DATA SECURITY THREATS IN THE HOME ENVIRONMENT

Tony Proctor
School of Computing and IT, University of Wolverhampton, U.K.

Abstract: The aim of this paper is to assess the relevance of data security in the home environment and to identify the nature of vulnerability. At the time of writing most data in the home is stored manually. The widespread use of the Internet, home pc's and mobile devices now means that increasingly individuals (and families) are storing "home information" electronically. It is highly likely to be a trend that continues. Information on specific data security related issues is widely available in terms of "how to protect your pc" and there are also many products that are available to assist with this. The level of actual understanding that home users have of the general data security issues and the means that they take to protect themselves are not well documented. The approach taken in this paper is to look at many of the data security threats posed to existing ICT devices and to put them in the context of systems that are currently used or may be used in future, in the home environment. The paper clearly defines that it is not concerned with the broader topics of data assurance (which would include fire, flood etc). The primary focus is the potential for malicious acts being committed by unauthorised use of the systems. Where are the threats from and what can be done to alleviate them? Are the main vulnerabilities in the connectivity, the systems, or both? Since technology now softens the "environmental" boundaries, this paper alludes to the scope of the home environment. It also discusses existing solutions to perceived threats; whether they appear to be understood and whether they appear to be working. It looks for the evidence to demonstrate the significance of data security in relation to the development of "intelligent homes". The paper then takes into consideration the directions in which technology appears to be developing in arriving at conclusions.

Key words: home security, data integrity, threats.

A. Sloane (ed.), *Home-Oriented Informatics and Telematics*

1. SCOPE OF THIS PAPER

A broader discussion of data assurance that could address issues such as fire, flood, system availability and resilience are outside of the scope of this paper which is concerned with the committing of malicious acts through access to technology. It is also worth noting that the increasing proliferation of technology will result in the increasing use of hardware that in itself may be of high value and hence increase the likelihood of robbery and burglary in order to steal these items. For the purposes of this paper the consequences of the theft of the data will be considered but not theft of the hardware itself. The paper will not consider the issue of hoax relating to technology. There are many web sites that describe this (a good example can be found [6]). It is not a reality and any consequences are as a result of psychology rather than process.

The scope of this paper does not allow for the discussion of the threats and preventative measures for manually held data. The degree of the perceived threat to an individual probably varies (some people may destroy utility bills, bank statements by the use of a shredder or burning, others may simply bin them). Increasingly we are being encouraged to bank on-line and pay our bills on line. This suggests that the manual storage of information will be less of an issue than electronic.

2. WHY IS DATA SECURITY AN ISSUE?

The growth of the internet and increasing use of computers in the home has raised the importance of data security in home computing. Some recent forecasts [14] indicate that 75% of UK households will have access to the internet by 2011 and that this access will be by a variety of different devices.

Fifteen to twenty years ago data security was little more than making sure that systems had adequate backups. It was also a technical activity performed exclusively by System Administrators and not a personal activity undertaken by a non technical person in the confines of their own home.

In recent times we have encountered many attempts to compromise computer systems; from writers of virus software to what might be termed cyber terrorists. Over time, the profile of the hacker is changing from a realm of "young geeks" to a more mature IT Professional using their skills to engage in criminal activity. Technology now enables traditional crimes to be committed more easily and is also facilitating new crimes.

Hackers are able to exploit the inherent weaknesses in operating systems. The innumerable combinations of hardware and software means that it is not possible to test new releases to "anything like destruction" and hence

operating system patches are released to close the door to the "hacks" that have opened them. Modern operating systems have many millions of lines of code. This increasing complexity of software exacerbates the problem.

From time to time the national media focuses on or exposes Information Security breaches, typically involving fraud. Often this involves corporate data, but the number of examples involving personal data is likely to increase. As the number of devices capable of storing data increases, the amount of personal data that we store electronically will also increase. Personal Digital Assistants (PDA's) and other wireless devices also present particular problems for data security.

Finally, high security and high usability are "mutually exclusive". This suggests that there is a compromise to be made between the two and this is of commercial significance to the developers and suppliers of these devices.

3. HOW IS THE "HOME INFORMATION ENVIRONMENT" CHANGING?

Just as we are more able to carry our work home with us, we are becoming increasingly able to carry some aspects of our home outside with us. Originally, devices like the telephone and home computer were strictly "home bound".

Technology is thinning the boundary between our working and domestic lives. From individuals who run a business at home to teleworkers and the many people who take work home or occasionally work at home for their convenience. ICT is the enabler, since electronic data is highly portable.

Technology that was once home-based is being used in more "creative" ways. For example, the ability to track individuals through their mobile phone (example service [13]). One of the typical functions that this could provide is for monitoring the location of family members at all times.

4. WHAT ARE THE EXISTING THREATS?

One of the main fears that individuals tend to be aware of in terms of technology crimes is fraud, "*concerns over security are stopping six million people in the UK from banking online*" [3]. Fraud is often the end product of many different, often complex computer related criminal activities. These include:

- Identity Theft. The fastest growing crime in the UK [5]. "Stealing identity to fraudulently obtain money from bank accounts, claim benefits or obtain false documentation (e.g. passports). Identity theft is used in a variety of crimes from banking frauds to people trafficking. Currently the majority of cases are accomplished via a non-technological means.
- Credit card theft. Data is normally obtained via a physical method e.g. robbery, observing a user at an ATM, installation of recording devices at ATM's rather than via the web.
- Hacking. Destruction of data, loss of service, use for third party attack (many users are unaware of this concept).
- Harassment. e.g. blackmailing and stalking
- Paedophilia. a complex threat associated with examples of a type of new crime only possible because of the Internet; such as "Grooming" and encouraging children to produce their own pornographic images, discussed by [11].

There is also a growing knowledge of and concern regarding the use of "spyware" which is one of the more recent IT security threats to be given media coverage [9].

4.1 Device or Connectivity, Where is the Threat?

Whether the threat lies in the systems or their connectivity is an issue worthy of discussion. The table in Fig. 1 helps to identify some of the more obvious systems, threats and whether they result from the systems or the environments to which they connect.

The information presented in Fig 1 identifies that the majority of threats are associated with connectivity. This is a problem that will magnify with the increasing usage of broadband and hence "always on connectivity".

Further examination shows that both devices and connectivity have vulnerabilities. Any device or medium that is capable of storing or processing data is potentially vulnerable. Where processing takes place there is a need to ensure that

- the processes are legitimate (I.E. these processes are allowed)
- change is controlled (I.E. only authorised changes are allowed to legitimate processes)

Device	Main Potential Threat(s)	Typical Vehicle for Delivery	Device (D) or Connectivity (C) Threat	Preventative Measures
Desktop PC	Altering of the way the system works to its detriment and / or the destruction of data.	Virus / Trojan / Worm Program installation or use of external storage devices	C & D A virus etc. is likely to be downloaded in some form but could be on removable media)	Regularly Updated AV / Firewall/ Spyware detection software. Care in the choice of software. Care in use of removable media
	Fraud E.G. fishing (Obtaining banking details in order to commit theft)	Web Page Rogue Program	C	Familiarity with site and procedures used by bank etc.
	Hacking; altering the way the system works to it's detriment and / or destroying / altering data by unauthorised access rather than by a virus	Cookies Rogue Programs Port Scanning / Wardialing Network / Telephone taps Inadvertent disclosure	C & D	Firewall/ Spyware detection software. Use of passwords and encryption where available. Keep login codes & passwords secret. Caution when being asked for any information relating to login codes / passwords etc. Loading of operating system patches as available. Disabling some operations (where appropriate)
Laptop	As Desktop PC	See Above		
	Portability of device	Physical Theft	D	Hide device when in transit. Use of passwords (inc. BIOS password)
PDA	Most of the threats listed for laptop also apply Less secure, as you cannot use BIOS passwords.	Most of the vehicles for delivery listed for laptop also apply	C & D	Most of the preventative measures listed for laptop also apply. However these may be less widely available for PDA's.
Phone	Unauthorised Use	Theft Virus / Trojan / Worm	C	

Figure 1. Threats, Sources & Prevention

4.2 Use of Existing Deterrents

The main categories of existing deterrents are the use of login codes & passwords, anti-virus S/W, Firewalls, encryption and physical deterrents like locks and keys.

As the major supplier of computer operating systems in the home, Microsoft offers a lot of information on security for home computing. Examples at the time of writing [10] are the top tips;

- to use an internet firewall
- get computer updates
- use up to date anti virus software

Implementation of these suggestions is often not straightforward for a computer professional or enthusiast. In theory it represents sound advice, but it would be interesting to discover how widely are they used and how well they are understood?

A preliminary survey (to provide an answer to the previous question a more rigorous study would be required) by the author from a random sample of 20 (non IT professional / non IT enthusiast) home users has indicated that;

- 5 % installed Firewall software
- 10% update their OS patches
- 75 % installed anti-virus software

Furthermore, most users in the sample were aware of the risk of viruses. Many had some idea of the purpose of a firewall (some of those talked about parental control with regard to this question). Some confusion regarding computer updates was apparent.

Even IT Professionals require discipline in order to keep up with the latest patches & releases of virus checkers, firewalls and operating system. It is also possible that installation of the latest release in order to prevent a potential security breach that hasn't yet been encountered by the user can result in the apparent failure of existing applications.

5. SECURING A DEVICE

A simple experiment was conducted by the author which demonstrated that a *reasonable* level of protection can be achieved in a short time provided that the user has a *basic* level of knowledge (words in italics may be subjective in definition and further study would require this to be defined); Firewall

protection was achieved in 10 minutes, antivirus protection in 5 minutes (details in the Appendix). In both cases the user was asked questions which could be challenging for the non-technical (although defaults were provided for most choices). The software was also downloaded via a broadband link. Since many users do not have this, the time taken to download could discourage them from taking preventative measures (a factor of 5 might be considered reasonable if using a modem link).

There are a number of necessary elements for a user to acquire these "preventative measures". They need to be aware of; the need for security, where to get protection from and how to use it (the latter typically being downloading from the web and installing). There is a wealth of information about data security available from the web and there are a growing number of sites aimed at home users.

An example of a website that offers security advice for the home computer user can be found at [7]. A twelve-point protection plan for home computers is defined by the CERT Coordination Centre [12]. This provides extremely useful and practical information. Again however, technical knowledge is required. Another important point is that implementing some of the advice will result in a loss of features (e.g. disabling JavaScript / Active X). This lends further evidence to an earlier statement on the mutual exclusivity of security and usability.

6. WHAT ARE THE FUTURE THREATS?

The threats to personal electronic data will continue to grow as the dependence on / proliferation of devices that store and / or process electronic data continues to grow. There will be an increasing use of

- Smart Cards; may in future contain critical information i.e. personal medical records...what would the implications be if someone could change these?
- Embedded Devices; many may be managed & controlled by service providers. What if their systems are compromised?
- Collaborative Systems; modern cars are already using sensors and bus lines instead of switches and circuits. What are the implications if a line or an intermediate device could be controlled by external intervention?
- Decreasing usage / availability of "manual" methods for backup. Increasing reliability and availability may make users complacent.
- Loss of power; should this be considered as part of a "broader context "of security.

7. INTELLIGENT HOME CHARACTERISTICS

Across the world many countries have Smart Home projects. Some European examples include Deutsche Telecom and partners (in Germany [2]) and Tampere University of Technology (in Finland [4]). Major IT suppliers are also committing their resources, "Intel has invested $200m in companies developing hardware and software technologies for the next-generation digital home" [8].

Telemetry will play a major part; the main embedded devices in an "Intelligent Home" will be Control Systems. Good examples of this which can already be seen are Anti-Theft, E.G. Alarm, Video Camera, Sensors, Lights on / off / intensity, curtain opening & closing and audio-visual control to make it appear that the home is occupied. Human monitoring systems are also under development using intelligent software to monitor patterns of behaviour and issue alerts on exceptions. Other devices will allow access control (for example opening and unlocking the door to your home via a mobile phone or proximity device).

Many future common "household items" will also store data. This category includes Fridges, Cookers and virtually anything electronic involved in the many processes that take place in the home. One of the key considerations is which devices will talk to each other and the means by which they will achieve this.

How much control will the user have? Always on devices are always on! We can pull the cable, but what if we depend on the communication link for a different vital process? (It is no longer possible to turn off the Internet). It is also possible that our homes may act as host to third parties. There are currently some examples of wireless network providers offering discounts to homes that will host access points. This concept further complicates the data security situation.

When it is considered that the security measures taken are strong, it may place systems in a more vulnerable position when they fail; many people have got into the habit of ignoring burglar alarms and car alarms.

Chip and Pin is regarded as being more secure than signing when using a credit card. But if an unauthorised person knows the PIN then they can potentially do more damage, more easily (the theory is that this will not happen as the card readers will download the stolen card data and render a stolen card useless by writing to the chip).

Interesting discussions of some of the consequences if a malicious agent were to be able to eavesdrop on home sensors or manipulate home actuators can be found in [1]. These range in severity from ease of burglary, stalking and control of the home environment to the creation of what they term a

"poltergeist virus" which turns the automated appliances in the home against the home owner.

Other than actual physical damage there is currently very little attack on hardware. Is this likely to change? Can code be written to directly interact with the physiology of devices to render their components un-usable, for example by use of fatal electrical or electrostatic charges (EMP attack). This will be more easily achieved with the move to solid-state devices.

8. CONCLUSIONS

Malicious actions caused via access to home technology are a serious factor, which could prevent the uptake and growth of this type of technology. There is potential for customers to be discouraged from buying and using mobile technology because of concerns related to data security. The extent to which this is a factor is likely to be influenced by media coverage given to incidents that will occur over time.

The more personal data that is stored, the more important the data, the more it is necessary to formally or informally perform personal data risk assessment. This involves asking?

- What data do we use and how do we use it
- What are the implications if we loose our data / if it is stolen? (To what extent could an unauthorised user achieve the activities of the previous point?)
- What data do we need to protect?
- How do we protect it?

It is unlikely that home users have a disaster recovery plan. In the event of a catastrophic system failure they are much more likely to reach for the Yellow Pages or to contact a knowledgeable friend or relative who has some technical knowledge.
So if the existing data or systems are of a sufficient importance or when they become ubiquitous, such a plan will need to be in place.

The issue of data security needs to continue to be a process of education as well as the use of security features and tools; more security does not always mean that something is more secure. It is sometimes taken for granted that a system that has more security is less likely to be violated and hence the implications if it is violated, are much greater. The main stakeholders in this "education" should be the suppliers, the government and the individual.

In terms of the homes of the future it can be seen that the increase in the processing, storage and communicating of electronic data associated with the increasing use of automation increases risk. For example, information could easily be obtained by a hacker to find out the times when the home was being "administered" remotely. Whilst there is no evidence to date, the fantasy of a remote burglary may in future become a reality.

The degree to which we become dependent on home automation and the associated applications has a major bearing on the importance and nature of security precautions. As an example, the concept of location tracking via mobile phones has been mentioned earlier in this paper. Consideration in this case would need to be given to the ease with which this "tracking" could be intercepted by a third party and what the possible implications might be.

Becoming the innocent third party in a hacking attack is a frightening but real possibility (already present in the commercial world). It is likely that there will be more use of third parties by hackers and organised IT criminals as they try to cover their tracks. This is more likely to affect organisations and industry rather than the individual but is likely to have some affect on the home user. It may be expected that in the event of such a claim by the victim, procedures (e.g. Insurance Cover) would be in place to compensate.

This paper clearly identifies that it is the connectivity that provides the major security weaknesses. In line with this, further protection will be needed to supplement the growing provision for data connectivity security currently available (e.g. virus detection and firewalls). The issue of protecting the actual devices may have less of a focus but this must not be neglected (particularly with the rate of technological advance in respect of small scale storage devices).

The paper has concentrated on loss of data or the implications of "unauthorised changing of data". As an increasing usage produces a dependence on personal ICT devices there will be an increasing importance placed on availability and continuity. This brings with it a whole host of other, related issues including operating system resilience and continuity of energy supply. Equally, the theme has been the unauthorised access to and misuse of data to engage in criminal activity.

The technology that is used to help prevent unauthorised use / access to home devices will depend upon the infrastructure(s) deployed. Whilst there are a number of connectivity proposals there is no single standard at this time. However, a reasonable assumption is that the Internet Protocol (IP) is likely to be a part of many systems. Good security requires a multi-faceted approach. The widespread use of encryption coupled with Biometric devices appears to offer considerable hope for genuine security and will be experimented with and deployed in the smart home where proven to be effective.

The current requirements for home automation require technical knowledge of some level (e.g. the use of a computer). There are many benefits to be gained from connecting the home to the internet since it allows for remote monitoring, improved control (more information is available) and ease of update. In order for home information to become ubiquitous, the level of technical knowledge required needs to reduce and this is likely to result in a dramatic increase in the number of embedded devices. These devices will be connected to the Internet and may be managed by service providers. Whilst this will provide ease of use it will also present security concerns. Mobile technology e.g. mobile phones are one of the proposed interfaces for facilitating external control. This further complicates the security perspective because it is then necessary to ensure that the communications between these devices and the home / host management system are secure.

REFERENCES

[1] Bergstrom P., Driscoll K., Kimball J. (2001) Making home automation communications secure. *Computer*, (October 2001), pp. 50 – 56.

[2] Miller, F. (2001) Information technology: wired and smart: from the fridge to the bathtub. *Fraunhofer magazine*, (2. 2002), pp. 30 – 32. Available from world wide web: http://www.inhaus-duisburg.de/en/projektbeschreibung/rojektbeschreibung.htm

[3] Greek, d. (2004) News: security breach hits another online bank. Computer active [online]. Vnu, [accessed 09 november 2004].. http://www.computeractive.co.uk/news/1159273

[4] Pirhonen, A.(2003) e.finland [online]. E.finland, [accessed 10 november 2004]. Intelligent and cosy e-home: the e.finland weblog. http://www.e.finland.fi/netcomm/news/showarticle.asp?intnwsaid=15743

[5] Halliwell, J. (2003) Combating identity fraud. International professional conferences. IPC, [accessed 11 november 2004]. Available from world wide web: http://www.ipc-conferences.co.uk/idfraud/idfraudframe.htm

[6] Anon (2004) Hoax warnings, F-secure [online]. F-secure.com, [accessed 11 november 2004]. http://www.f-secure.com/virus-info/hoax/

[7] Anon (2004) Data security in our connected world is now about information security. Close protection [online]. [accessed 11 november 2004]. http://www.closeprotection.ws/data-security.htm

[8] Jacques, R. (2004) Intel inside the home of the future. computer active [online]. Vnu, [accessed 11 november 2004]. http://www.computeractive.co.uk/news/1151886

[9] Ward, M. (2003) The spy inside your home computer bbc [online]. [accessed 12 november 2004]. http://news.bbc.co.uk/2/hi/in_depth/sci_tech/2000/dot_life/2487651.stm

[10] Anon (2004). Security at home: protect your pc. *Microsoft.com* [online]. Microsoft, <http://www.microsoft.com/athome/security/protect/default.aspx>.[accessed 09 november 2004].

[11] Anon (2004) United kingdom threat assessment of serious and organised crime 2003: 9. Sex offences against children, including online abuse. *National criminal intelligence service* [online], [accessed 09 november 2004]

<http://www.ncis.co.uk/ukta/2003/threat08.asp>
[12] Anon (2001) Cert coordination centre: home network security. *CarnigieMmellon software engineering* [online]. Carnegie Mellon University Pittsburgh, [accessed 11 november 2004]. <http://www.cert.org/tech_tips/home_networks.html >.
[13] Dolby, J. (2003) Home: Telecomms: new mobile phone tracker pinpoints and verifies locations over all UK networks. *pressbox.co.uk* [online]. [accessed 17 december 2004]. http://www.pressbox.co.uk/detailed/10083.html
[14] Anon (2001) Short survey of published material on UK key trends 2001-2011 *UK cabinet office performance & innovation unit.* Available from world wide web: http://www.number-10.gov.uk/su/key.pdf [accessed 17 december 2004].

APPENDIX – ANTI-VIRUS AND FIREWALL SOFTWARE INSTALLED

AV Software

Installation of Sophos
File Size; 14.5 MB
Time to install; 5 minutes (including un-zipping)

Firewall

Installation of Zone Alarm 5.1 from Zone Labs.
File Size; 8.2 MB
Time to install; 10 minutes (to view the optional tutorial was an additional 6 minutes)

(please note that the choice of products was random)