Network Security and Wireless Networks

Alec Tunbridge

November, 2002

Precis of *The Economist* Article *Keeping out the Kaos Club* [3]

Computer security is lax and the problems that this poses will only be exacerbated by the growth of computer networks. There have been many recent high-profile attacks such as the repeated breaches of NASA’s network by the Kaos Club, a gang of crackers from West Germany. A modern OS has around 6 million lines of code and ensuring that there are no flaws within it that can be maliciously exploited is a considerable undertaking. In an attempt to quantify the security of operating systems the American government has developed a simple classification which ranges from A (most secure) to D (least secure). Very few current systems rate above a grade C and those that do tend to be less user-friendly. Higher grades have mechanisms which assign security clearance to individual files and explicitly check their activities, rather than relying upon the user’s password. There are however some important minor improvements that can be made to enhance security, such as ensuring that deleting a file removes its data not just its directory entry. Aside from being less easy to use secure systems also carry a considerable overhead, actually reducing the resources available for real computation.

Issues of national security can further complicate the implementation of secure systems. Governmental insistence upon high security can hamper productivity and inhibit legitimate access, especially if different nations adopt incompatible protocols. Furthermore many fear that government involvement in specifying their secure systems may compromise their civil liberties by granting agencies access to their private data through the back-door.

The Current State of Affairs

As predicted the problems arising from flaws in computer security have multiplied many-fold. In the late 80’s The Internet was in its infancy and cracking was largely the province of individuals with plenty of time on their hands and a modem. The term War Dialing was coined to describe the process of systematically dialing phone numbers with the hope of finding a computer offering
a connection that could be exploited [11]. The advent of The Internet made such techniques unnecessary as simple programs known as port scanners became available which could systematically work through IP addresses scanning all the services which they offered and thus exposing their weaknesses. Along with a proliferation in the number of inter-connected computers the systems themselves became much more standardized. Gaining illicit access no longer required hand-crafted tools but generic exploits could be written potentially affecting millions of users. Many of these methods are relatively simple, for example there has been much press attention devoted to so-called script-kiddies. These children in their early teens have mounted attacks upon major institutions with considerable success using only a modicum of knowledge and some freely-available tools [7].

The security of operating systems is of continuing concern. Whilst the classification system mentioned in The Economist article has been super-ceded there are continuing American efforts to certify machine security [5]. Their program has the benefit of involving several nations, e.g. Britain, France and Germany, thus hopefully avoiding compatibility issues. It is perhaps the sheer connectivity of networks though that poses the greatest threat to security.

The Internet is not the only new technology to shake the foundations of system security. The last few years have seen rapid growth in the area of wireless networking, mainly using low-power radio communications to provide network communications over short distances. The concept of a wire-free connection is quite seductive, whether for facilitating business practices in a roaming environment, or merely reading your email from the sofa. Indeed there are some projects using this technology to provide high-speed Internet access in otherwise unaccessible areas, eg. the Edenfaster project [4]. There is even a movement promoting the advertisement of open wireless access points called War Chalking which has designed a special set of symbols to describe such nodes (Fig. 2).

Such schemes evoke the pioneering days of the net when access was to be free and unlegislated. Unfortunately that very lack of regulation runs contrary to the interests of security. Keeping a network secure relies upon being able to identify and restrict users and their activities, whereas wireless networking is the “equivalent of placing an Ethernet port in the parking lot” [8]. War Dialing has been supplanted by War Driving, the process of driving around town with a wireless-equipped portable and a suitable aerial (Fig. 1) seeing whose networks can be accessed.

**Current Wireless Standards**

The current dominant standard for wireless connections is IEEE 802.11b [9] more commonly known as Wi-Fi. The protocol includes various security measures such as Wired Equivalent Privacy (W.E.P.) which as its name suggests attempts to provide a similar level of protection to conventional wired connections. The encryption system employed uses a common private key shared by all nodes which is combined with an initialization vector to generate a pseudo-
random stream cipher. This cipher is then XORed \(^1\) with the data before being transmitted wirelessly to the receiver who then repeats the XORing process to retrieve the data. However there are some fundamental flaws in the implementation of this system that seriously compromise its effectiveness. The size of the initialization vector is small and its value is sent “in the clear” meaning that passive monitoring of traffic will eventually intercept several messages encoded with the same stream cipher. Combining these messages can yield the secret shared key value and enable subsequent decryption of all traffic by a third party. Indeed there are several applications freely available on The Internet which offer this means of decryption, e.g. AirSnort a Linux utility which claims to be able to overcome W.E.P. after monitoring 5-10 million packets (less than a day’s worth of traffic). There are several more specific attacks to which Wi-Fi is vulnerable \([1]\) all of which could be seriously compromising. Defenders of the protocol claim such attacks are highly specialized and unlikely to occur. Furthermore they stress that W.E.P. is precisely that, a means of providing security equivalent to wired connections which themselves are only a single element within a comprehensive secure system \([6]\). The detractors claim that while this might be so the security of the current system could be improved dramatically by resolving its implementation. Despite this debate the greatest flaw in many systems is that they fail to even activate the safety-meaures that are available for their wireless nodes. Even though current counter-measures have their weaknesses they are infinitely preferable to no encryption at all which is often the default setting for new equipment.

**The Future**

There are already schemes to improve the W.E.P. encryption system which will be commercially available within six to twelve months. For the mean-time it is perfectly possible to use Wi-Fi with an acceptable level of protection for most applications. Secure end-to-end transmission can be achieved using the higher protocol layers to encrypt traffic using tools such as ssh \([10]\) or even establishing a Virtual Private Network \([2]\). Unwanted users can be denied access by fire-walling wireless access points in a similar manner to conventional untrusted networks.

Other wireless protocols are also on the horizon. The much hyped Blue-Tooth is already commercially available for specific applications such as data-communication with mobile phones and there are enhancements in the pipeline for 802.11. With the increasing diversity and popularity of wireless communications, security concerns can only grow. The fact that many wireless-enabled devices are portable means that the threat of simple theft poses a real risk \([8]\), especially given forthcoming advancements in phone technology such as 3G.

Security exploits and fixes are always in a kind of dynamic equilibrium. Systems are sufficiently complex and rapidly changing for there to always be loop-holes needing patching. The key is to be aware of a system’s limitations

\(^1\)Logical exclusive or
and ensure that its security is at least up-to-date. Ultimately computer security systems are not that far removed from the more mundane physical protection installed in an individual’s car or home. Much of their function is to deter intruders from attempting to break in and divert their interests to other softer targets. The determined will always find a work-around.

References

[1] Intercepting mobile communications: The insecurity of 802.11. WWW, 2002. DRAFT.