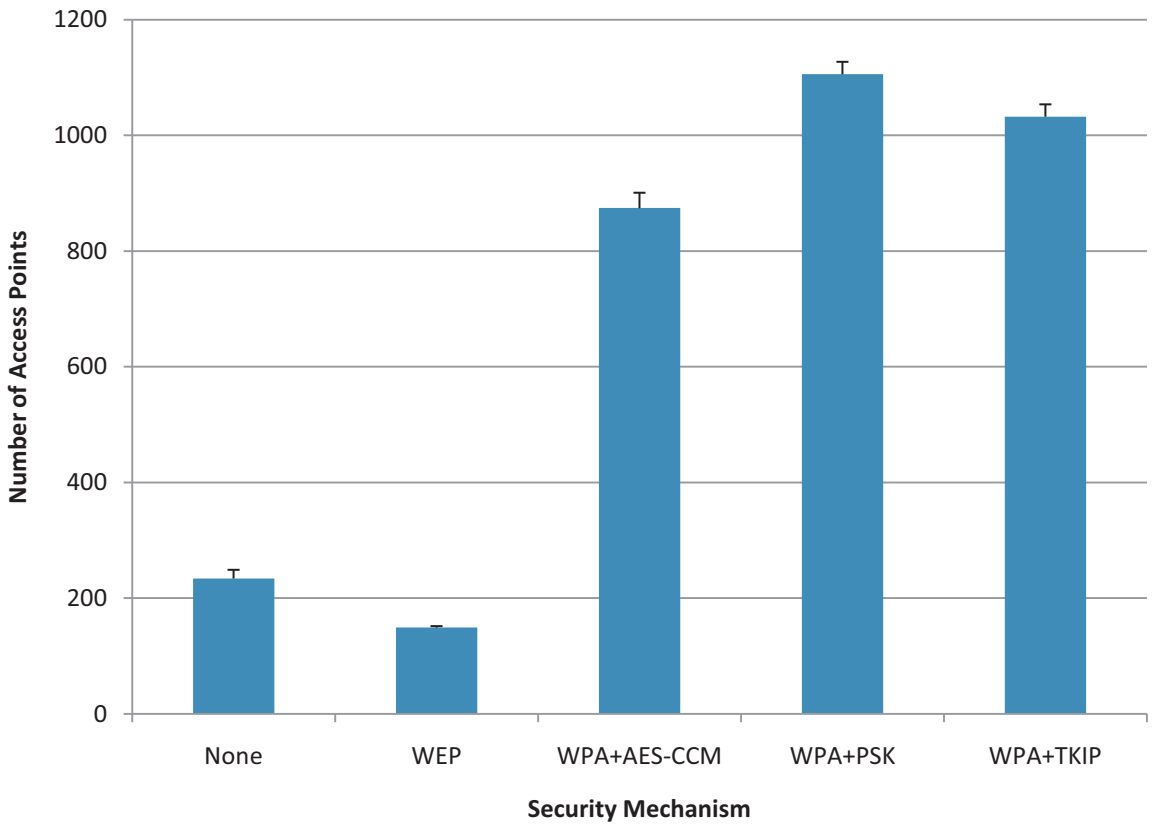

Figure 4: Average of six scans in 2011 showing numbers of Wi-Fi access points detected in the Perth CBD represented by the security mode that each AP was operating in. Vertical bars are standard errors.

DISCUSSION

One of the more positive results of this investigation was that over the period of time from 2008 to 2011, the number of both open and WEP protected Wi-Fi networks fell significantly. Given the reasons stated above in relation to the security, privacy and legal issues, it is a good outcome for security that the number of unsecured devices has fallen. Whilst a reasonable number of the Wi-Fi networks detected are likely to be for private use, it is a reasonable assumption, and one used in this study, that the majority of Wi-Fi networks detected belong to business. As such, it is also a reasonable assumption that they would have the financial and technical resources to at least be using WPA-TKIP based authentication, if not full enterprise 802.1x / EAP mutual authentication with RADIUS.

It is also reasonable to assume that those devices which are open are either Wi-Fi hot-spots, or are employing some other security mechanism. During the infancy of Wi-Fi, and before the finalisation of the 802.11 standard (IEEE, 2004), using open or null authentication with a VPN to authenticate and encrypt traffic was a fairly standard practice. Given the issues with the four way handshake which is a known vulnerability with WPA personal mode, protecting a Wi-Fi AP in this fashion is still acceptable from a security perspective. However, the type of VPN technology used must be carefully considered as some have weaknesses e.g. clear text passwords.

One would hope at this point that with the duration of time that Wi-Fi has been in mainstream use that any open access point has been deliberately left open for public use, and not done so through lack of knowledge. Additionally, given that WEP has been broken for a decade (Fluhrer, Mantin, & Shamir, 2001), there really is no excuse for using WEP as a means of authentication or encryption. Given that its cryptographic mechanism is so flawed, and that it can be broken so easily, it only serves to provide a false sense of security. In addition to some businesses providing free open Wi-Fi for their customers, there is a belief amongst some in the community that you should leave Wi-Fi open for others to use. Schneier has stated openly that he leaves his own Wi-Fi open for others to use, equating it to basic politeness such as offering a cup of tea (Schneier, 2008). He goes to further state that he believes the risk to him of such activities as stated above are minimal. The Electronic Frontier Foundation also supports leaving Wi-Fi APs open for other to use, and is publicly pushing for operators of Wi-Fi devices to make them open (Eckersley, 2011). They argue, and with valid grounds that not being able to operate open Wi-Fi which is at the same time encrypted, adds a risk to using open Wi-Fi, namely that of eavesdropping, or from an information security perspective, confidentiality. Whilst these are examples of leaving wireless open for positive reasons, leaving Wi-Fi open can also be used to create reasonable doubt for those owners of Wi-Fi who are using them for illegal purposes. There is evidence of such behaviour in the literature with one example becoming known as the "cheerleader defence". Tammie Marson of California was accused of having illegal music files on her computer, as the evidence lead investigators to the IP address belonging to her Wi-Fi AP. Her defence was that she was a cheerleading coach, and that she frequently had people coming through her home, and that any one of them could have done it (Robertson, 2006). The music industry eventually dropped the lawsuit which they had lodged against her, but relying on open Wi-Fi to cover your illegal activity is not to be encouraged.

Also of interest is the increase in the total number of recorded Wi-Fi networks. An initial scan of the Perth CBD undertaken by Webb in 2004 discovered a total of 735 Wi-Fi APs in a scan conducted in January of that year (Webb, 2004). This number increased to approximately 1400 in 2008, and increased again to almost 3500 in 2011. Given that there are only three non-overlapping channels available to co-located APs, and with so many EM radiating devices in such a small area, and with so little EM spectrum available to them to operate in, there must be a great deal of interference. Additional devices added to this area must be a diminishing return, and only serve as a source of interference to those devices already operating. This can in turn create a problem from an information security perspective, namely that of availability. Two APs operating in the same area on the same channel may be able to cohabit with little issue, but if usage of one of these devices is to increase, it may prevent the other AP from being able to communicate with its clients. As such, these devices would have no connectivity, and hence the availability of the network has been prevented. It would effectively be what is known as an unintentional denial of service.

The discovery of vulnerabilities in the four way handshake employed by WPA-TKIP mode leaves users of this type of authentication / encryption vulnerable to attack. Although it is a longer and more complex process to break this form of security as opposed to WEP, it should still be considered a greater risk to an organisation to employ this mode of security as opposed to 8021x based mutual authentication. The increasing use and subsequent decreasing cost of cracking Wi-Fi keys using general purpose GPU (GPGPU) computing makes this an increasing threat. There are technical and resource implications of using so called enterprise mode WPA security, but these must be balanced against a formally risk assessed use of WPA-TKIP security.

CONCLUSION

The data presented in this paper shows that the number of Wi-Fi APs being used in the Perth CBD has increased fairly significantly in the last seven years, and that the number of devices using both WEP and no security has decreased. Wi-Fi devices were still in their infancy in 2003, and the final version of the 802.11i standard known as WPA was not released until later in 2004.

It is difficult to make too much of the small number of open APs given that these may be either public Wi-Fi hot-spots, or they may be null authentication devices utilising some other security technology such as a VPN to prevent access to upstream networks. It would be a good outcome from a security perspective if all of the open devices detected fall into one of these two categories.

The decline in the number of devices that used WEP was encouraging, as this security protocol can be readily defeated by freely available tools. Anyone, and any organisation in particular, that is relying on WEP to protect corporate or sensitive information is accepting a risk which they would have a difficult time in justifying. Even continued use of WPA/TKIP based security will start to become difficult to justify from a risk perspective, as GPGPU computing is making this security measure weaker.

Future research will undertake annual scans of the same location in the Perth CBD to examine whether the trends uncovered in this research to date continue, and to examine the number of devices using insecure protection.

REFERENCES

Aircrack. (2011). Aircrack-NG. Retrieved October 6th, 2011, from http://www.aircrack-ng.org/

Anon. (2011). Pyrit. Retrieved October 6th, 2011, from http://pyrit.wordpress.com/

Cox, J. (2009). Police in India sweep for unsecured Wi-Fi networks. Retrieved October 6th, 2011, from http://www.techworld.com.au/article/273312/police_india_sweep_unsecured_wi-fi_networks/

Eckersley, P. (2011). Why we need an open wireless movement. Retrieved October 11th, 2011, from https://www.eff.org/deeplinks/2011/04/open-wireless-movement

Fluhrer, S., Mantin, I., & Shamir, A. (2001). Weaknesses in the Key Scheduling Algorithm of RC4. Selected Areas in Cryptography. In S. Vaudenay & A. Youssef (Eds.), (Vol. 2259, pp. 1-24): Springer Berlin / Heidelberg.

Gadgil, M., & D'Monte. (2009). Mumbai police plug Wi-Fi security holes. Retrieved Thursday 6th October, 2011, from http://www.business-standard.com/india/news/mumbai-police-plug-wi-fi-security-holes/00/56/346002/

IEEE. (2004). IEEE 802.11i-2004: Ammendment 6: Medium Access Control (MAC) Security Enhancements. USA: IEEE.

Leyden, J. (2003). Wi-Fi hacker caught downloading child porn. Retrieved October 6th, 2011, from http://www.theregister.co.uk/2003/11/26/wifi_hacker_caught_downloading_child/

Robertson, S. (2006). Do not try the cheerleader fefence. *Out-Law, 15,* 5475.

Schneier, B. (2008). My Open Wireless Network, *Schneier on Security* (Vol. 2011).

Thompson, C. (2011). Bizarre pornography raid underscores Wi-Fi privacy risks - Password-protect your wireless router, or risk falling victim to villains Retrieved October 6th, 2011, from http://www.msnbc.msn.com/id/42740201/ns/technology_and_science-wireless/

Webb, S. (2004). *Growth in the Deployment and Security of 802.11b Wireless Local Area Networks in Perth, Western Australia*. Paper presented at the Australian Computer, Network & Information Forensics Conference.

Wright, J. (2009). CoWPAtty. Retrieved October 6th, 2011, from http://www.willhackforsushi.com/?page_id=50