Issues in Trusted Home-Networking

Andrew Kay*　Toshio Nomura*　Tim Wilson*

Abstract

Present trends suggest that in the future digital and home appliances of all kinds (not only the PC, hi-fi and digital camera, but also central heating controls and personal medical sensors) will be on-line at least some of the time; and that people will increasingly embrace digital information and transactions as an essential part of their lifestyles. We discuss the importance of digital security in protecting people, their homes and their networked communities; and we explore some of the reasons why it is difficult to get security right, both for digital appliances and for services. We stress the importance of trust, and discuss whether certification could help customers evaluate the security of products.

現在の状況から推測すると，将来あらゆるデジタル機器や家電製品が（例えばPC，オーディオ，デジタルカメラなどにとどまらず，セントラルヒーティング制御や個人用の医療センサーなども）場合に応じてオンライン化され，人々はますますデジタル情報に囲まれ，生活の一部としてそのやりとりを行うようになるであろう。本稿では人々やその家庭およびネットワークされたコミュニティを守るという観点からデジタルセキュリティの重要性について議論する。またデジタル機器やサービスについて，うまくセキュリティを確保することがなぜ難しいのか，その理由を検討する。筆者らは信頼性の重要性について強調する。さらに認証が製品の安全性を判断する上で使用者の助けになるかどうかについて論ずる。

1. The digital, networked future

Hobbyists and enthusiasts have been experimenting with home networking for over thirty years [1]. Now the relevant technologies are becoming cheaper and more widespread, and will soon be easily accessible by ordinary people without specialist technical knowledge.

Present trends in increased use of and reliance on digital networks suggests that in future many houses will contain networks, so that not only traditional data appliances (such as computer, phone, TV, hi-fi, camera and mp3 player) will be connected all or much of the time, but other appliances too (lights, central heating, fridge, washing machine and so on), perhaps even the kitchen sink. Appliances will be controlled and monitored remotely, and some may be able to communicate their need for spare parts or maintenance to a device with a better display. For just a few examples see Table 1.

As a special case, the sick and the frail will be able to wear networked healthcare devices (for example pacemakers and blood monitors) so that conditions can be monitored and logged remotely, and proper medical

Table 1 Examples of the benefits of home networking.

- Operate the lights or front door without leaving the sofa.
- Monitor the house while on holiday.
- Adjust the heating controls if you are coming home late.
- Reduce washing machine servicing costs with a remote diagnostics service.
- Receive alerts from security alarms or for faults and emergencies.
- Locate appliances remotely if they are stolen.
- Connect medical sensors wirelessly for 24 hour health monitoring.
- Back-up data and personalisation settings easily, and off-site.

* Sharp Laboratories of Europe, Ltd.

or welfare attention can be provided in emergencies. Older citizens will be able to live more independently in their own digitally equipped homes, receiving care and support and (virtual) company, previously available only in institutions. Sensors will detect wrong doses of medicine, missed meals, falls or general confusion, so a carer can be contacted by video link.

With time-pressures of contemporary life at home and in business we can be sure that people will demand quick solutions to problems, and that always-on networking technology will form a significant part of those solutions. However, users will not tolerate extended learning times to make use of intricate features unless they can use them incrementally and productively.

Digital information and services will be available to people wherever they go, via their network appliances. Some of this information will be highly sensitive, including medical, legal, government, business and financial details; personal identity and privacy; and proofs of ownership and rights. Many of the transactions will involve legally binding contracts, and though most of these will individually be of low value, some will be for far more expensive products and services.

2. The risks of networking

Well-designed networking technology has the potential to provide great benefit of convenience and flexibility to users. However, it is indisputable that increased connectivity creates extra risks (both malicious and accidental) to personal privacy, identity, integrity and possessions. More flexible devices with many customisable options and downloadable applications naturally add to the kinds of errors and confusion that create opportunities for crime. Similarly, putting a larger range of products and services on the network provides potential for more kinds of crime.

Putting home appliances on a network creates the potential for new kinds of attacks which were not previously possible. We start by listing some points of attack.

- The home network is likely to have a network hub with a rich human interface and access to the internet. Such a machine is open to all the usual internet attacks-including virus, worm, key logging, phishing and other social attacks. If it is designed to take commands from the homeowner concerning operation of the home network it also has the authority to cause the misbehaviour of almost all devices on the network.
- An 802.11 wireless network can be joined from remarkably far away, even several kilometres [2], given appropriate equipment. There are several attacks on wireless LAN protocols, including spoofing the network master, causing client devices to trust a hostile network. In built-up areas many wireless LANs overlap, and you can easily imagine an attack which enters through a single insecure internet hub and spreads from LAN to insecure LAN throughout a geographical neighbourhood. Similar considerations could apply to Bluetooth.
- Other LAN technologies are available, but each may have its own weaknesses. For example, inter-device communication through the electrical mains [3]. With this technology private signals easily travel via the electricity supply point to and from neighbouring houses, from where remote attacks can potentially be mounted. It's also easy for a visitor to plug in (perhaps inadvertently) a malicious or compromised appliance.
- Electronically controlled doors and windows invite the risk of giving physical access to potential thieves.
- Mobile or portable equipment, such as mobile phone, video camera or car may be compromised when away from home, and wreak havoc when re-connected to the house LAN.
- The appliances themselves may be compromised, perhaps even by residents or visitors who have rights to operate them, and used to compromise the network (deliberately or accidentally) or to collect information from other appliances.

Some examples of risks are shown in Table 2. The point is not that these attacks are likely, nor that they cannot be prevented in theory, but that they must not occur in practice. Today's experience of many internet worms shows that often their writers just want to cause damage, the more the better. They don't need to have any other reason. It is important therefore that people are protected from even potential network attacks, because sooner or later someone will try. It is also interesting to note that more than half of US identity fraud is committed by someone known to the victim [4], not by a remote and faceless cracker.

3. Security is important

It is clear, therefore, that security of the appliances,

Table 2 Some examples of home network risks.

- Your front door (or back window) is unlocked remotely, the alarms deactivated and your house burgled.
- Your network authentication device fails, and you can't get into your house. Or a virus attack means you can't turn the lights on.
- Protected content (such as video) is copied as it travels around your LAN
- Your central heating controls are taken over while you are away, and either your fuel bill is enormous or (possibly) the house burns down. Or the central heating won't switch on in winter, and you get very cold.
- Private medical data is snooped on, or your personal habits are monitored.
- Spam is displayed on every appliance.
- Appliances are stolen, along with your data, private information and perhaps passwords to your network.

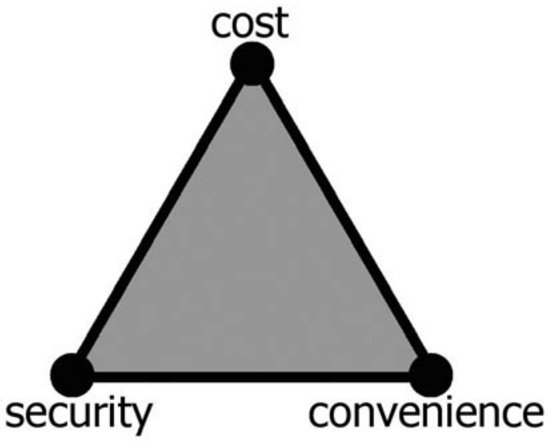

Fig. 1 The eternal trade-off triangle.

the network and the services will be of importance to everyday lives. Security is naturally important to businesses and individuals. A recent report [4] states that two thirds of US citizens shred sensitive documents before disposing of them. As physical paper is being replaced by its digital equivalent we can be sure that people will increasingly be prepared to pay for similar digital security too. These are real risks, not hypothetical. For example, over 4% of Americans have at some time suffered from identity fraud, with an average loss of over $600 [4].

4. Why Security is Not Easy

Creating and maintaining a secure component, appliance or system is not an easy task, and requires co-ordinated effort at many levels.

When a network is set up, or when a new component is added to an existing network it must be secure from the start. Customers expect that a new network or new component should just work, and this generally means that manufacturers adjust security settings in the factory to be rather permissive. However, it is also important that components are secure as soon as they are plugged in, and this requires that factory defaults should be restrictive. This conflict between convenience and security is well known (see Fig. 1), and applies throughout the lifetime of the network. Solutions may involve more complex set-up support, though this can be more expensive.

Any single part of a system can potentially compromise the security of the whole. Security is a code of conduct between all parties involved. Without tight regulation and standards it can be difficult to determine who or what is to blame when there is a breach. For the customer, even finding which supplier to approach with configuration issues can be a substantial problem.

Security may also depend crucially on software applications that are not traditionally considered security-relevant, such as word processors and file viewers. To see this one need only consider the number of security alerts generated by Microsoft Word. Moreover a system includes not only the hardware, software and network, but also the operators and users, and any related services or devices with even temporary right of access.

In a recent survey [5] three quarters of the respondents (office workers) were willing to give up their passwords to a stranger on being offered a bar of chocolate. This kind of social engineering attack is pervasive, and can be very difficult to work around. So people are part of the security challenge too.

Protecting oneself from new risks implies having a new understanding of what is secure. Putting more devices on the network, and devices with longer lifespans, means more can go wrong, and the stakes are higher because people do not like to feel vulnerable in their own homes. Most people will not understand the new risks–it takes a long time to get used to them, and develop the right instinctive behaviours. If a device fails to get permission to operate on the network, it is very tempting for the owner to just turn off the security, with potentially disastrous results. Education is a very slow process, and is always out of date. So the security must be designed in, and be automatic.

It would be naïve to suppose that any ‘secure’ system will remain secure forever. Security is a process, not a product, and is never absolute. New attacks are always being found, and changing economic factors can turn a low-risk application into a high-risk one (for example, chip probing stations are getting cheaper, so the potential for attacking silicon directly to read its secrets is raised). A device in a secure system must be monitored and maintained with care after it is sold, and it is necessary for the supplier to respond quickly to new attack methods with information, education, software updates and policy changes.

Strong authentication, using passwords and so on is not the whole answer. If an appliance is shared by several users then one user may wish to obtain information illicitly about the others. Here an authorised user (perhaps even the owner) is also the attacker.

When things do go wrong (as they occasionally will), the secure system must be able to provide a fall-back position. The customer would be sorry to lose her collection of digital photos following a random attack or a hardware failure; she would be more than angry to lose all her tax receipts and product licences. For this reason the home requires a secure system for backup that ensures privacy of the information. Very critical documents (such as property deeds) should prudently be printed and deposited in a bank.

A serious challenge for security engineering is to prevent attack without making the device too difficult to use, nor reducing its functionality so that it cannot compete with similar but less secure devices.

People may wish to lend their digital devices to family or friends. To do this they must temporarily grant rights of use, but often these rights need to be restricted–perhaps the borrower should not be allowed to change certain settings, or add new accounts, and certainly should not be able to restrict the rights of the lender. An appliance must (even though it is secure) be able to be used by an 'appropriate' guest user; or by a single user with several distinct rôles (e.g. for business or for personal use); or by a user who is simultaneously authenticated on a different device; or in conjunction with other secure and insecure devices and services; or when a key-token is lost, or a password forgotten (though perhaps after a delay for re-authentication); and whether it is on-line or off-line. The list goes on, but each of these requirements makes good security difficult to achieve for the whole system.

It is also important to avoid adding complexity to create functionality. For example, no ordinary user will carefully construct lengthy access control lists or specify rights for multiple users to multiple functions. There must be good default values and simple models for modifying these. There must be useful hints and reasons given when things go wrong.

Normal engineering practices depend on assumptions about the environment in which the product will be used. If something small goes wrong it could easily be ignored as 'something for the user to work around', or 'to be fixed in the next release'. Small deviations from the specification can be tolerated if they are 'unlikely to occur' or occur only 'outside normal conditions'. This is because the users are considered to be fairly benign. However, in security engineering, the attacker must be considered to be trying deliberately to break the system. For example, it is enough to state that the device must not be operated with the lid open, and a typical user will probably comply, as it is in his interest for the device to work. This is not the case with an attacker, who might open the lid in order to try to probe the circuit. Similarly, 'back-doors' left in devices for maintenance or testing purposes can be exploited by the unscrupulous.

This kind of consideration shows that engineers have to use a different way of thinking and be trained explicitly to work on secure systems or components of secure systems.

5. Guaranteed Security

It is easy for a product slogan to declare security, but such a claim is very hard for end-users to substantiate, even if it is true.

There is no such thing as perfect security–products will be used in new situations, and new attacks will be developed. Any 'secure' product with a reasonably long lifespan will have to be provided with a method for updating its security protection.

A company that produces products that are powerful and convenient, yet secure and easy to use, is in a strong position to create a brand which is trusted by its customers. Trust must be carefully managed and protected, since it is built only slowly by continuous positive performance, but can be lost quickly after just a few bad experiences. Unfortunately, security depends on the whole system, which may not be supplied by a single manufacturer, and blame may be unfairly placed on the wrong system component.

One method to achieve secure design is through interoperability standards and industry consortia, such as for network protocols. On the whole these are aimed at adding functionality to products; they are not designed to ensure that other behaviours are ruled out. For example a device in compliance with a 'secure' protocol may also accept insecure connections, outside the protocol, or be easily modified to do so (think of how easily DVD players are 'adapted' to become multi-region).

These standards are often self-policed, and customers will soon complain if appliance A doesn't connect to benign network B; but less likely to notice (in the short term) that evil network E also connects to appliance A, when it should not have permission.

Another method is through certification, such as common criteria (CC) [6]. CC certification tests that a product does what it claims to do (from a security point of view), relative to a given 'protection profile' which can be a standard for a whole class of devices from different manufacturers. Sharp already has experience in this approach through its secure printer and smart card businesses. However, CC is expensive and can be slow.

It is possible to use a hybrid route, in which some functions are tested independently, and some functions are self-policed according to a well defined set of criteria. The US government FIPS [7] standards work this way.

Successful interoperability and convenience that maintains security is not an impossible goal. The international networks of both cashmachines (ATM) and mobile phones are amazing examples that have been running for years, in which different institutions have co-operated on maintaining technical standards and improving them gradually as security flaws have been exposed.

Another example in progress is the forthcoming electronic passport defined by the International Civil Aviation Organization (ICAO) [8]. Each country has its own cryptographic keys and its own physical formats. ICAO has worked hard to ensure that the keys can be distributed reliably and securely, and that the physical devices (passports and passport readers) will interoperate. We will see how well this works in practice over the next few years.

6. Hardware Security Modules

Some network protocols rely on each device being able to keep secret data really secret. For example, a device D may have to prove its identity (and therefore its authenticity) by demonstrating that it has knowledge of a certain piece of information, usually a cryptographic key. If the information could be copied then any other device could impersonate device D.

In most digital devices it is relatively easy to extract information by probing the hardware directly. For example, network passwords are usually stored somewhere in the device's EEPROM or Flash memory, and an attacker can simply read the memory.

To prevent this, the secure part of a device can be implemented in a hardware security module, or HSM. The HSM is usually a single chip, including CPU, RAM and persistent storage, and is carefully constructed so that information is very difficult to remove illicitly.

Perhaps surprisingly, HSMs are very common. For example, the chip-and-PIN credit card is an HSM in the form of a smart card; and the card reader or ATM which reads it also contains an HSM. This is why it is difficult to clone a chip-and- PIN card.

An attack against an HSM must be more sophisticated, as the password memory cannot be accessed directly. On method is to modify the circuit inputs (data signals, clocks or power) in unexpected ways and trick the device into revealing its secrets. With another approach, it is sometimes possible to determine decryption keys by monitoring how much power the device uses, or how much electromagnetic radiation it emits, when it is known to be manipulating the bits of the key.

Technologies for countering these kinds of attack do exist, but their implementation is subtle, and not every manufacturer can implement them. Special sensors detect attempts to modify the inputs; shielding layers prevent attacks with chip probing stations or laser beams; and balanced circuits and specially masked algorithms prevent information leaking through the power supply. For such a complex system it can be hard to know whether the countermeasures are adequate.

It is possible that an HSM could be certified by itself as safe to add to a range of network appliances. In this scenario, each networked appliance may be required to contain an HSM that connects it securely to the network. The HSM would be able to authenticate itself unambiguously to the rest of the network, guaranteeing that the appliance could not gain network privileges to which it was not entitled. Such a policy would make it harder for malicious or badly implemented appliances to get on the network and create a security hole which could be exploited. Since a single HSM certificate could cover a range of appliances the cost would be much lower for a similar or higher standard of security.

Conclusion

Consumer electronics manufacturers cannot ignore the potential market for automated homes and home networks. However, there is a danger of companies rushing to produce immature products which do not have sufficient security. If there are security breaches customers will be wary of buying in future, and the market will shrink.

So security is important, even on home networks, yet it is complex. It remains to be seen how customers will determine whether the products they intend to buy are actually secure enough. If the problem is bad enough for a single manufacturer, it is worse when the customer builds a heterogeneous network of appliances from different suppliers. Existing certification schemes are likely to be too expensive for most appliances, yet voluntary standards often do not actually ensure security. For heterogeneous networks, when configuration issues occur or when upgrades are required in response to new security risks, the customer may not know whom to ask.

Part of the technical solution may be that network secrets and protocols will be entrusted only to hardware security modules that can be reused in many different appliances. Certification for such HSMs could be to a suitably stringent level, since the cost is shared over several products, and would give the public confidence in using the products into which they are built.

It will be interesting to see how the security challenge can be met. Making home networks which are trustworthy and yet affordable and convenient to use may be the only way to create a sustainable market for the future.

References

[1] X10 home automation protocol, http://en.wikipedia.org/wiki/X10

[2] Defcon Wi-Fi Shootout, http://www.wifi-shootout.com/

[3] Home Plug powerline alliance, http://www.homeplug.org/

[4] 2005 Identity Fraud Survey Report, Javelin Strategy & Research, Jan 2005 http://www.javelinstrategy.com/

[5] “Passwords revealed by sweet deal”, BBC News, April 2004, http://news.bbc.co.uk/2/hi/technology/3639679.stm

[6] Common Criteria, http://www.commoncriteriaportal.org/

[7] Federal Information Processing Standards, http://www.itl.nist.gov/fipspubs/

[8] Machine Readable Travel Documents homepage, International Civil Aviation Organization http://www.icao.int/mrtd/Home/Index.cfm

(received October 11, 2005)