Journal of Universal Computer Science, vol. 1, no. 1 (1995), 35-47
submitted: 8/10/94, accepted: 20/12/94, appeared: 28/1/95

Levels of Anonymity

Bill Flinn
(Computer Science Department, University of Auckland,
Auckland, New Zealand
b_flinn@cs.aukuni.ac.nz)

Hermann Maurer
(Institute for Information Processing and Computer Supported New Media,
Graz University of Technology, Austria
hmaurer@iicm.tu-graz.ac.at)

Abstract: In this paper we make a first attempt at systematically investigating levels of anonymity required in networked computer systems: we feel it is often overlooked that beyond such obvious cases as identified by means of a password" or "anonymous use" there are many other levels of anonymity, identification and authenticity necessary in various applications.
Key Words: security, anonymous use, access control, authentication, big brother
Category: C.2.0, D.4.6, K.6.5

1 Introduction

At present, most users of computers are usually aware of two modes for operation within a computer system:

- Logging on with user-id and password. (The standard way of operating any networked computer systems.)
- Using the computer anonymously; in this situation the user is unidentified, and does not have to provide a password. (This latter version, maybe first introduced in the Austrian videotex systems [Maurer 84] is becoming increasingly propular with Internet services such as anonymous FTP to download files or with networked multimedia systems such as Gopher, WAIS, WWW or Hyper-G, see [Maurer 92] or [Kappe 93])

However, there exist many alternative modes for interaction with a computer system. In this paper we will identify several such modes and show their appropriateness in the context of particular applications.

2 An overview of possible levels

Level 5. Super-identification. Here the user must be authenticated; i.e. the user has to be identified uniquely to the system in a completely secure way. Ideally, no-one can impersonate a user, and all transactions carried out by each user are associated unambiguously with that user (maybe even a complete audit trail is kept). This might e.g. be necessary in a commercially sensitive environment, particularly where a company is operating large mainframe systems which may be accessed (and modified) by large numbers of users.

In a wider context, and looking more from the point of view of the user, consider the problem of ensuring the authenticity of information acquired from a computer system or network, or determining that a message purporting to be from a particular person really is from that person. More generally, how can a user validate the credentials of an author of an article which is undergoing electronic distribution? These situations require total identification (and therefore zero anonymity). This may be provided directly i.e. suppliers of such information may be required to identify themselves completely, or alternatively the information may be supplied under the auspices of some some third party organisation which could guarantee the authenticity of such information that it provides.

Oberve that with super-identification there are a number of completely different issues involved:

- identification of a user vis-a-vis a system (so that the "system" is assured that this is indeed a duly authorized user; passwords may not be safe enough for such purpose as we will discuss later)
- identification of a user vis-a-vis another user (so that the receiver of an email or reader of a file does indeed know for sure who the originator of the file is; special cryptographic protocols like digital signatures [Salomaa 90] may be useful to achieve this aim)
- objective knowledge about the person or organisation associated with an identification (so that the user knows that person X is indeed "qualified" to write about topic Y; this may require a third party broker as mentioned above).

Level 4. Usual identification. The user is known within the system by a user-name and associated password. The user has to log on with this user-name and use the correct password to be admitted into the system. This is typically the case today for multiple user systems.

Level 3. Latent (potential) identification. Here the user is known as person to the system. Each user may develop a set of pseudonyms. These sets of pseudonyms are mutually disjoint (so two distinct users may not share a given pseudonym). Distinct users cannot directly identify other users using the computer system; however the system has exact knowledge of each user. This mode is used in some computer assisted instruction (CAI) settings and electronic bulletin board discussion forums.

Level 2. Pen-name identification. The user is known within the system by some user-name, but there is no proper identification of the user as person. Users log on with their pen-name, and using a password. Again multiple pseudonyms can be used. Mail may be sent to such a user (pen-name). This mode may also be used for bulletin board systems; some game playing systems operating on networks such as Internet employ this technique, too.

Level 1. Anonymous identification. Here the user is identified by the system, but not as a specific individual and without pen-name, i.e. is not "addressable". Typically, a user logs on anonymously (probably using a password), and the system keeps a log of events engaged in by that particular user. This allows the system to tailor its interactions with the user according to the log - for example in a museum visitor system.

Level 0. No identification of user. This is the usual situation in using a PC; however even here there is the possibility of an application which keeps a log as in Level 1 and tailors its interactions with the user accordingly. Such so-called "intelligent" applications , or more precisely, applications utilising intelligent agents, will certainly proliferate as processing and memory power of PCs increase.

We observe that the existence of a log as in Levels 1 and 0 provides a kind of profile of the (unknown) user, and can be used by a third party to gain information about user behaviour. In this regard, true anonymity would even go beyond that and would correspond to the absence of any personal history within the system or application.

3 Detailed discussion of various levels

3.1 Level 5

Super-identification may be required either by the computer system or the application being accessed, or by a user attempting to access information across a network, or communicate securely with another person across such a network (maybe in a far away location).

With currently applied technology, particularly in regard to Internet, it is impossible to guarantee authenticity of this kind unless cryptographic protocols are used [Salomaa 90]. Generally today, Internet users are identified by their email (electronic mail) address. It is possible to forge the originating address of a message, either by corrupting the mailing software itself, or by connecting via telnet to the sendmail socket of another machine on one's local network, and typing in a mail message which purports to come from someone else. It is also possible, although much more difficult, for a message to be intercepted en route and modified. This requires the interceptor to have access to network nodes en route and to be able to access and modify the system software which is forwarding mail. This would appear to require resources beyond most individuals (although not necessarily beyond government agencies).

In the near future, it will be possible to embellish electronic communications with facial image and voice data. However in itself this will not resolve the authenticity issue, because these can be modified or forged as readily as text! Already forged and reconstructed images are regularly posted in Internet newsgroups.

In order to guarantee authenticity and privacy of electronic communications it is necessary to use cryptographic techniques. There is currently much debate on the use of crytography, particularly in the US, largely because of governmental desire to be able to monitor electronic communications. As stated in [Detweiler 93]:

"To date no feasible system that guarantees both secure communication and government oversight (monitoring) has been proposed (the two goals are largely incompatible) ... Electronic privacy issues, and particularly the proper roles of networks and the Internet, can be foreseen to become highly visible and explosive over the next few years". For an easy to read introduction on the state of the discussion of the "Clipper Affair" see [Time 94].

3.2 Level 4

This kind of identification is currently the most commonly used means of access to a computer system or network. The reasons for this are largely historical; when timesharing systems were originally set up, it was necessary to ensure that only those users who were properly entitled could access the system and use system resources. In particular, a check had to be kept for accounting purposes on the scope of each user's activities. In fact computer users today who work on company or other institution computer systems are largely subject to the same disciplines. However with the advent of large-scale computer networks and ever more powerful personal computers, both in terms of processing power and disk storage space, the situation is changing and it is with these developments in mind that the considerations to follow become relevant.

3.3 Levels 1-3 for partial anonymity

In keeping with the theme above, partial anonymity corresponds to partial identity. There are a number of reasons why an individual might wish to use a computer system in a partially anonymous way.

First, a person may wish to be consistently identified by a certain pseudonym or "handle" and establish a reputation under it in some area. The pseudonym would in some sense 'belong to' that person. In order to ensure that only one particular person could use a particular pseudonym requires a controlling application. This controlling application may or may not require exact identification of its users. These situations give rise to levels 3 and 2 respectively.

Second, a person may wish to be anonymous as person but carry on a conversation with others (with either known or anonymous identities) via an anonymous return address. This is level 2 anonymity.

Third, users may wish to make public certain important and sensitive information, but to do so in a way that makes them untraceable because to do so openly might jeopardise their lives or those of their families in some way. This would require the user to be completely anonymous (Level 1 or even Level 0). However, information publicised without being able to trace the originator is probably only possible for small groups (like in decision room situations) but is not viable for public services such as Videotex in Europe, or Internet: such anonymity tends to lead to personal slander, to the violation of laws (such as on pornography, or on encouragmenet of criminal actions, etc.). In most cases Level 3 anonymity is required here.

Fourth, a user may wish to make use of an electronic service and hide all signs of this usage, for reasons of privacy. See for example [Maurer 84].

Fifth, during the use of a certain application (even across session boundaries) users may want to keep track of their actions: to get an objective evaluation by some CAI package at the end of a number of sessions (yet without anyone having a way to establish a connection between the performance achieved and a particular person), or by visitors of e.g. the Franklin Institute at Philadelphia or the Information Age Exhibit of the Smithonian at Washington who have the option of printing information concerning their visit on exiting.

3.4 Level 0

This basically corresponds to turning on a PC that is not password protected: The default situation for use of PCs is for files etc to be accessible to whoever happens to switch the machine on. The user in this case is completely unidentified. Even if files etc are password protected, there is no real notion of the identity of the user. In the absence of such identity, we have true anonymity, with the proviso that no logs are kept as discussed at the end of Section 2.

3.5 Rationale for anonymity

Allowing users to access a computer system anonymously has a number of possible consequences; we shall discuss these in general here, and consider them in more detail later in this paper, where we consider several specific example applications.

On computer bulletin boards and in other discussion forums such as decision rooms - see later - opinions and ideas can be put forward anonymously. Many people find it easier to put forward ideas in this way, particularly if they are unsure of themselves or of their ideas. One may have an idea which one is not sure about, and by floating it for discussion, very quickly get some useful feedback. Again in a discussion forum, a single individual using two pen-names may put forward two opposing sides of an argument to spark discussion. This doesn't necessarily require anonymity; however there are situations where this anonymity makes it easier to put forward the ideas. The freedom to publicly air one's point of view has a long tradition in several countries. In certain situations citizens are allowed the right to speak their minds on any topic. Speakers Corner in Hyde Park, London is a prime example. Soapbox orators in such a situation are not required to identify themselves to a watching policeman - unless they break the law.

Again in public arenas like computer bulletin boards, there are advantages in being able to converse and get to know people anonymously.

The ability to express a proposal anonymously has definite advantages in an employment situation or heavily politicised arena. Most employees do not feel able to put forward ideas, no matter what their merit, in the presence of a boss who is known to strongly disagree with those ideas. In Parliament, it is not generally possible for members of a particular party to view objectively a proposal coming from "the other side" - or indeed one coming from their own party. Anonymous interactions allow ideas to be argued about and to stand or fall on their own merit, rather than on the status and power of the individuals concerned.

Another benefit of anonymous interactions is the user's privacy. For example, as pointed out in [Maurer 90], why should a user suffering from cancer who is desperately searching the medical pages in a videotex system for help be required to identify him or herself? Such users are unlikely to want their database accesses logged. Again there is the every-day analogy of the public library; it is not usually necessary to identify oneself before going to consult a book on a publicly accessible shelf. Extending the analogy, the Internet itself, viewed as an information resource, may be considered as a huge library. Like many large libraries, it will contain information that may be considered offensive by some users but interesting to others. If we do not believe in censorships in libraries (and the authors of this paper don't), such potentially offensive material should be accessible if someone actively searches for it (and only then!), yet anonymity might well be desirable to avoid embarassement or fear of reprisals.

Of course there is a downside to anonymous usage, particularly with respect to bulletin board systems and indeed any publicly accessible network or computer system: allowing users to voice opinions anonymously means that any and every perverted viewpoint can be expressed - much as currently occurs on a wider scale with graffiti on public lavatory walls. The electronic versions of lavatory graffiti include pornographic images, racist attacks, slander, and incitement to commit criminal acts. It is interesting to observe that the situation is somewhat blurred by the fact that networks are now globally accessible, and as of now, and probably for the forseeable future, there are disparities in law between countries. One immediate example is in the area of cryptography; the RSA public key encryption method is patented in the US, but not elsewhere in the world. There are a number of sites on the Internet which hold copies of an application program called PGP (for Pretty Good Privacy). PGP uses RSA's patented algorithm, and so is legally unable to be used by US citizens, yet perfectly legal outside the US.

It is the fact that anonymous usage of public systems below Level 3 has often led to much misuse that we strongly propagate Level 3 for public discussion and have indeed implemented this version in the E.R.D.E., the electronic discussion corner of the Austrian Videotex system: although users are anonymous with respect to each other, an encrypted record of the real identity of each user is kept, allowing to determine the identity of a penname if a court-order is issued. This limited amount of "non-anonymity" is known to the users and has been successful in preventing serious misuse of the system.

In general we are in a much better position with computer systems and networks to enforce decency and at least local legality than the hapless custodians and users of public lavatories. It is possible to use identification at several levels. For example, akin to what has been described for the E.R.D.E., in order to make use of a particular system or network, a user can be required to identify themselves completely. Then the user can choose one (or several) pen-names and, once the pen-name has been associated with that particular user by the system, users can then make use of the bulletin board or other system using one of their associated pen-names. Other users are not able to identify the user from a particular pen-name in the usual course of events. However if a user were to violate the conventions of the system or institution or the laws of the country in which the server resides, some authority could be invoked to retrieve the connection between the anonymous pen-name and the actual user.

For a network like Internet, which operates internationally, however, the situation has proved rather more problematic. Within the Internet community, many people feel very strongly about the issue of anonymity. At the time of writing, there is at least one anonymous server in operation in Finland, but the future of such servers, and anonymous services in general, is extremely uncertain. Several such servers have been closed down in the recent past, either voluntarily by their operators or forcibly by higher authorities. An anonymous server operates by assigning an anonymous identity (pen-name) to a user who requests such an identity. The user may protect usage of their pen-name via a password. From then on, the user can communicate with other people or newsgroups on the internet, using only their pen-name. Any such message appears to originate from the anonymous server.

Strong opinions in favour of such anonymous services come from people seeking advice or therapy over the net, or advertising in 'Personal' ads. Strong opinions against come from people who have been attacked or slandered anonymously, and from those who feel that no sanctions can be brought to bear against an anonymous user who violates the ethical code of the Internet or indeed acts illegally. Several newsgroups have adopted a policy of filtering out all anonymous messages. This policy is difficult to automate however, because automation relies on detecting certain characteristics of the incoming message, and these can be altered by the anonymous server.

As stated in [Detweiler 93], the future of anonymous services on the Internet is extremely uncertain. There are strong forces for and against anonymity. However, from network traffic statistics, it appears that there is a large demand for anonymous services. Several thousand messages per day pass through the anonymous Finnish server mentioned.

When communicating electronically in a situation where pen-names are being used, it is possible for users to not only conceal their identity, but also to project a completely disguised persona. For example, one can appear to be of a different sex, different profession, etc. Such an ability to disguise oneself may be beneficial but clearly it may also be abused.

In many ways, being able to hide "superficial" features such as looks or some physical handicap encourages communication between persons who would never start to communicate, otherwise. Persons who would never meet otherwise first meet electronically, start to like each other and end up setting up real-life rendezvous.

A celebrated case is the case of a paraplegic girl who made friends via the Austrian Videotex network, giving away her physical problems only after having established quite a "fan club". When that fan-club finally met in person with her (the second author was amoung them) the usual problems of a healthy person confronting a handicapped one, i.e. the usual mixture of pity and not-knowing how to react (stifling any real contact) was completely absent.

How often do persons (men in partiuclar?) react on the basis of looks, rather than on other at least as important values? How often are people intimitated by the position of a person, turn to flattery because of the wealth of someone involved, etc. How many movies are there where a rich guy pretends to be poor just to make sure he is loved for his own sake, not for his money! Well, electronic pen-name based contacts do have exactly this property of disregarding some superficial layers: we like a person electronically because we like the ideas, the wittiness, the softness, the kindness ... and are neither distracted by looks, age or other external features. One of the authors has coined the term "electronic shards" [Maurer 93] to describe the phenomenon of persons inadvertently revealing facets of themselves during extended electronic communications. One can form a partial picture of such a communicant, in the same way that one forms an image of an ancient vase by seeing a broken fragment of the whole. Thus, it is not surprising that pen-name based electronic communication has lead to many deep relationships.

On the other hand, the idea of pen-names can also be misused. An interesting example is detailed in [van Gelder 85]. This concerns a persona known on the CB channel of the Compuserve network as "Joan". Joan supplied an elaborate biography about herself to others on the network, and over a two year period (1983-1985) became a major on-line presence. She presented herself as a severely disabled neuropsychologist who was using the computer network to communicate and make friends with others on-line. She did this so successfully that over this period she served both as a support for other disabled women and as an inspiration to the able-bodied. It was a great shock to her intimate on-line pen-pals when it transpired that in real life Joan was not disabled at all - and in fact was a prominent male New York psychiatrist. What had apparently begun as an experiment had escalated out of control over an extended period of time. "Joan", despite her supportive friendship to others, had clearly violated their trust.

While this particular case seems clear-cut, there are delicate issues involved here. Perhaps newcomers joining electronic networks should be warned ahead of time that any data presented to one across such a network may not be as it seems. However there is also the situation to consider where a user deliberately misleads others for personal gain. If there are as yet no laws in place to deal with this kind of misrepresentation, there surely will be in the future. Once again there are implications for international law.

At the pen-name level, it is still often the case that users inadvertently reveals their identity, at least to other persons who know their "electronic style" – much as an expert chess player may be able to identify a player from a game record, simply by knowing that person's style of play. Indeed on the chess and go servers on the Internet, where players are not required to make their identity public and may play under several pen-names, there is often discussion between the kibitzers as to whether player "x" is really the same as player "y". (For Chess servers see ics.ucknor.edu 500 or 130.225.16,82 500; for Go servers see flamingo.pasteur.fr or hellspark.wharton.upenn.edu).

In order to remain totally anonymous, it would thus appear that a "style scrambler" is required. It is an open question whether such a scrambler could be automated: we are investigating this further. The idea is to define a set of syntactic parameters which might be used to modify a text message, or sequence of such messages. Such parameters might include: gender of author, use of upper case letters, punctuation devices, ranges of spelling errors (set at one of a number of levels). Each pseudonym would appear consistent, but there would be no relationship between pseudonyms. There are several variations on this idea, for example the user might choose a set of parameters, or alternatively, the system could randomly allocate a set. Thus, we may at some stage be able to establish two different pen-names with sufficiently different "style-parameters" to disguise that the two pen-names belong to the same person!

3.6 Implementation

Ensuring the high degree of identification (and authentification) at Level 5 requires cryptographic techniques as discussed in [Chaum 85] and [Salomaa 90]. Briefly, the ideas are as follows: Each person communicating within the system does so using a digital signature. This term is a little misleading, since it refers to a complete message which is encoded using a pair of keys, one private and one public. One important property of digital signatures is their resistance to forgery. To decode a message in digital signature form without knowledge of the private key using currently available techniques is regarded as an infeasible computing problem. From the standpoint of this article, digital signatures have a further important property; they can be extended to blind digital signatures which as well as being secure are also anonymous. This will be discussed further in the Section below.

As Level 4 is the standard mode we will not consider it further, except to note that in many systems, administrators have power to access all files. As a result, security may be significantly undermined, so the whole rationale for identification with user-id and password becomes weakened. This situation could be improved by requiring at least two people to co-operate to gain access to user files.

Level 3 identification is implemented as follows: In order to be admitted to a system, the user has to log in and be identified in the usual (level 4) way. A first time user then chooses a pseudonym, which the system confirms available or not. Existing users may also add to their set of pseudonyms.If the pseudo is available (not already associated with a user), the system asks the user to choose a password to go with that pseudonym. From then on the user may interact with the system using the pseudonym plus password. The system keeps an encrypted file connecting each user-name with the pseudonyms chosen. If a public and private key encryption mechanism is being used, the keys can be kept separate as an additional security measure. As mentioned above, normally the connection between pseudonyms and user-names remains secret; however in exceptional circumstances the link can be made explicit.

Level 2 identification is maintained by the system maintaining a file which links pen-names to passwords. Messages can be transmitted between pen-names, or stored by the system and made available to users when they next log on using their pen-name with password.

Level 1 identification is maintained by the system independently of the users, whose only knowledge of it is via their log-on character sequence (name or password). See the museum visitor system example below.

4 Applications

4.1 Once more: Level 5

For a number of applications top-notch secure identification is crucial. The first wide-spread application where this became apparent was telebanking via systems such as Videotex in Europe, now used by well over 5 million customers.

Initial ideas of using a sequence of two pass-words were discarded in favor of one-time TAN's (TransAction Numbers). The advantage of TAN's is that even a "spy" observing the log-in process and the TAN cannot make use of the TAN, since it is only good for one transaction.

Modern cryptographic protocols involving so-called zero-knowledge proofs might provide even more elegant solutions: a user can be identified with certainty without ever revealing the password! [Salomaa 90].

4.2 Some example applications

The first example we consider is a system due to David Chaum ([Chaum 85]) for making payments to an organisation for goods or services. In this system a consumer wishing to make a purchase for say \$100 would do the following. First, using digital signatures, users would instruct their bank to deduct \$100 from their account and issue a "certificate" worth \$100. This certificate is in fact just a number which has the properties that

- It is constructed by both the user and the bank.
- (Although the bank is guaranteeing the authenticity of the certificate, it does not know the final number (and therefore to which user it was supplied). This is the concept of the blind digital signature.
- It can be validated by a third party and the bank as being a genuine certificate.

This certificate would then be presented to a third party in payment for goods or services. This third party then presents the certificate to the bank for payment. Such a certificate is like a cash note that has a valid serial number but not the number under which it is circulated from the bank. Although the consumer has to initially identify himself to the bank, the payment process itself is totally anonymous in that the number issued by the bank cannot be linked to the number supplied in payment, which can only be checked for validity (and that it has not been previously presented).

Our second example is a system for anonymous delivery of goods. Following [Maurer 84], the idea is that a user ordering merchandise x from company 'A' chooses two passwords 'p' (public) and 's' (secret) and a post office 'm' for delivery. Company 'A' sends merchandise x to post office m. The merchandise has 'p' visibly marked on the outside and inside has a sealed envelope containing 's'. The user goes to post office 'm', asks for the parcel labelled 'p', and presents his secret password 's'. If this matches with the password inside the sealed envelope the post office releases the merchandise.

Notice that this system, combined with the first example, allows for completely anonymous purchase and delivery of goods, in marked contrast to current systems involving credit or debit cards, which contain complete histories of customer usage, thus allowing detailed profiles of user spending patterns to be constructed.

For our third example we consider electronic discussion and games corners. The E.R.D.E. discussion corner and its Level 3 anonymity has been mentioned already above. Early versions just using Level 2 did not work: there was too much slander, abuse and often shrill arguments.

In a similar fashion a Level 3 server for chess in the Austrian Videotex system is working well, but similar Level 2 servers for Chess and Go seem to be running into problems. The Internet Go-server mentioned earlier is one such example: several anonymity issues arise: many people using the server are upset at others actions, including denigrating other players, antisocial behaviour while playing games etc. There is an interesting clash of cultures also: New York "street language" versus professional go players precisely formal interactions. Several professional players have become so incensed at comments of kibitzers that they regard as intolerably rude that they have refused to play again on the server. Anonymity is a rather peripheral issue here, although some users have felt that bad behaviour was being accentuated by anonymity. All in all though, it seems to prove that Level 3 should be used if a large number of persons is involved, rather than Level 2.

For our fourth example we look at software systems which are known variously as Decision Rooms, Group Support Systems or Electronic Meeting Support Systems. See for example [Nunamaker 91], [Sheffield 93], [Visotschnigg 85]. In particular we consider some findings of the Decision Support Centre established at the University of Auckland in 1990. In the Decision Support Centre, face-to-face meetings are augmented with each participant in a meeting able to converse via a workstation as well as in the normal way. Meetings are guided by a trained facilitator. The actual meeting process is a combination of facilitated group discussion, and the use of a software system to collect and organise ideas from all group members. Participants in the meeting are able to switch between "public" and "private" windows. Comments on a particular topic are entered in private windows and may shortly afterwards be viewed by all participants via their public windows. The public display of messages is anonymous. In [Sheffield 93], the following results for meetings of this type are reported:

1. Because the ideas are presented anonymously, each idea must speak for itself. Unlike a conventional face-to-face meeting, attention is focussed on the content of the message rather than its form (which essentially involves its originator).
2. The sending of an unpopular message may or may not be a personal attack. In a normal face-to-face meeting, social and emotional damage may result as the receiver may feel duty bound to defend him/herself by making remarks to avoid loss of face which may escalate the conflict. The anonymity which ensues when the messages are communicated on screen assists in depersonalising these attacks.
3. All participants can send and receive as they feel like it; consequently there is no need for speakers to play to the gallery, hold the floor or generally over-dominate the group.
4. Participants can report bad news or a state a point of view that they know will be unpopular without fear of being "stamped on" by superiors.

We observe that the software system used at Auckland ensures that the messages are presented completely anonymously. There seems no reason in principle why such a system should not operate with a variety of modes - say from Level 3 down to Level 0.

Our fifth example looks at anonymity in an educational setting, where the facility to have an anonymous electronic discussion removes the authoritarian role from the teacher or lecturer and enables the more diffident students to advance ideas without threat. Perhaps the most useful mode here is level 3. The teacher may wish to review or assess the degree and quality of statements and ideas expressed by participants, and in order to do this needs access to the system records to link pseudonyms to actual student ids. One very useful aspect of being able to use multiple pseudonyms comes into play in this example; the teacher (or any other participant) is able to present several different viewpoints or sides of an argument using different pen-names. We feel that this is particularly valuable in an educational setting : it would appear a useful skill to be able to look at an argument (or scientific theory, or hypothesis) in the round, without being forced to be identified with or even to strongly hold a particular point of view. What is important is being able to marshal the appropriate facts to support or cast doubt on a particular hypothesis. Using the physical world as an analogy, it is generally accepted that in order to fully perceive or appreciate an object such as a mountain, we need to perceive it "in the round". We are advocating a similar approach to understanding ideas and concepts. Students might be encouraged to assume different standpoints and to construct supporting arguments. In [Lennon 94] the case of Level 2 is recommended for certain learning situations.

For our sixth example we consider a museum or exhibition visitor system. In this system, on entry to the museum, visitors acquire a card which they plug into card slots as they move about the museum. The computer system keeps a history of the visitors movements and thereby is able to 'personalise' various interactions such as languages or which parts of a recording are played at which exhibit. In this way visitors are spared needless repetition and can even be assisted with information about additional exhibits related to their interests as the system develops knowledge about them. In order to carry out the above, all the system requires to identify the users is a number on the card, perhaps together with a pseudonym chosen by the user as a form of address (also stored on the card). The visitor's history could be stored on the card (preferably), or centrally in the system's computer. This is an example where Level 1 identification is appropriate.

5 Concluding Remarks

Applications of modern computer networks require a rethinking of how anonymous users should be for various applications. We have made a first attempt to point out some of the issues involved and hope that this will stimulate further work and discussion.

Thanks are due to Bruce Benson who helped us figure out some of the intricacies of e-mail and the Internet.

References

[Chaum 85] D. Chaum: Security without Identification: Transaction Systems to make Big Brother obsolete, Communications of the ACM, October 1985, pp 1030 - 1044.

[Detweiler 93] L. Detweiler: Privacy and Anonymity on the Internet FAQ, sci.crypt newsgroup (Internet).

[van Gelder 85] Lindsy van Gelder: The Strange Case of the Electronic Lover, Ms Magazine, October 1985, pp 364 - 375.

[Kappe 93] F. Kappe, H. Maurer, N. Scherbakov: Hyper-G – A Universal Hypermedia System, J. EMH 2, 1 (1993), 39-66.

[Lennon 94] J. Lennon, H. Maurer: Lecturing Technology – A Future with Hypermedia, to appear in: Educational Technology (1994).

[Maurer 84] H.A. Maurer, N. Rozsenich, and I. Sebestyen : Videotex without "Big Brother", Electronic Publishing Review 1984, Vol. 4, No. 3.

[Maurer 90] H. Maurer: Privacy and security on videotex systems, New Media: Communication Technologies for the 1990s.

[Maurer 92] H. Maurer: Why Hypermedia Systems Are Important, LNCS 6022, Springer Pub.Co. (1992), 1-15.

[Maurer 93] Die Elektronischen Scherben, Maurer's Meinung 153, Austrian Videotex *MAURER###4.

[Nunamaker 91] J. Nunamaker, A. Dennis, J. Valacich, D. Vogel, J. George: Electronic Meeting Systems to Support Group Work, Communications of the ACM, 34, 7 (1991), pp 40 -61.

[Salomaa 90] A. Salomaa : Public Key Cryptography, EATCS Monographs 23, Springer-Verlag 1990.

[Sheffield 93] J. Sheffield: The Impact of Electronic Meeting Systems on New Zealand Organisations, Vol 1 of Proceedings of the 13th New Zealand Computer Society Conference, John Hosking ED., NZCS (1993), pp 21 - 40.
[Time 94] Time Magazine: Who Should Keep The Keys?; Time Magazin March 14 (1994), 38-39.
[Visotschnigg 85] P. Visotschnigg: Verstaendigung im machtfreien Raum; P. Zolnay Pub Co Vienna (1985)