

Security: Are things getting better or worse?

Chris Mitchell

Royal Holloway, University of London
<http://www.isg.rhul.ac.uk/~cjm>

Agenda

- **Introduction**
- Technology trends
- Conflicting requirements
- Concluding remarks

Background I

- Those of us working on new and emerging security technologies tend to focus on:
 - what their properties are;
 - what can be done to develop/improve the technologies; and
 - what the technologies can be used for.
- However, from time to time it merits looking at the bigger security picture.

Background II

- 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 for research; and
 - set priorities for future research.
- This is the main goal of this talk.

Scope

- We will examine two key issues for future information security:
 - **Technology trends** – what do they mean for future information security?
 - **Conflicting requirements** – how security/privacy requirements are pushing in very different directions to economic and technological pressure (and economic/business pressures are very powerful).

Agenda

- Introduction
- **Technology trends**
- Conflicting requirements
- Concluding remarks

Key trends

- We look at six key emerging technology trends with serious security and privacy implications:
 - Ubiquitous/ambient computing;
 - Clouds/proxies/Grids;
 - Growing system and component complexity;
 - Integrated peripherals;
 - System intelligence/autonomy;
 - Orchestrated attacks.

Ubiquitous computing I

- The advent of always connected devices is already with us (mobile phones, wireless PC connectivity, RFID, ...).
- Systems have evolved piecemeal – there is no overall security architecture.
- Network access protocols offer very limited security (device authentication of network is sometimes non-existent), e.g. giving rise to:
 - ‘fake network’ attacks (GSM, 802.11, ...);
 - compromised access points (either by software or hardware attack).

Ubiquitous computing II

newswireless.net

[Find Local Wifi Access](#)
Locate WiFi access areas near you - Try Google Maps.


[WIFI-Link antennas online](#)
Buy Hi-Gain Wi-Fi / WLAN antennas
Booster your wireless signal.

Ads by Google

the home of
Guy Kewney's
Mobile Campaign

- Home
- Blog
- Comment
- Events
- News
- Features
- Gossip
- Sponsors
- PR releases
- about Guy
- contact

Search




site by
horus web
engineering
ltd

News

Watch out! That's not a real hotspot!

by [Guy Kewney](#) | posted on 19 May 2004

You're in a public hotspot, and logging onto the Internet. ID and password? Sure. Connected! Well, yes, but that's not all. You may have logged onto an Airsnarf box, which is busily faking the connection, and meanwhile, stealing all your details.



And the danger is: this is a very attractive exploit to juvenile hackers because, potentially, it would allow several users to share a single expensive subscription.

The Airsnarf exploit is in most respects identical to an ordinary access point. But it is a private one. It belongs to a hacker; and it logs onto the public AP as if it were an ordinary client. Then it puts up an imitation login that looks just like the public one. And while it does a wonderful job at passing on all your Web packets, and sending the replies back to you, it also keeps track of all the data it handles.

"Airsnarf was developed and released to demonstrate an inherent vulnerability of public 802.11b hotspots - snarfing usernames and passwords by confusing users with DNS and HTTP redirects from a competing access point," says the [investigator](#), at [The Shmoo Group](#).

It's effectively using the techniques of network address translation (NAT) to fool the real hotspot into thinking that several other subscribers are all one. "Basically, it's just a shell script that uses open source software to create a competing hotspot complete with a captive portal."

Well, **as a risk, it would initially look to be quite a low one**. It allows the snarfer to collect email IDs and logins, or other passwords for other Internet services; but it takes quite a lot of work - compared to how much you can get by smuggling a trojan onto the Internet.


The typical script kiddie probably doesn't want your email login. Your email would bore a SK solid in an hour. But your credit card details might be worth sitting in a coffee bar to catch.

And of course, if a bunch of kids all want access through a high-cost (like, BT OpenZone) hotspot, all they have to do is set up a laptop to act as the rogue AP, and then they all log in through it, sharing the cost.

Here's the sweet part, for the kids: they can use your account to do the next log-in, once they have your password. One paid-for hour is all they need. After that, they can be any of the other subscribers who used the spot.

"With a setup like Airsnarf one can obviously create a leading candidate of many popular, nationally recognized, open-to-all

sponsored by...



in News

[First WiFi "RFID" tags appear - to track office equipment](#)

[What's Palm up to? The wireless shutters open Monday at Lehman's conf](#)

[Palm boasts about the number of corporate developers it has already](#)

you're reading:
Watch out! That's not a real hotspot!

["Up skirt" photography. Would anybody really, truly, do it? Yes!](#)

[Your car keys can call your phone. No charge.](#)

[Glyndebourne music festival tunes into WiFi](#)

Ubiquitous computing III

- Similarly, pair-wise device authentication is sometimes not robust.
- Growing risk of widespread malware attacks, as devices become more ‘smart’ and flexible.
- Apart from poor security fundamentals, privacy is a major issue – device tracking is far too simple.

Ubiquitous computing IV

- The Register (12/2/07) reported:
 - 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 have been discovered.

Third party computing I

- There is growing trend to move data and processing to the cloud.
- Security and privacy concerns are widely documented – especially as the cloud providers offer very little guarantees about security, privacy and availability.
- This is just one part of a long-term trend to outsource IT provision.
- Users of outsourced services need to start asking deep questions about security and availability.

Third party computing II

- Daily Telegraph (10/12/09) reported:
 - 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”, says Marc Rotenberg, executive director of the US *Electronic Privacy Information Centre*. “That's not fair from the privacy perspective”.

Complexity I

- Another long-term trend is that towards increasing complexity, covering:
 - hardware of individual devices;
 - software running on devices (e.g. move towards general purpose OSs on special purpose devices);
 - system itself – growing interconnectivity adds huge complexity.

Complexity II

- According to Maraia (2005), the number of source lines of code (SLOC) for operating systems in Microsoft's Windows NT product line are as follows:

Year	Operating system	SLOC (millions)
1993	Windows NT 3.1	4-5
1994	Windows NT 3.5	7-8
1996	Windows NT 4.0	11-12
2000	Windows 2000	More than 29
2001	Windows XP	40
2003	Windows Server 2003	50

Complexity III

- Long known 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.
- A lot of wishful thinking about emergent properties permeates the industry ...

Ubiquitous peripherals

- Ubiquitous computing devices come equipped with growing numbers of external interfaces – cameras, microphones, biometric readers, ...
- Who controls these?
- Do you trust all your applications running on all your devices not to misuse these functions?
- These peripherals represent a huge threat to personal and organisational security and privacy.
- Ubiquitous sensors pose a related threat.

System intelligence

- There is huge pressure on developers to enable complex components to configure themselves and also adapt to changing environments.
- Particularly relevant in context of ambient computing, where devices can set up links and exchange data in an autonomous way.
- Driven by perceived user need (inability to do the necessary work manually – or lack of time).
- This is despite the fact that the security and privacy issues are far from solved.

Orchestrated attacks I

- 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 orchestrated attacks, by governments or other organisations (e.g. terrorist groups, criminal gangs, protesters, ...).

Orchestrated attacks II

- The Guardian (28/1/10) reported:
 - 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 new 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.

Other issues I

- Privacy technology – requirements for providing anonymity will make it more difficult to trace attacks.
- New and unexpected types of malware are bound to emerge. Known classes of malware will spread across multiple platform types – e.g. rootkits on mobiles ...
- Security threats to embedded devices pose an ever-increasing safety threat through their control of physical devices (e.g. vehicle control systems, radio power control and battery management systems in mobiles, ...).

Other issues II

- Provenance of software/hardware has become almost impossible to determine – how do we know our systems do not incorporate deliberately engineered vulnerabilities?
- Open source software in theory helps with discovering vulnerabilities, but in practice means assigning responsibility for flawed software is difficult/impossible.
- Automatic updating of complex software is both very helpful and a huge risk – e.g. through ownership & influence of large corporates and foreign governments.

Other issues III

- User authentication techniques are not getting any better – still overwhelmingly rely on passwords (tokens, public keys, etc. are still not widely used).
- Long term availability of personal and corporate data is far from guaranteed, is despite rapid growth in capacity of range of media. Modern storage media tend to have short working lives ...

Underlying threads I

- There is huge business pressure to market products first and worry about security second.
- Technology gets used in ways unanticipated by designers (e.g. SMS, IP for everything), which means initial threat analyses no longer hold.
- Retrofitting security is very difficult – perhaps impossible in practice.

Underlying threads II

- Available 'retrofit' security technology is not used (e.g. trusted computing, identity management, SET, ...).
- Improving security and privacy rarely has a big pay off to the user (individual or corporate).

Agenda

- Introduction
- Technology trends
- **Conflicting requirements**
- Concluding remarks

Background pressures

- Requirements:
 - High robustness – because of criticality of IT;
 - Privacy protection – growing legal frameworks and user interest.
- Economic/technological factors:
 - Increasing complexity (inevitable technological drift) directly threatens robustness;
 - Increased use of third parties (outsourcing) makes privacy and security assurance very hard.
 - Smarts everywhere (flexibility) also threatens robustness.

Conflicts

- These security/privacy/reliability requirements often conflict with business and technological forces.
- Inevitably, business forces and social trends are a lot more powerful than security and privacy requirements.
- We look at a few examples.

Efficiency versus robustness

- Efficiency pressures:
 - use of third party providers;
 - integration across sectors;
 - just in time issues (minimise IT investment);
 - green/environmental issues.
- Robustness requirements:
 - avoid reliance on systems outside of direct control and single points of failure;
 - avoid possibility of cascading failures;
 - redundancy (multiple systems, ...).

Efficiency versus diversity

- Efficiency pressures:
 - minimise number of types of platform/system to reduce maintenance and purchasing costs;
 - minimise number of suppliers (economies of scale).
- Diversity requirements:
 - reduce impact of vulnerabilities by using diverse systems;
 - spread risk through diversity.

Complexity versus reliability

- Complexity pressures:
 - hardware and software development more and more removed from human understanding – more complex – more intermediary layers (libraries, CAD tools, ...).
- Reliability requirements:
 - the simpler a system is, the easier it is to make it reliable.

Flexibility versus stability

- Flexibility pressures:
 - re-use of a standard platform (e.g. a PC), even in embedded applications, reduces cost;
 - end users want flexibility to gain maximum benefit from their investment.
- Stability requirements:
 - keeping things simple increases assurance;
 - flexibility vastly increases the attack surface.

Novelty versus stability

- Novelty pressures:
 - manufacturers want to get their latest idea out there asap to grab market share;
 - end users want the latest gadget for social/fashion reasons.
- Stability requirements:
 - new almost certainly means less stable – never buy v1 of anything as it will be full of unanticipated flaws;
 - over time, systems become more stable.

Agenda

- Introduction
- Technology trends
- Conflicting requirements
- **Concluding remarks**

Are things getting better or worse?

- 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 (sigh!) and things are getting worse – perhaps this is inevitable ...

How do we fix this mess?

- What should governments do?
 - Does regulation help?
- What can/should major technology providers (Microsoft, Google, Apple, etc.) do?
 - They all believe in getting products out and fixing them later.

How do we fix this mess? (cont)

- What can/should end users do?
 - Can we expect users to be sensible?
- What can the academic community do?
 - Is the solution yet more new crypto/protocols?
 - What should we be doing?
- Can anyone resist business and social pressure?
 - How can we turn these to our advantage?

Getting technology deployed

- It does not seem to be a problem of the availability of good security/privacy technology.
- We need to find ways of getting this stuff 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 chicken and egg problems).

Are we all doomed?

- Maybe not ...
- Some areas in which we might discern security-positive events:
 - growing diversity of platform types (e.g. games platforms as IT platforms);
 - better software;
 - growing awareness of seriousness of security threats;
 - possible future in ‘locked down’ devices.

Questions

- ...

- Contact details:
 - me@chrismitchell.net
 - www.isg.rhul.ac.uk/~cjm