Advanced videogame consoles – a new and unrecognised threat to secure service provision?

James Reed
SPECIALIST REGISTRAR IN FORENSIC PSYCHIATRY, REASIDE CLINIC, BIRMINGHAM

Nicholas Taylor
CONSULTANT FORENSIC PSYCHIATRIST, EAST MIDLANDS CENTRE FOR FORENSIC MENTAL HEALTH

John Mackay
IT SYSTEMS MANAGER, EAST MIDLANDS CENTRE FOR FORENSIC MENTAL HEALTH

ABSTRACT

Games consoles are ubiquitous in the community, and increasingly in demand in secure forensic psychiatric settings. They contain a range of sophisticated technologies, which may pose a significant security risk, including provision for secure wireless communication, Internet access, playing and duplication of video and audio discs, and storage of large amounts of potentially worrying video and audio content. Staff awareness of this risk is limited by ignorance and the perception that games consoles are 'toys' for the use of children and adolescents. This paper highlights the risks related to specific machines and provides guidance on effective management of these risks.

KEYWORDS

security; technology; video games; risk assessment

Introduction

Games consoles, once the preserve of technological enthusiasts and children, now have wide appeal. Current examples include Sony's PlayStation, Microsoft's Xbox and the newer Nintendo Wii. The industry surrounding them is worth many billions of dollars, on a par with the film industry. They are ubiquitous in the community at large and, as a result, many inpatients in secure forensic psychiatric units are likely to possess or wish to purchase a games console.

Requests of this nature may be granted by clinical teams with little knowledge or experience, and little thought may be given to the security implications of these complex machines. The technology contained in games consoles has changed dramatically over recent years, and it is now at a stage where it has potential security implications for secure settings.

History

Electronic games are almost as old as computer technology itself. A version of 'tic-tac-toe' (noughts and crosses) was written for a very early electronic computer in 1952. Games were, initially, of strictly academic interest, but the potential for commercial exploitation was quickly realised. The first home computer game system designed to connect to a television was launched in 1972, beginning a trend which continues to the present day.

Computer games have, traditionally, had a reputation as children's entertainment, and games for home computers were marketed for (and frequently produced by) the under-18s. For many years, graphics took the form of crude and often cartoon-like images. Companies such as Sega and Nintendo marketed gaming consoles of increasing sophistication, but they remained a concern of young people. This changed with the launch of the Sony PlayStation in 1994, which was marketed largely to adults and was accompanied by a range of games with noticeably more mature themes. This strategy was extremely successful, and spawned an entirely new market.

Games consoles have always been sold as game-playing appliances, distinct from personal computers, which are more versatile, expensive and complex. Early games consoles used cartridges to load games, but the PlayStation introduced compact discs as the primary means of loading software. It also began a trend of including existing appliances (such as a CD player) as part of the console which has continued to the present day. The level of technical sophistication in modern consoles is now far in excess of most desktop personal computers, and this may pose very significant risks to security if not well understood.

Technologies of risk

DVD drives

DVDs (or digital versatile discs) have now replaced the VHS tape as the standard means of distributing video, and almost all game consoles come equipped with a form of DVD drive. Most currently have the capacity to read DVDs, but technology for writing to DVDs is widely available and may be incorporated into consoles in the near future. This would provide potential to duplicate discs. The data capacity of a DVD is very large, an individual disc holding as much as six hours of video, albeit of relatively poor quality. So-called 'high definition' DVDs can store substantially more (up to 60–70 hours at similar quality). The new Bluray DVD format cannot be used in standard DVD players and is relatively rare, so it could prove difficult to examine the content of such discs. They can, however, be played using the Playstation 3 console.

The potential for security breaches is clear. DVDs can be perfectly legitimate, but they could very easily be used as a means of smuggling in banned material (such as violent, sexually explicit or paedophilic images or video) disguised as acceptable material. Such material could be stored in a format (encrypted) which would be difficult for staff to detect. As DVD writers become more common as accessories to consoles, it is possible rapidly to duplicate and distribute such material within the confines of a secure unit.

USB connections

The USB (universal serial bus) is a standardised connection universally used by personal computers. It allows for the connection of a range of devices (including scanners, cameras and keyboards) to a computer. One of the most important uses is the connection of high-capacity storage devices, particularly pocket-sized devices (known as 'USB sticks', 'key drives' and so forth). These have recently shown a dramatic drop in price, accompanied by a dramatic increase in capacity. It is now possible to store amounts of data comparable to many DVDs on such a tiny, postage stamp-sized device. Other USB devices might also be of concern; it is now common to find small USB devices which add the capability for wireless data connections (see below).

USB drives provide another easy means of concealing large amounts of prohibited material in the form of videos, pictures or other data (including instructions on weapon or bomb making, readily obtained from the Internet). The drives themselves can be very small, light and robust, and could easily be concealed in very small spaces, including in opaque liquids, which are unlikely to damage them.

Wireless communications

The ability to connect computers together using high-speed wireless links is commonplace. This technology has more recently found an application in games consoles, often being used in conjunction with the capability for Internet access or to allow a connection with other games consoles to allow multi-player gaming. This can allow secure and practically undetectable communication between similar machines (akin to a walkie-talkie), allowing

exchange of messages and transfer of data. These consoles are usually able to connect to the Internet, given an appropriate gateway. Owing to the general public's poor understanding of the security measures on these devices, unsecured systems are plentiful and easily exploited. This provides the potential for a patient with access to a games console (plugged only into an electrical socket, with no extra equipment) to have free access to the Internet using a wireless connection in a nearby house or office.

Using such technology, patients with appropriate equipment could easily establish a clandestine communications system which might be used to subvert security in any number of ways.

Console accessories

As described above, many of these technologies are still developing and may not be included as standard features of a games console when purchased. However, they are often made available as accessories which can be added to existing equipment. For example, wireless networking can often be added using a small (and apparently innocuous) USB device which simply plugs into an existing console.

A further risk is found in the form of memory cards used to store data. These have effectively replaced floppy discs as the most common storage medium. As many readers will be aware, these (often tiny) devices can store enormous amounts of text, video, audio or other information. The Nintendo Wii console can be used to access and display information from these devices.

Management of risks

Given the range of new and potentially serious risks which might be posed by games consoles, it is important to consider how the threat could be sensibly managed. A policy of outright prohibition is likely to be unpopular, and may not be necessary. Many consoles (like Nintendo's Wii) have 'parental control' functions designed to prevent children from accessing some of the functions (for example to restrict Internet access). These could be used before the patient is given the device, and as a condition of its being permitted. Any items with high-risk capabilities which could not be disabled reliably would need to be strictly controlled or prohibited. The policy on games consoles should be exactly that applied to DVD players, TVs and so on. In many secure units they are allowed only in communal areas, and allowing unsupervised access to consoles in bedrooms may increase the possibility of abuse.

Increased awareness of these matters is essential among clinical and security staff. In most prisons USB devices are banned, but this is often not the case in secure hospitals. Staff may not always be well briefed on the forms these devices can take, and what the risks are.

The possibility of accessing the Internet over local unsecured wireless networks must also be investigated. This is accomplished relatively easily using standard equipment, and neighbours may need to be given appropriate advice if unsecured networks are found. Were illegal material to be accessed using their network connection, it might be very difficult for them to prove that they had not themselves been responsible for it!

Finally, staff need to stay up to date. Technology continues to advance rapidly, and it is only by being fully aware of what is available and how it could be used (or abused) that staff can be confident in the security of the unit.

There has been some recognition of these threats by the Department of Health. The Ashworth, Broadmoor and Rampton Hospitals Amendment Directions (DH, 2003) specifically restrict access to 'games consoles that can be adapted as a computer'. However, at what point a console is considered to be so adapted is not clear, and it is arguable whether any modern console would be excluded by this direction.

Game content

An associated and very controversial issue when discussing this area is the content of the games themselves. It is now possible to buy from mainstream retailers games which accurately and realistically portray, among other things, the experience of being a professional hitman, the maker of a 'snuff' movie or an organised crime professional. There are often strong violent and sexual themes in many of the games produced, which often carry an '18' certificate. There is little consensus on the impact on individuals of playing games such as

these, but it must be questioned whether it is appropriate for inpatients in a psychiatric unit who may have committed such crimes in reality to be allowed ready access to such material.

Conclusion

Games consoles are no longer simply 'kids' stuff'. They pose a range of challenges to security in psychiatric units, which are likely to increase as technology becomes more sophisticated. To counter this threat, a robust and pragmatic approach is needed that is founded on a sound knowledge of what is available and how it might be used.

A similar neglect of available technologies and their potential uses was uncovered in the Fallon Inquiry (1999); it would be a tragedy if it took a further inquiry for this issue to be addressed properly.

References

DH (2003) *The Ashworth, Broadmoor and Rampton Hospitals Amendment Directions.* Available from: www.dh.gov.uk/en/Healthcare/NationalServiceFrameworks/Mentalhealth/DH_4108513 (accessed 24 November 2008).

The Fallon Inquiry (1999) *Report of The Committee of Inquiry into the Personality Disorder Unit, Ashworth Special Hospital.* London: Stationery Office.