Security For Whom? The Shifting Security Assumptions Of Pervasive Computing

Frank Stajano

University of Cambridge
http://www-lce.eng.cam.ac.uk/~fms27/

Abstract. Pervasive computing will introduce hundreds of computing devices per user. This change is of such magnitude that it is qualitative as well as quantitative. Old solutions may not scale when the size of the problem grows by such a factor—passwords, for example, will no longer be a suitable user authentication method.
In this paper we examine new security issues for pervasive computing including authentication, biometrics and digital rights management. But the potential impact of pervasive computing on society is such that we have a responsibility to look further than just the technical issues.

1 Introduction

The Weiser vision [1] of computers becoming ubiquitous and invisible is now turning into reality: most of us own, and daily interact with, dozens of processor-driven devices. Today watches, telephones, home video systems, cameras, cars, musical instruments, washing machines and even toilet seats often embed one or more microprocessors. Computers migrate into everyday objects and break away from the cliché of keyboard-and-monitor boxes. There was a time in the recent past in which being able to afford one computer per person—as opposed to one per department or, going further back, one per country—was considered as the ultimate luxury. Tomorrow, hundreds of invisible computers per person (a situation indicated as *ubiquitous* or *pervasive* computing, or *ubicomp* for short) will be normal and unremarkable.

Superficially, this transition may appear as nothing more than a quantitative change: the ratio of computers per person, formerly a small fraction below unity, now becomes a two-digit integer. Reality, however, is more complex, and quantitative changes of several orders of magnitude often also imply *qualitative* changes. When the size of the problem grows by a hundred times, there is no guarantee that the old solution will scale in the same way. Think for example about user authentication to a computer, traditionally solved by asking the user to remember and utter on demand a hard-to-guess password; then imagine how practical it would be to have to do the same with hundreds of different ones. Multiplying the old solution by the same growth factor as that of the problem may make it completely impractical. To put things into their correct perspective

M. Okada et al. (Eds.): Software Security—Theories and Systems, LNCS 2609, 2003.

it is therefore appropriate to look at pervasive and ubiquitous computing not as an incremental change, but rather as a paradigm shift—something as significant and revolutionary as the World Wide Web.

As an example, witness how many current PC applications expect, if not demand, to be run maximized, monopolizing all the available screen space and impeding any other concurrent activity. They constrain their users with obsolete usage patterns from the 1970s, when personal computers were strictly single-task machines and all screens had the same size. This widespread and contagious mistake (witness the many web pages that demand a full screen to be usable) is not the product of backwards compatibility obligations: it is just the consequence of blindly reusing a surpassed paradigm (a more comfortable choice for the lazy programmer) without noticing that the computing context has evolved.

Failing to recognize that pervasive computing is a substantive qualitative change will cause us to apply surpassed computing paradigms to many other situations. However, in the security domain, applying obsolete paradigms when assumptions have changed is a guaranteed recipe for expensive mistakes.

2 Authentication and usability

The three fundamental security properties of confidentiality (preventing unauthorized reads), integrity (preventing unauthorized writes) and availability (ensuring authorized users are not denied service) all rest firmly on a distinction between authorized and unauthorized users. This in turn depends on being able to discriminate between these two classes, often in the Turing-test-like context in which all the available evidence consists of bits supplied by the user being verified. The archetypal example is the familiar twofold interrogation of "Userid? Password?", consisting of a trivial *identification* phase ("Who do you claim to be?") followed by the crucial *authentication* phase ("Prove it."). After successful authentication, *authorization* ("I'll grant you these rights.") may follow, depending on the verified identity of the claimant.

As we said above, it is obvious that passwords are no longer a viable solution to the problem of authentication when each user interacts daily with hundreds of computers. But is authentication always necessary?

The very first computers, of ENIAC and EDSAC vintage, didn't have any authentication procedures. An operator would just walk up to the machine, input a program, let it run and collect the result. The very notion of user accounts was not needed until the time when shared resources (in particular online storage) became available and the need arose for allocating ownership of and controlling access to such resources.

Three decades later, the first personal computers also didn't require any authentication—precisely because they were *personal* and therefore each one of them was completely dedicated to one user who had complete control over it. The login interrogation was only re-introduced once these personal computers were connected together to form a LAN.

Nowadays it still is uncommon for personal computers in the home to ask for a password, except perhaps if they're owned by nerds; but a password is usually needed to log in to the ISP that offers network connectivity.

The Big Stick principle [2, section 4.2.8], a very high level security policy model [3], identifies a class of cases in which authentication is superfluous:

> **Big Stick principle:** Whoever has physical access to the device is allowed to take it over.

This is the way in which most of our everyday devices behave: from fridges and lawnmowers to CD players and calculators, if you can touch them, you can operate them. One of the reasons why the Big Stick principle is better than so many other policies is because it is cynically realistic: when someone has unsupervised physical access to the device, she can usually do anything she wants to it [4,5]. Consequently, most of the policies that go against the Big Stick principle are very difficult to enforce and therefore of little practical use.

Of course there are cases for which the Big Stick principle is definitely an inappropriate model—think of a vending machine, or a safe. Besides, Big-Stick-compliant devices have no protection against loss or theft. To offer stronger protection, authentication is usually adopted (although it will often be defeatable unless coupled with an adequate amount of tamper resistance).

From the point of view of the pervasive computing scenario, some interesting questions arise:

1. How often do we really need a stronger protection than that afforded by the Big Stick principle?
2. When Big Stick is no longer enough, do we always need *user* authentication?
3. In cases where user authentication is required, can't we adopt a more friendly mechanism than passwords?

To answer the first question, let's ask two more:

1a. Do we consider today's fridges, lawnmowers etc. to be insecure?
1b. If we find them acceptable as they are, will the situation change once we move into pervasive computing?

The extremely paranoid might label yesterday's fridge as too insecure, in so far as Alice can take out and eat the ice cream bought by Bob. Most regular humans, though, will dismiss this threat as unworthy of countermeasures, particularly in the common case in which the two characters are sister and brother. The Big Stick principle seems appropriate for a fridge: if you can open the door (i.e. if you are in the house), you are authorized to eat the ice cream—even if it was actually bought by your brother. Non-home environments may be borderline cases ("Other unknown students drank the beers I left in my college fridge!" was one of the comments to the above scenario) but on the whole the most appropriate protection seems to be social and territorial ("if we allow you to be in here, surely we also allow you to drink what's in the fridge—within reason").

In other words, the social convention implicitly recognizes that the guest, once inside, could do much worse damage than drinking all the beers in the fridge, and that he is trusted to behave correctly or he wouldn't have been allowed in. We don't *expect* him to drink all the beers, but we don't go to any trouble to ensure that he won't be able to.

As for sub-question 1b, the major changes I see in the move to pervasive computing are *storage of private data* inside the devices and *spontaneous wireless connectivity*. Let's see if they introduce any security requirements not satisfied by the Big Stick principle.

Let's imagine a **digital media jukebox** for the home—the natural evolution of the hi-fi in the pervasive computing era: a multi-terabyte repository with all the movies, camcorder clips, still images and music that members of the household have acquired or generated. Particularly for user-generated material I feel that, while sharing should obviously be allowed wherever desired, individual family members should also have the option of keeping some data items private. This will require some form of access control and consequently user authentication.

Similarly, if bathroom scales, heart monitor and fridge all cooperate to monitor our health, it seems courteous to keep the results private unless the subject explicitly wishes to divulge them to other family members. This, again, requires user authentication. Besides, at least user *identification*, if not authentication, is absolutely necessary in order for the individual measurements to be meaningfully correlated—it would otherwise make no sense to check whether Alice's heart rate matches Bob's weight, or to warn Alice that today she is 22 kg lighter if yesterday's measurement was actually Bob's.

The spontaneous wireless connectivity, on the other hand, an essential element of the ubicomp vision, corresponds to invisible hands plugging and unplugging invisible cables into the devices, and sucking and blowing data and commands at will. Since the invisible cables might even terminate outside the household, the territorial model breaks down: even someone without physical access to the device is able to manipulate it. If we want to be able to prevent this, some form of access control (though not necessarily authentication) is clearly necessary.

Coming back specifically to question 2 on page 3, regulating access to private data such as weight measurements certainly requires user authentication; however, as far as securing wireless connections goes, it is possible (using encryption) to reproduce the level of security afforded by cables without for that having to identify the user. In this case, though, before deciding on a scheme, some thought must go to the situation in which one of the devices is stolen. Does this just cause the loss of that device (reasonable) or does it also imply a compromise of all the other entities that were happy to connect to that device (much less desirable)?

There are also cases in which neither Big Stick nor user authentication is sufficient: a vending machine, for example, which as we already remarked needs

to be governed by a stronger policy than Big Stick[1], is still subject to denial of service attacks of the glue-in-the-coin-slot variety, which a hypothetical user authentication mechanism for buyers would do nothing to prevent.

The third question on our list, about alternatives to passwords for user authentication, is probably the most important. The well-known (but not necessarily exhaustive) taxonomy of authentication methods refers to "something you know, something you have or something you are", suggesting in the first instance tokens and biometrics as candidate replacements for passwords.

Tokens are familiar and time-honoured authentication devices for home users: the front door, the car, the bike chain and the desk drawer are all unlocked with a cleverly shaped metal token. The main inherent vulnerability of a token-based system is the one arising from loss or theft of the token and consequent impersonation of the owner by another party. On the other hand, the ability to delegate access rights simply by lending the token may in some cases be a great advantage, as may the plausible deniability [6] (i.e. the fact that it's impossible to disprove your claim that someone else was using your key instead of you). We shall discuss related ideas in section 4.

In the pervasive computing context, tokens in the shape of metal keys would probably not be practical, but contactless tokens that could perform the authentication wirelessly within a radius of half a meter or so might be an interesting choice and would blend in well with the ideal of "do-nothing technology" [2, section 2.5]. Issues to be carefully evaluated include replay attacks, man in the middle and just spontaneously authenticating to a malicious device without the consent or knowledge of the token holder.

Biometrics [7, chapter 13] such as fingerprints or iris recognition have not gained widespread use as yet, but they offer the advantage of providing an authenticator that can't be inadvertently left at home (unlike a token) or forgotten (unlike a PIN). The absolute performance of such systems depends on the usual tradeoff between false positives (mistakenly accepting an impersonator) and false negatives (denying access to a legitimate user).

One inherent problem of such systems is the difficulty of revocation: what can I do when a crook makes a plastic clone of my index finger from the prints I left on that drink glass?

Another one is the potential for discrimination: the rich Westerners, for whom the iris and fingerprint recognition systems would work without problems, would be placing other races (dark-eyed Africans or Asians) and social classes (manual workers with damaged or missing fingers) at a disadvantage by inflicting usability problems on them.

Finally, looking at the whole system as opposed to the authentication subsystem in isolation, there may be scenarios in which biometrics prevent one kind of crime but trigger a worse one: if your expensive motorbike won't start unless the ignition button senses your thumbprint, the bad guys will be forced to chop off your finger rather than just stealing your keyring. But this is not the main problem, and it may be argued that a better technology would be able to tell

[1] Note how this translates directly into a tamper resistance requirement.

the difference between a live and a dead finger (although recent studies [8] indicate that we are not quite there yet). For the ubicomp context of hundreds of authentications per day, the issues of usability and intrusiveness are much more relevant.

Combinations of the above technologies may offer benefits not available from any single one. For example I like the idea of two wireless tokens, one in my pocket and one in my watch, that spontaneously authenticate me to the ubicomp gadgets I walk past; the tokens would be initially activated by me typing a PIN, and they would deactivate automatically when out of range of each other—so losing one would not be as bad as losing my keys, while losing both at the same time would be unlikely. Of course, man-in-the-middle and related issues still need a solution as in the case of the single token.

I also think that the importance and relevance of the Big Stick principle to ubicomp is underestimated. While do-nothing solutions (in which everything happens spontaneously through a wireless link) have clear usability benefits, security might be enhanced if the device had a way to distinguish remote commands from those issued by a local user. A physical button on the device may still be a useful discriminator in such cases.

Talking of usability and security we cannot fail to mention the problem of administration and maintenance. The problem is already hard enough for single desktop computers in the hands of non-expert users, so it ought to be clear that the standard approach (hole discovered, fix developed, security bulletin issued, patch applied by diligent administrator) will never scale to the ubicomp scenario of hundreds of machines per user. Even professional system administrators fail to keep up with all the fixes that manufacturers issue, so we cannot rely on ordinary mortals applying all the required security patches. Ubicomp systems must be designed for resilience, with the reasonable expectation that some of the devices I own will at some point be compromised. Interaction protocols must be designed in such a way that this kind of failure will not contaminate all of my other devices. In other words we must account for the possibility of insider fraud, as opposed to partitioning the world into the trusted "us" and the untrusted "them".

Finally, while we have so far insisted on the assumptions of the developers, the assumptions of the *users* are equally important. In the ubicomp scenario, computers hide inside everyday objects and disappear from view. Users will therefore expect certain behaviours of these objects, based on a mental model that does not involve computers. In people's experience, real world objects such as furniture and clothes don't randomly "break"—so the unexpected failures of the programs running on the invisible computers inside those objects will always be shocking. In the words of my colleague Jon Crowcroft, "Have you ever seen someone having to reboot a car? It does happen, but it sure confuses people!".

3 Security for whom?

As we have seen, the three traditional security properties of confidentiality, integrity and availability rely entirely on authentication—on a method, that is, to distinguish authorized users from unauthorized ones. But there is a more fundamental question that is rarely asked: authorized by whom? For whose benefit? This question is directly relevant to pervasive computing and has recently been made topical by the surge of interest [9,10] around what has been euphemistically[2] called *Digital Rights Management* (DRM).

Until recently, if the question was seldom asked, it was perhaps because the answer was obvious: the owner (or at any rate the principal in charge) of the system, the one who demands and pays for the security countermeasures to be installed, is the one who sets the security policy and decides who is and who is not authorized. But things aren't that simple any more. When my minidisc player prevents me from backing up my own recordings of my own university lectures [2, section 2.6.12], for whom is it providing security? Who is the bad guy being kept out?

Secure software needs a Trusted Computing Base to bootstrap. But trusted by whom? Could there be a conflict of interests between owner (buyer) and maker? If so, how can the owner believe (or check) that her rights are being honoured? And what should these rights be in the first place? What rights is it fair for the owner to claim? We should first form clear ideas on this, then state our requirements for the security architecture. Allowing deployed technology to dictate "this is what you can do, so these are your rights" is to exchange cause and effect.

The technical requirements of Hollywood (a standard nickname for the big-name content producers, regardless of whether their products are movies, music, books or whatever else) are straightforward to understand: assuming that the ability to duplicate digital material without loss of quality is a disincentive to the purchase of the material, they seek to be able to sell (or, better, license) digital bits that will be useless to anyone other than the principal who paid the appropriate fee. In order to do this they need complete control of the playback devices, which must refuse to play content unless *they* (not the owner of the player, of course) authorize it. So, for Digital Rights Management to work, every media player must be part of Hollywood's Trusted Computing Base. A player that were not Hollywood-compliant could otherwise save a plaintext copy of the content after having made it playable. This is a system-level observation that stands regardless of the particular DRM implementation.

Such restrictions, however, almost invariably clash with some perfectly legitimate uses of the devices. I mentioned above the case of my digital minidisc recorder that doesn't allow me to take a bit-by-bit backup of my discs—even

[2] Stallman [11], with characteristic sarcasm, redefines the DRM acronym as "Digital Restrictions Management". He also renames "Trusted Computing" as "Treacherous Computing", correctly remarking that the allegedly "trusted" computer will actually disobey its owner.

when all the content has been generated and is copyrighted by me. Another situation is that of the digital media jukebox introduced above in section 2 on page 4. Such a jukebox will either offer or not offer the capability of backing up its content and restoring it to another jukebox. If it will, then it will be possible to duplicate movies without authorization. If it won't (which appears more likely given Hollywood's clearly expressed desiderata) then, if the jukebox breaks down or is stolen, all its content will be lost.

The point being made here is that Hollywood's explanation for the legitimacy of their requests ("we produced this content so we should have the technical means to disallow its unauthorized duplication") glosses over the equally legitimate requests of honest users. If the movies I buy are only delivered to me as bits over the wire, and they disappear if my jukebox breaks because I can't back them up, then shouldn't Hollywood be liable for the loss of my entire software collection (probably one or two orders of magnitude more expensive than the hardware of the jukebox) because it prevented me from protecting it?

The alternative technical solution of checking licences online, which both Microsoft and Apple have adopted for their latest operating system products, is easily subject to abuse and privacy invasion: do you really wish Hollywood to know which disc you're playing every time you do? Microsoft, for example, is not new to using the backchannel provided by the licence checking system (or by their update-via-web service) to acquire and log detailed information on the hardware and software configuration of your machine.

4 Ethics

Security for pervasive computing will require many new technical solutions to address new technical problems. But it would be a mistake to focus only on these. When computers pervade our environment, the impact on society is going to be significant. Before delving into the technical questions it will be worth investigating basic issues of policy. Not "how do we protect it?" but "*what* should we protect?", and why, and for whose benefit?

Without exaggeration, with ubicomp we are building a new world. We must foresee the consequences of this act. In particular, as architects of the new world, we have a moral duty to protect the technically illiterate for whom this new wave of invisible and pervasive technology will be an inescapable and unsolicited imposition. These people are the ones who won't understand the risks and who won't be able to defend themselves: it is our responsibility to make this new world fair towards them as well.

As for biometrics, for example, we saw above that it is not clear whether they provide a suitable technical answer to the authentication problem in ubicomp. Assuming they did, though, it would still be unwise to adopt them without a critical assessment not just of their security (in the narrowly technical sense) but also of their side effects. A hypothetically perfect biometric authentication method, non-intrusive and with negligible false positives and false negatives, would always yield the unforgeable identity of the user at each attempted access.

But a side effect of user authentication is a proof that the authenticated individual was accessing the service at that time and, at least in most cases involving biometrics, that the user was physically there at that time. This side effect may not be intended, but it is inescapable. It becomes dangerous if, perhaps owing to auditing requirements, that information is not thrown away immediately. The pervasiveness of devices requiring authentication would then cause users to leave around very explicit and detailed trails of their whereabouts and activities.

Concerns about this kind of issue are often dismissed with superficial comments to the effect that "only dishonest users have anything to hide" and that honest ones will never worry about disclosing where they have been. Such a comment is arrogant and short-sighted. The fact that you were not doing anything illegal should not automatically mean that you have no reason to retain your right to decide who gets to know precisely what you did over the past month on a minute-by-minute basis. Giving up this right, and welcoming complete observability, is akin to welcoming thought police—after all, by the same argument, why would an honest individual worry about thought police?

A comment I always found inspiring was offered in 1996 by Phil Zimmermann [12], creator of PGP. It was originally about Clipper (the infamous "key escrow" mechanism by which the government would have been able to wiretap encrypted communications), but applies equally well to the subject discussed above:

> When making public policy decisions about new technologies for the government, I think one should ask oneself which technologies would best strengthen the hand of a police state. Then, do not allow the government to deploy those technologies. This is simply a matter of good civic hygiene.

It would be irresponsible for us to build a pervasive computing world that could easily be misused as surveillance infrastructure. As Zimmermann himself remarks elsewhere in the same piece, this would also remove the feedback mechanism by which a healthy society can get rid of bad laws, or of bad lawmakers. The simple-minded comment that "if you don't do anything illegal you have nothing to hide" actually depends on the definition of "illegal", which may change much more rapidly and dramatically than a deployed information infrastructure. Think of what counts as "illegal" not just in your country today, but in a dictatorship. Protecting privacy and anonymity is also a system-level safeguard to protect free speech from the censors.

It would be evil if pervasive surveillance were built into ubicomp on purpose, but it would be tragically idiotic if this just happened by negligence—simply because thinking of appropriate safeguards was too hard and therefore too expensive.

It is also irresponsible for technologists to assume that, if nobody complains, there is no problem. Often the public does not complain because it lacks the technical astuteness even to *see* the problem—but it would complain if only it understood what is at stake. I have been in the privileged position of spending a decade in a research environment equipped with a system to track the location of

personnel in real time [2, section 2.5]; this gives me a unique perspective on the relevant privacy issues based on actual *experience*, as opposed to speculation and conjecture. From this point of view it is interesting to note that many visitors to our laboratory, when first introduced to our Active Badge [13] and Active Bat [14] systems, used to voice concerns about the privacy implications of divulging one's location information; but none of them had any second thoughts about voluntarily carrying that global location-tracking device known as the *mobile phone*! So mobile phones might easily raise concerns of location privacy, if only users realized that the devices continuously report their geographical location[3]. One of the great merits of the Badge and Bat projects in this context was to make the issue visible and explicit.

Beresford and I [15] are currently studying location privacy, based on the experimental setup of the Active Bat but keeping in mind applicability to other location systems including those based on mobile phones. We have been working both on protection techniques and on measurement techniques to assess the actual strength of the protection that can be provided.

For another example of the necessity to think about a fair policy before attempting implementation, let's go back to the digital recordings of my lectures (see section 2 on page 7). The risk that a DRM infrastructure such as TCPA might be abused [10, question 11]) is so great that it is probably unwise to accept its deployment in the first place. But even if, as a society, we decided to grant Hollywood the right to control the distribution of the content it produces, then why shouldn't individuals be granted the same right for *their* own creations? In other words, why shouldn't you be able to control, with similar mechanisms, who gets access to the songs you compose, the novels you write, the photographs you take? (And of course you should be free to choose whether to charge for such access or not; your policy wouldn't have to be the same as Hollywood's.) Why should this right only be granted to you if you accept the intermediation (and taxation, and potential censorship) of a Hollywood member? Think back to the Web and to the unquestionable libertarian[4] revolution it triggered by giving everyone the option to become a publisher. If we built a world in which access to digital content were ubiquitously governed by DRM systems, then giving Hollywood the *exclusive* licence to publish would mean a return to the digital Middle Ages. Giving the same digital authorship rights to all individuals, instead, would restore some of the freedom that the Web originally introduced.

[3] Awareness of this fact is slightly higher now, as a consequence of the published requirement of being able to trace emergency calls from mobiles. But, in the mid-1990s, very few members of the general public understood that they could be located through their cellular phone.

[4] To avoid potential misunderstandings: I use this word in the etymological sense of "in favour of liberty", without any of the right-wing overtones it might suggest to some US readers.

5 Conclusions

Pervasive computing is happening. Computers already pervade our society and our lifestyles. More computers will integrate into more everyday objects. We are inevitably making ourselves more dependent on the machines. But there is no reason to see this as a bad thing, so long as we choose the rules and foresee the consequences.

I invite the reader to rethink about security for pervasive computing by challenging any implicit assumptions. What needs protection, and why, and from what threat, and for whose benefit? An awareness of the big picture is necessary to allow us to build a pervasive computing world that is empowering and liberating, rather than irritating and oppressive.

By being professionally active now in this field, we are blessed with a unique chance to create a new world. This brings along exciting opportunities, but also great responsibilities. Let's think about policy before burying our brains in the details of implementation, and let's think about fairness towards the future inhabitants of this new world before agreeing to any policy.

6 Acknowledgements

I am grateful to Alastair Beresford, Richard Clayton, Bruno Crispo, Jon Crowcroft and Stewart Lee for their comments on a previous draft of this paper, as well as to several attendees of the Symposium for resonating with me on these issues.

Going up a level, I am also grateful to all the responsible computer professionals (some of whom appear in the bibliography) who are raising awareness of the security issues of ubicomp. Above all, I especially thank those who are already devoting their skill, expertise and creativity to the development of ethical solutions to these problems.

References

1. Mark Weiser. "The Computer for the Twenty-First Century". *Scientific American*, **265**(3):94–104, Sep 1991. `http://www.ubiq.com/hypertext/weiser/SciAmDraft3.html`.
2. Frank Stajano. *Security for Ubiquitous Computing*. John Wiley and Sons, Feb 2002. ISBN 0-470-84493-0. `http://www-lce.eng.cam.ac.uk/~fms27/secubicomp/`.
3. Ross Anderson, Frank Stajano and Jong-Hyeon Lee. "Security Policies". In Marvin V. Zelkowitz (ed.), "(untitled)", vol. 55 of *Advances in Computers*, pp. 185–235. Academic Press, 2001. ISBN 0-12-012155-7.
4. Ross Anderson and Markus Kuhn. "Tamper Resistance—A Cautionary Note". In "Proc. 2^{nd} USENIX Workshop on Electronic Commerce", 1996. ISBN 1-880446-83-9. `http://www.cl.cam.ac.uk/~mgk25/tamper.pdf`.
5. Oliver Kömmerling and Markus G. Kuhn. "Design Principles for Tamper-Resistant Smartcard Processors". In "Proceedings of the USENIX Workshop on Smartcard Technology (Smartcard '99)", pp. 9–20. USENIX Association, Chicago, IL, 10–11 May 1999. ISBN 1-880446-34-0. `http://www.cl.cam.ac.uk/~mgk25/sc99-tamper.pdf`.

6. Michael Roe. *Cryptography and Evidence*. Ph.D. thesis, University of Cambridge, 1997.
`http://www.research.microsoft.com/users/mroe/THESIS.PDF`.
7. Ross Anderson. *Security Engineering—A Guide to Building Dependable Distributed Systems*. John Wiley & Sons, 2001. ISBN 0-471-38922-6.
8. Lisa Thalheim, Jan Krissler and Peter-Michael Ziegler. "Body Check: Biometric Access Protection Devices and their Programs Put to the Test". *c't*, **11**:114–??, 22 May 2002. `http://www.heise.de/ct/english/02/11/114/`. Originally in German, but translated into English at the URL provided.
9. John Gilmore. "What's Wrong With Copy Protection", 16 Feb 2001. `http://www.toad.com/gnu/whatswrong.html`. Originally posted to the mailing list `cryptography@c2.net` on 2001-01-18 in response to an invitation by Ron Rivest.
10. Ross Anderson. "TCPA / Palladium Frequently Asked Questions, Version 1.0", Jul 2002. `http://www.cl.cam.ac.uk/users/rja14/tcpa-faq.html`.
11. Richard Stallman. "Can you trust your computer?", 21 Oct 2002.
`http://newsforge.com/newsforge/02/10/21/1449250.shtml?tid=19`. Also archived at `http://www.gnu.org/philosophy/can-you-trust.html`.
12. Philip R. Zimmermann. "Testimony of Philip R. Zimmermann to the Subcommittee on Science, Technology, and Space of the US Senate Committee on Commerce, Science, and Transportation", 26 Jun 1996.
`http://www.cdt.org/crypto/current_legis/960626_Zimm_test.html`.
13. Roy Want, Andy Hopper, Veronica Falcão and Jonathan Gibbons. "The Active Badge Location System". *ACM Transactions on Information Systems*, **10**(1):91–102, Jan 1992.
`ftp://ftp.uk.research.att.com/pub/docs/att/tr.92.1.pdf`. Also available as AT&T Laboratories Cambridge Technical Report 92.1.
14. Andy Ward, Alan Jones and Andy Hopper. "A New Location Technique for the Active Office". *IEEE Personal Communications*, **4**(5):42–47, Oct 1997.
`ftp://ftp.uk.research.att.com/pub/docs/att/tr.97.10.pdf`. Also available as AT&T Laboratories Cambridge Technical Report 97.10.
15. Alastair Beresford and Frank Stajano. "Location Privacy in Pervasive Computing", 2003. Accepted by *IEEE Pervasive Computing*. To appear.