SignSpot™
You have the final say™

SignSpot Limited
West Hill House
West End
Frome
Somerset
BA11 3AD

Tel. +44 (0)1373 454220
Fax. +44 (0)1373 454221

www.signspot.org

SignSpot:
A new approach to tackling Identity Fraud

Background

Current Solutions

- **Evidential**
- **Certification**
- **Coherence**

Problems with existing methods

The SignSpot approach

- **Solution Components**
- **Registration**
- **Operation**
- **Example: Credit Agreements**

Advantages of SignSpot approach

- **Barrier to fraud**
- **Conspiracy detection**
- **Deterrent effect**
- **Resilience**
- **Voluntary participation**
- **Strength through mutuality**
- **Confidentiality**
- **Protecting the deceased**
- **Universal, consumer-friendly operation**

Background

Although the anonymity surrounding Internet transactions has drawn increased attention to the problem of identity fraud, its scope is by no means limited to this area: indeed, its history long pre-dates the world of electronic communications. Identity fraud is committed whenever an identity is assumed in order to obtain a dishonest advantage. It may involve the assumption of an innocent living person, a dead person, or even (when the intention is to conceal true identity) a wholly fictitious person. One well-established ploy is to use false or stolen documents. With the advent of electronic communications, the production of forged devices (e.g. cards) or misappropriated information (e.g. passwords) will serve the same end.

Current Solutions

Identity fraud presupposes a situation in which the parties to a transaction do not know one another, and one party (the “relying party”) seeks to verify the identity of the other. To date, solutions to the problem have followed three main routes.

Evidential

The first solution involves the production of identifying evidence. Examples of such evidence are birth certificate, bank statements, utility bills and similar documents. Their evidential weight relies on the fact that it is generally difficult to assemble a collection of such evidence unless it is already legitimately in the individual’s possession. However, an impostor may obtain such evidence by means such as theft and forgery.

Certification

The second solution involves what we might call “certification”. According to this model, the individual acquires a certificate of identity by applying to an authority with evidence of his identity. The authority checks the evidence and, if satisfied, issues a certificate. One time-honoured example of this approach has been the issuance of passports. In this case, the certificate is the passport. In order to acquire a passport, the applicant has to obtain photographs and present them in person to a reputable member of the community (the authority in this case) who either knows the applicant or who is able to assess the veracity of evidence produced by him. If satisfied, the authority signs the photographs. Trusting the authority, the passport office then issues the certificate bearing one of the photographs.

The second solution may be seen as a special case of the first. The evidence appears stronger, because the evidence has been subjected to impartial scrutiny by a trusted authority; and typically the certificate is more closely bound to the certified individual, by means of a handwritten signature, a photograph, a secret PIN or similar means.

Coherence

The third solution, which we will refer to as the “coherence” solution, is a relatively recent development. Here, identifying information volunteered by the individual is compared with a number of large databases containing identifying information. This approach relies upon the fact that in modern times, individuals interact with many institutions that build up records of identifying information. Credit records, health records, the electoral register, census returns and other large databases provide a wealth of collateral information that can be used to check identity.

ü

Problems with existing methods

All three approaches have important drawbacks. In the case of the first and second approaches, as has already been mentioned, theft and forgery are all too possible. In addition, they both impose upon the individual the burden of carrying proofs of identity. In the third, it is possible for the malefactor to obtain access to databases of identifying information and so make a convincing, though fraudulent, claim. This is particularly a problem where “insiders” are party to fraud, for example call centre staff or bank employees (see, e.g. *Data Security Chief arrested for Account Hacking* at http://www.finextra.com/fullstory.asp?id=14133).

The weakness that all three solutions have in common is that they tend to concentrate risk by seeking impersonal guarantors of identity – documents, certificates or a plurality of databases. To put it simply, they rely upon touchstones or criteria of identity that are all too easily identifiable by the impostor, who can therefore direct his resources to counterfeiting similar touchstones or satisfying the criteria. They may make it difficult, but the impostor knows exactly what he must do in order to circumvent the safeguards.

The SignSpot approach

By contrast, the SignSpot method seeks to establish identity by mapping the position of the individual in the social structure. It recognizes that individuals can only be uniquely defined by their relationships with other people, and that human relationships provide the only reliable guarantor of identity.

It also addresses the identity fraud problem from a different perspective. Instead of seeing the problem as that of a relying party who needs to identify an unknown individual, it approaches the question from the viewpoint of the individual who is at risk of identity fraud. In simple terms, it attempts to answer his question “how do I protect myself from identity fraud?”

Solution Components

The first element of the SignSpot method is a database of identity information. This information may come from different sources: for example, an institution might contribute information about members, employees or customers. Indeed, much of the information may be contributed directly by the individuals who wish to protect themselves. Much, if not all, of this information will already be in the public domain.

The second and most important element is linking information, which will in every case be contributed by the users of the system when they register for protection.

Registration

The registration process principally involves the individual identifying a number of referees chosen from his family, friends and associates. The essential requirement for a referee is that he be able to recognize the applicant in the course of a short conversation (typically, but not necessarily, by telephone). If a nominated referee agrees to act for the applicant, then a link is established. Typically this will be a reciprocal link, i.e. in the normal course of events, two people who know one another well will agree to act as referees for one another (for example, a mother and her daughter). When a referee agrees to act for an applicant, the proposed system will make a voice recording of the referee saying the applicant’s name (or nickname or other appellation normally used by the referee to refer to the applicant), and this will be stored in the system as part of the linking information.

Once a person has registered in this way, the system can be used to prove his identity.

ü

Operation

When a relying party wishes to verify the identity of an individual, it presents information identifying the individual (e.g. name and address) to the system. If the individual is registered, the system will locate him by means of the identifying information. Then, using the linking information, the system will determine the set of referees who have agreed to act for that individual. Next, the system will telephonically contact a randomly selected referee from the set and put him in telephonic contact with the first individual. When the referee is ready to identify the individual, he will indicate this to the system (e.g. by pressing a button on his telephone). The system will then ask the referee to say the individual's name. The resulting voice sample will then be compared with the recording made by the referee when his consent was originally sought. Based on whether the referee indicates that he knows the individual, and on the match between the voice samples, the system will then indicate to the relying party whether or not the individual was positively identified.

In the future, a widespread video telecommunications infrastructure may be established. It is apparent that the use of video in addition to audio would make the SignSpot system easier to use and impersonation even harder.

Example: Credit Agreements

Since credit agreements provide a particular locus of identity fraud, it may be instructive to consider an example of how the SignSpot method would apply in this case.

At the outset of the transaction, the lender would supply the system with the borrower's name, address and such other collateral information as enabled the system to identify the borrower's record in the database. If necessary, the lender would also supply a telephone number by which the system could presently contact the borrower. Having identified the borrower's record in the database, the SignSpot system would select in turn from a randomly ordered list of the borrower's referees and make outgoing calls until contact is made. The borrower and the referee will be connected together and allowed a short period to converse; at the end of that time, the referee will be asked to say the borrower's name. The voice sample will be compared with the previously stored recording and if the samples match, the borrower's identity is verified. The result of the comparison is then returned to the lender.

Advantages of SignSpot approach

Barrier to fraud

It is instructive to consider how difficult it is to perpetrate a fraud against someone using the SignSpot method. An impostor would be faced with creating and maintaining a convincing impersonation throughout the course of a live conversation, to the extent that even the victim's parent, spouse or sibling would not be able to detect the difference — assuming, that is, that the impostor had sufficient knowledge of the victim in the first place.

Conspiracy detection

It might be objected that an impostor could set up a network of bogus referees, perhaps involving a conspiracy of several people each using multiple false identities. However, it is in the nature of a conspiracy that it must be disconnected from the law-abiding majority. It will be recognized that in the typical case, people's relationships are so widespread that it is said that there are only "six degrees of separation" between any two individuals in the world. Whether or not this is true, it is clear that interconnected communities of registrants and referees will tend to establish transitive links across the whole community of registrants. It is a relatively straightforward exercise for a computer program to detect the existence of small, isolated populations, whose very existence will tend to attract suspicion, as will an individual who acts as referee for an inordinate number of people.

Deterrent effect

As well as providing a method of identity verification that is strong enough to prevent identity theft, the SignSpot method will necessarily act as a powerful deterrent to prospective fraudsters. The process of identity verification requires the subject and the referee to communicate using a telecommunications system. It would be a rudimentary adjunct to the SignSpot system, using well-known techniques, to add audit trail and reporting facilities that would enable law enforcement agencies to obtain full evidence of fraudulent activity. The very nature of the SignSpot method would be to build an evidential trail to the identity of any and all fraudulent agents seeking to misuse the system.

Resilience

Another interesting property of the SignSpot method is that whilst it uses a database of identity information, it does not place particular reliance on the accuracy of this information. If, for example, someone were to give a false address or other false identifying information, the result would simply be that the system would identify the referees (if any) corresponding to the known holder of those identifying attributes, who would of course fail to identify any impostor. This is because **the information held on the database is not used to verify identity**, but rather to identify what set of referees to contact for that purpose. In theory, therefore, an individual could be identified purely on the basis of, say, his personal telephone number; and if a relying party had independent means to associate that telephone number with the individual, the proposed system would function without the need even to know the individual's name.

Voluntary participation

It is useful to bear the foregoing point in mind when considering the motivational structure underlying the SignSpot method, and contrasting it with other personal identification methods. In the case of the evidential and "certification" methods, the relying party imposes on the individual the burden of carrying supporting evidence or certification of his identity. The "coherence" solution relies upon aggregation of personal data by institutions that are not directly answerable to the individuals concerned. By contrast, the SignSpot system uses personal information only to link the individual to his chosen referees.

Whereas the other identification systems require such specific evidence or information as satisfies the norms of those systems, the SignSpot method allows individuals to contribute as much or as little personal identifying information as they require.

For example, an individual might register his bank account or credit card numbers with the SignSpot system. Thereafter, any impostor who attempted to use that individual's stolen credit card or bank statement as evidence of identity would be automatically linked to the rightful owner's chosen referees, who would naturally detect the fraud.

Strength through mutuality

It should also be noted that whereas previous identification methods focus upon the relationship between an individual and certain authorities or institutions, the SignSpot method focuses upon the relation between an individual and his peers. The relationship between an individual seeking to protect himself from identity fraud and his chosen referees is in principle a reciprocal one, so that in practice it is to be expected that individuals will voluntarily commit themselves to act co-operatively as referees for one another.

Confidentiality

Further, the SignSpot method protects the personal confidentiality of the individual better than previous identification methods, all of which require that certain identifying information be put either into the public domain or into the hands of authorities. According to the SignSpot method, all identifying information (e.g. name, address, bank account details, etc.) volunteered by the

individual is used merely to locate the individual's chosen referees in the database. It is never necessary for any such identifying information to be disclosed.

Protecting the deceased

Preventing the identities of dead people from being assumed, particularly the recently deceased, is a considerable challenge. With existing solutions, it can be many days or even weeks before the various authorities are informed of a death and for them to have updated their databases, leaving a considerable window within which fraud can be perpetrated.

By contrast, the SignSpot method is immediately effective in preventing such frauds because the referees, being relatives or close associates, will necessarily be more immediately aware of the victim's death and detect the impostor at once.

Universal, consumer-friendly operation

Finally, the SignSpot method has the advantage that without imposing any burden on the individual, it is available everywhere and in all circumstances where it may be expedient to verify identity. The individual does not need to remember to take with him any special tokens of identity; nor does the relying party need to obtain a multiplicity of corroborative information or consult a multiplicity of databases.