Is security a lost cause?

Chris J Mitchell

c.mitchell@rhul.ac.uk

Information Security Group
Royal Holloway, University of London
Egham TW20 0EX, UK

Abstract

We examine two key issues for future information security, namely: (a) what do current technological trends mean for future information security, and (b) what effect do conflicts between security/privacy requirements and economic and technological pressures have on the future prospects for a more secure Internet? We consider the effects on security and privacy of six key emerging technology trends, namely: ubiquitous computing; third party computing; growing system and component complexity; integrated peripherals; system intelligence; and orchestrated attacks. We go on to consider a range of ways in which economic and technological pressures are making it ever more difficult to provide effective security and privacy. We conclude by considering whether there is any light at the end of the tunnel.

Keywords: security, privacy

1 Introduction

Those of us working on new and emerging security technologies tend to focus on issues relating to the technologies themselves, such as:

- what their security properties are;
- what can be done to develop and improve them; and
- what applications can be found.

However, from time to time it is helpful to look at the bigger security picture. That is, it is worth looking at the major IT trends, and how they affect security and privacy. This could help to suggest new directions and set priorities for future research. This is the main goal of this paper.

We examine at a high level two key issues, namely:

- **Technology trends** — what do they mean for future information security and privacy?
- **Conflicting requirements** — how security and privacy requirements are pushing in very different directions to very powerful economic, technological and social pressures.

Our preliminary analysis suggests that many ongoing trends are helping to make security and privacy problems worse, and that the security community faces an uphill battle in trying to keep mission critical data and services secure.

2 Technology trends

In this section we examine six key emerging technology trends, each of which have serious implications on the provision of information security and privacy. The areas we consider are as follows.

- Ubiquitous (or ambient) computing;
- Third party computing, e.g. Clouds, web proxies or Grids;
- Growing system and component complexity;
- Integrated peripherals;
- System intelligence and system autonomy;
- Orchestrated attacks.

We also briefly look at a number of other areas, and conclude by identifying some overall trends.

2.1 Ubiquitous computing

Always-connected devices have gone from being an area of research to a current reality, including such common devices as smart phones and PCs connecting via wireless networks (as well as still emerging technologies such as RFID tags and sensor nodes). These systems have evolved, and will continue to evolve, on a piecemeal basis; in particular there is no overall security architecture. This lack of a single security framework and set of security principles poses a huge risk, since these devices routinely communicate with each other, often without direct human intervention.

The common binding element is the use of TCP/IP across a wide range of underlying network technologies. However, these protocols have also evolved over a long period of time, and, although we do have IPsec, not only is this far from universally deployed but it also does not address any security issues arising at lower layers of the protocol hierarchy.

The technology-specific network protocols themselves often offer a very limited set of security features. For example, authentication of the 'access network' to the device is sometimes non-existent, e.g. as is the case for GSM and 'Wi-Fi' (i.e. wireless local area network devices based on the IEEE 802.11 standards). The emphasis as far as security solutions is concerned has typically been on controlling access to the network to protect the investment of the network owners, rather than the serious threat to end nodes posed by unauthenticated access points.

The effects of such a lack of authentication of the network has been widely documented in the academic literature (see, for example, [4, 13]), as well as more widely on the Internet. This has given rise to a series of public domain implementations of 'fake network' attacks on GSM and IEEE 802.11, as well as attacks arising from compromised access points (where the compromise might arise from software or hardware attack).

There are a host of examples of such software, including AirJack[1] and airsnarf[2] — see, for example, Potter [15]. Airsnarf, for example, is a rogue wireless access point utility designed to demonstrate how a rogue access point can steal usernames and passwords from public wireless hotspots. A graphic description of how airsnarf could be used to compromise user security is provided on Kewney's blog[3].

Similarly, pair-wise device authentication is sometimes not robust; for example the original Bluetooth device pairing scheme was rather weak [8]. In general, as a result of the lack of comprehensive and integrated security solutions for mobile connected devices, there is an ever-growing risk of widespread malware attacks, as devices become more 'smart' and flexible.

The Register reported in February 2007 [11] that 3G malware attacks in mobile networks have reached a new high, according to McAfee. 83% of mobile operators were hit by mobile device infections in 2006, according to analyst group Informa. The number of reported security incidents in 2006 was more than five times as high as in 2005. Around 200 strains of mobile malware had been discovered at the time of the report. Things appear to have become significantly worse in the three years since this report was published.

Finally, apart from poor security fundamentals, privacy is a major issue. Device tracking is a particular problem. In any network protocol, addresses of some sort are exchanged between devices, and, at least at some level of the protocol hierarchy, these addresses need to be exchanged in cleartext. If the address of the mobile device is fixed, then this offers a simple way of tracking the location of that device, and by implication, its owner. Much work has been done to try to address this problem for a wide variety of protocols, including for mobile networks [5] and RFID tags [16].

2.2 Third party computing

As has been widely discussed, there is growing trend to move data and processing to the cloud. The security and privacy concerns arising from such a move are well-documented (see, for example, Cachin, Keidar and Shraer [3]). It is especially worrying since many cloud providers appear to offer very few guarantees about the security, privacy and availability of the data they store. Reports of real-life security breaches are not hard to find; for example, a July 2009 report [10] describes how a hacker accessed confidential Twitter documents after breaking into a Twitter employee's e-mail account.

[1] `http://sourceforge.net/projects/airjack/`
[2] `http://airsnarf.shmoo.com/`
[3] `www.newswireless.net`

Of course, the move to the cloud can be seen as just one part of a long-term trend to outsource IT provision. All users of outsourced services need to ask deep questions about security and availability. As reported in late 2009 [17], data security has become 'the number one issue' in outsourcing contract negotiations at his firm, according to John Delaney, partner and co-chairman of the Technology Transaction Group in the New York office of Morrison & Foerster.

Social networking provides a particularly pervasive example of third party computing. Huge numbers of individuals trust social networking sites with very sensitive personal data, but the measures taken by these sites to protect this data (and their liability if anything goes wrong) is far less clear. Other privacy issues abound. For example, in late 2009 the London-based Daily Telegraph reported [2] that privacy campaigners and civil liberties groups have criticised an update to Facebook users' profile settings, saying it was pushing members to share personal information. "Facebook is nudging the settings toward the 'disclose everything' position", said Marc Rotenberg, executive director of the US Electronic Privacy Information Centre. "That's not fair from the privacy perspective".

2.3 Growing system and component complexity

Another long-term trend with serious consequences for security is the ever-increasing complexity of both hardware and software. That is, the complexity of both individual devices and the software running on these devices has continued to increase for many years.

This is often for reasons other than increases in functionality. For example, the rapidly reducing cost of sophisticated computing capabilities makes it simpler and cheaper to put a powerful processor and a complete operating system into a small embedded device, rather than write special-purpose code. Systems built out of individual components are also becoming more complex — growing interconnectivity potentially adds huge complexity.

As an example of growing software complexity, we consider the development of Microsoft Windows NT. Following Maraia [12], the numbers of source lines of code (SLOC) for operating systems in Microsoft's Windows NT product line are as given in Table 1.

Table 1: Growing complexity of Windows NT

Ship Date	Product	Dev Team Size	Test Team Size	SLOC
Jul 93	NT 1.0 (released as 3.1)	200	140	4–5 million
Sep 94	NT 2.0 (released as 3.5)	300	230	7–8 million
May 95	NT 3.0 (released as 3.51)	450	325	9–10 million
Jul 96	NT 4.0 (released as 4.0)	800	700	11–12 million
Dec 99	NT 5.0 (Windows 2000)	1,400	1,700	29+ million
Oct 01	NT 5.1 (Windows XP)	1,800	2,200	40 million
Apr 03	NT 5.2 (Windows Server 2003)	2,000	2,400	50 million

It has long been accepted as a fundamental principle that complexity is the enemy of assurance. Simple arithmetic says that if there are a certain number of vulnerabilities per 1000 SLOC, then the more code there is, the more vulnerabilities there will be. These issues have been explored by many authors (see, for example, Ho, Zhao and Pepyne [7]).

Finally we observe that a lot of wishful thinking about emergent properties appears to permeate the industry; in particular that, somehow, a secure system can be built out of a collection of insecure components. The notion of an emergent property is, of course, well-established, but it is far from clear whether security and reliability can 'emerge' in this way.

2.4 Integrated peripherals

Computing devices (laptops, phones, PDAs, etc.) now come equipped with a growing number of external interfaces, including cameras, microphones and biometric readers. Users need to consider who or what controls these devices. For example, does a user trust all the applications running on a device not to misuse these functions? In fact these peripherals represent a huge threat to personal and organisational security and privacy.

This is not just a theoretical threat. For example, in October 2008 it was reported [9] that Adobe Systems had warned users that hackers could use 'clickjacking' attack tactics to secretly turn on a computer's

microphone and web camera. By duping users into visiting a malicious website, hackers could hijack seemingly-innocent clicks that, in reality, would be used to grant the site access to the computer's webcam and microphone without the user's knowledge.

These threats look likely to grow. Additional, highly privacy-sensitive, peripherals, most notably including GPS receivers, are becoming commonplace in smart phones and kindred devices. The desire for autoconfiguration of systems and devices (as discussed immediately below) will also increase the risk posed by these peripherals.

2.5 System intelligence/autonomy

With the growing number of small, network-enabled, components in widespread use, there is a corresponding pressure on developers to enable these components to configure themselves and automatically adapt to changing environments. For example, users expect newly purchased components, such as smart phones, wireless headsets, PDAs, and notebook computers, to seamlessly intercommunicate and interoperate; this clearly poses a non-trivial task for the developer.

In the future world of ambient computing, the problem will only grow, and will probably involve many small devices without a complex user interface (or, in the case of small sensor nodes or tags, without any user interface at all). There is thus a potentially huge demand for technology to enable devices to set up communications links and exchange data in a completely autonomous way. This is despite the fact that the security and privacy issues are far from solved. Reputation systems of many types have been proposed as a possible solution, but whilst this may be appropriate for informal relationships of low sensitivity, it is hard to see such schemes as a solution to medium or high-level security requirements, since such systems are notoriously easy to 'game'.

It is perhaps too soon to see much practical impact (in terms of real life attacks) of the threats arising from autonomous configuration. However, this is not to say that there is an absence of concern in the research community — for example, Papazoglou et al. [14] list security as a major research challenge in their survey of self-organising service-oriented computing.

2.6 Orchestrated attacks

A key trend in the development of malware and other attacks has been the shift from 'proof of concept' by amateurs to attacks with criminal or other sinister intent. We can expect continued growth in such orchestrated attacks, conducted by a range of organisations including governments, terrorist groups, criminal gangs, protesters, etc.

The London-based Guardian newspaper reported in early 2010 [1] that 'Critical systems are coming under attack more often from cyber criminals or state-sponsored hackers. More than half the companies running critical infrastructure, e.g. electrical grids, gas and oil supplies, have suffered cyber attacks or stealth infiltrations by organised gangs or state-sponsored hackers, according to a study by the US Center for Strategic and International Studies (CSIS). The attacks are part of a 'cyber cold war', going on silently across the internet, the study suggests. A growing number of company executives believe foreign governments are to blame. The study puts the attack cost to the world economy at £1.4bn annually — but the threat to essential services is most serious.'

Some idea of the scale of the organised attacks can be obtained from Microsoft's Security Intelligence Report series[4]. These extensive reports provide a wealth of statistical data on malware and other attacks gained from Microsoft's own experience.

2.7 Other issues

We briefly mention a number of other technology trends with serious security and privacy impacts.

- **Privacy technology**: The fact that security and privacy sometimes push in opposite directions, particularly in attempting to support both accountability and anonymity, is well-established. A considerable volume of research has been conducted in recent years on ways of supporting technologically-guaranteed anonymity — indeed, the new subject area of *Privacy Enhancing Technology* has emerged.

[4] Available at: `http://www.microsoft.com/security/portal/Threat/SIR.aspx`

Whilst this technology offers much to support individual freedom, if deployed it may well also make it more difficult to trace cyber attacks on individuals and organisations. That is, anonymous criminals may be much harder to detect and convict.

- **Malware techniques**: New and unexpected types of malware are bound to emerge. Even in the absence of new techniques, known types of malware will spread across multiple platform types; for example, if they are not already out there we should soon expect to see rootkits on mobiles.
- **Safety threats**: Security threats to embedded devices pose an increasing safety threat through their control of safety-critical physical devices. For example, highly complex embedded computing systems are used in a very wide range of applications including vehicle control and engine management systems, radio emission power control and battery management systems for mobiles, and control of a wide range of domestic appliances. Whilst computer control of such devices is nothing new, the increasing use of highly complex operating systems as the basis for such embedded systems greatly increases their vulnerability.
- **Provenance issues**: The provenance of both software and hardware has become almost impossible to determine. As a result, how do we know our systems do not incorporate deliberately engineered vulnerabilities? Indeed, it seems almost inevitable that this is already occurring (possibly at the instigation of governments). In principle, open source software helps with discovering accidental or deliberately incorporated vulnerabilities, but in practice use of such software makes assigning responsibility for identifying and fixing flawed software difficult or impossible.
- **Automatic software updates**: The automatic updating of complex software is both very helpful and a huge risk. Its widespread use makes just about every computer system vulnerable to large corporations and (by implication) governments.
- **User authentication**: User authentication techniques are not getting any better, despite the increasing range of available technology. That is, tokens, public keys, etc., are still not widely used. We still overwhelmingly rely on passwords [6], with all their well-documented shortcomings.
- **Long-term data availability**: The long-term availability of personal and corporate data is far from guaranteed, despite (or perhaps even because of) rapid growth in the capacity of a range of media. Modern electronic data storage media tend to have short working lives, which contrast poorly with the lifetime of paper. Without appropriate action, huge volumes of data could be lost.

2.8 Overall trends

There is, without doubt, huge business pressure to market products first and worry about security second. This, as we have seen in recent years, by itself causes enormous security problems. However, technology gets used in ways unanticipated by its designers (with obvious examples being GSM SMS and the universal use of IP); this means that, even if conducted rigorously, initial threat analyses are no longer valid.

This combines with the principle that retrofitting security is very difficult, perhaps even impossible, in practice. Indeed, where it is available, 'retrofit' security technology is often not used (e.g. trusted computing, identity management systems, SET, etc.).

Above all else, improving security and privacy rarely has a big visible financial pay-off to the user (individual or corporate). Of course, serious fraud may be averted, but that only seems like a gain in retrospect (i.e., after a disastrous event you may wish you had spent more resource on security, but the loss is not known in advance).

3 Conflicting requirements

Another way of looking at the problems we have identified is in terms of conflicts. We suggest that not only are there technological trends which threaten security, as discussed above, but many commercial, technological and social pressures conflict directly with improving security and privacy. We start this discussion by briefly reviewing key security and privacy requirements, as well as certain major economic and technological factors.

There are two major security and privacy requirements of interest in our discussions, namely:

- the need for *high robustness*, because of the criticality of IT;
- the need for *privacy protection*, not least because of the emerging legal frameworks and user demands.

We suggest that the above requirements often conflict directly with business, technological and social forces. Inevitably, business forces and social trends are a lot more powerful than security and privacy requirements. The major economic, technological and social factors of relevance here are as follows:

- increasing *complexity*, arising from inevitable technological drift — which directly threatens robustness;
- the increased use of third parties (*outsourcing*) — which makes privacy and security assurance very hard to achieve;
- the use of *intelligence* (sophisticated IT) everywhere, not least to improve flexibility — which also directly threatens robustness.

We next look at some specific examples of where conflicts can arise.

3.1 Efficiency versus robustness

Business pressures force organisations to improve their operational efficiency. Some of the ways operational efficiencies are commonly achieved is through:

- use of third party providers;
- integration across sectors;
- just in time operation (and minimisation of IT investment);
- taking account of green/environmental issues.

However, our robustness requirement suggests that we should:

- avoid reliance on systems outside of our direct control and on single points of failure;
- avoid the possibility of cascading failures;
- build in redundancy (employ multiple parallel systems, etc.).

3.2 Efficiency versus diversity

Efficiency pressures also suggest that we should:

- minimise the number of types of platform/system to reduce maintenance and purchasing costs;
- minimise the number of suppliers to achieve optimal economies of scale.

However, trying to achieve reliability argues in favour of maximising diversity to:

- reduce the impact of vulnerabilities;
- spread risk across multiple technologies.

3.3 Complexity versus reliability

Continuous technological development results in increasing complexity. In particular, hardware and software development is more and more removed from direct human understanding through a growing number of intermediary layers (libraries, CAD tools, etc.). However our desire for reliability suggests we should take note of the often observed maxim that the simpler a system is, the easier it is to make it reliable.

3.4 Flexibility versus stability

The desire for maximising flexibility in business investments, for obvious economic reasons, suggests maximising re-use of a standard platform (e.g. a PC), even in embedded applications. This reduces cost and helps to speed up the development of new products. However, our requirement for stability (as part of reliability) suggest that keeping things simple will increase assurance, and it is again well-established that maximising flexibility also increases the attack surface.

3.5 Novelty versus stability

We finally observe the business and social pressure for novelty, almost for its own sake. Manufacturers want to get their latest idea in the marketplace as quickly as possible in order to grab market share; also, end users want the latest gadget for social/fashion reasons.

However, experience suggests that new almost certainly means less stable. We have all been told never to buy version 1 of anything, as it will be full of unanticipated flaws; in general systems become more stable over time.

4 Concluding remarks

We all see news items about security breaches on almost a daily basis. As security experts we are inclined to shrug our shoulders and say 'I told you so'. However, no-one seems to pay attention to us, and despite our best efforts things are getting worse. Perhaps this is inevitable?

The key question would appear to be 'What should we all do about this?' Well, we all have a role to play.

- *Governments* can help by tailoring regulation to help enforce reliability. They can also invest in law enforcement to help detect and prevent criminal activity.
- *Major technology providers*, such as Microsoft, Google, Apple, etc., need to change their business practices, as far as is commercially practical. In particular they need to move away from the model of deploying products first and fixing them later. To be fair, the signs are encouraging, at least from some of the big players.
- *End users* need to be made aware of their responsibilities for their own security and for protecting the privacy of their and others personal data. However, can we reasonably expect users to be sensible?
- The *academic community* needs to try to take account of commercial realities when developing new and improved security technologies. It is far from clear whether the solution is yet more new cryptographic schemes and security protocols. Perhaps ways of simplifying the deployment of the technologies we already have would be a better goal.
- More generally, can any of us resist business and social pressure? Can we turn these pressures to our advantage?

Overall, it does not seem to be a problem of the availability of good security and privacy technology. We need to find ways of getting this technology properly deployed. Typically this means finding evolutionary paths with low costs to all parties (as opposed to revolutions, which almost never happen, not least because of the chicken and egg problem).

Are we all doomed? Well, perhaps not. There are some areas in which we might discern security-positive events. There is a growing diversity of platform types, covering everything from smart phones to games platforms, all of which seem to have possibilities as platforms for IT. Software engineering practices appear to be improving, at least as far as the big players are concerned. There is, it would seem, a growing awareness by the community at large of the seriousness of security threats. Finally, it is also becoming evident that not everyone wants the most sophisticated computing technology, as the rapid growth in Netbooks demonstrates. Perhaps there is a future for the simpler, less flexible, and more secure/reliable product after all?

References

[1] C. Arthur. Cyber attacks widespread, says report. *The Guardian*, January 28th 2010. Available at: `http://www.guardian.co.uk/technology/2010/jan/28/cyber-attacks-hacking`.

[2] C. Beaumont. Facebook privacy changes criticised. *The Daily Telegraph*, December 10th 2009. Available at: `http://www.telegraph.co.uk/technology/facebook/6778396/Facebook-privacy-changes-criticised.html`.

[3] C. Cachin, I. Keidar, and A. Shraer. Trusting the cloud. *ACM SIGACT News*, 40(2):81–86, June 2009.

[4] D. B. Faria and D. R. Cheriton. DoS and authentication in wireless public access networks. In *Proceedings of the 1st ACM workshop on Wireless security, Atlanta, GA, USA, September 28, 2002*, pages 47–56. ACM, New York, NY, 2002.

[5] Q. He, D. Wu, and P. Khosla. The quest for personal control over mobile location privacy. *IEEE Communications Magazine*, 42(5):130–136, May 2004.

[6] C. Herley, P. C. van Oorschot, and A. S. Patrick. Passwords: If we're so smart, why are we still using them? In R. Dingledine and P. Golle, editors, *Financial Cryptography and Data Security, 13th International Conference, FC 2009, Accra Beach, Barbados, February 23–26, 2009. Revised Selected Papers*, volume 5628 of *Lecture Notes in Computer Science*, pages 230–237. Springer-Verlag, Berlin, 2009.

[7] Y.-C. Ho, Q.-C. Zhao, and D. L. Pepyne. The no free lunch theorems: Complexity and security. *IEEE Transactions on Automatic Control*, 48(5):783–793, May 2003.

[8] M. Jakobsson and S. Wetzel. Security weaknesses in Bluetooth. In D. Naccache, editor, *Topics in Cryptology — CT-RSA 2001, The Cryptographer's Track at RSA Conference 2001, San Francisco, CA, USA, April 8–12, 2001, Proceedings*, volume 2020 of *Lecture Notes in Computer Science*, pages 176–191. Springer-Verlag, Berlin, 2001.

[9] G. Keizer. Webcam users warned of 'clickjacking' threat. *TechWorld*, October 8th 2008. Available at: `http://news.techworld.com/security/105430/`.

[10] G. Keizer. Hacker break-in of Twitter e-mail yields secret docs. *Computerworld*, July 16th 2009. Available at: `http://www.computerworld.com/s/article/9135591`.

[11] J. Leyden. Mobile malware menace hits high — McAfee. *The Register*, February 12th 2007. Available at: `http://www.theregister.co.uk/2007/02/12/mobile_malware/`.

[12] V. Maraia. *The Build Master*. Addison-Wesley, 2005.

[13] C. J. Mitchell. The security of the GSM air interface protocol. Technical Report RHUL-MA-2001-3, Mathematics Department, Royal Holloway, University of London, Egham, Surrey TW20 0EX, UK, August 2001. Available at `http://www.ma.rhul.ac.uk/techreports`.

[14] M. P. Papazoglou, P. Traverso, S. Dustdar, and F. Leymann. Service-oriented computing: State of the art and research challenges. *IEEE Computer*, 40(11):38–45, November 2007.

[15] B. Potter. Next generation wireless security tools. *Network Security*, 2003(9):4–5, September 2003.

[16] M. R. Rieback, B. Crispo, and A. S. Tanenbaum. RFID guardian: A battery-powered mobile device for RFID privacy management. In C. Boyd and J. M. Gonzalez Nieto, editors, *Information Security and Privacy, 10th Australasian Conference, ACISP 2005, Brisbane, Australia, July 4-6, 2005, Proceedings*, volume 3574 of *Lecture Notes in Computer Science*, pages 184–194. Springer-Verlag, Berlin, 2005.

[17] B. E. Rosenthal. Legal voice: If there's a data security breach, who's responsible and who pays the fine? *Outsourcing Journal*, November 2009. Available at: `http://www.outsourcing-journal.com/nov2009-legal.html`.