White Paper

Cell-ID: a practical method for implementing strong user authentication

Expertron Group (Pty) Ltd

Tel: +27 (0) 12 349-0390
Fax: +27 (0) 12 349-0360
info@expertron.co.za
http://www.expertron.co.za

August 2001

Abstract: Cell-ID is a strong, token-based user authentication system that uses possession of a GSM SIM card (effectively the mobile telephone) as an authentication token to authenticate the identity of a person trying to gain access to a secure computer/network service. When a user logs into a computer-based system protected by Cell-ID, a random one-time passcode is sent to the user's mobile telephone. This passcode is valid for a limited period of time for only a single and unique authentication session. Cell-ID can also be combined with a password or a PIN for a stronger two-factor authentication mechanism.

Introduction

This paper deals with the security issues around access to secure Internet subscription services, and in particular, the issue of user authentication. Here, a subscription service refers to any kind of online service where an authorized user is required to authenticate his/her identity before being granted access to privileged information or services. These online subscription services include access to Internet banking and other financial services, access to health services (such as sensitive/private medical information provided by medical funds), etc.

There are three fundamental requirements when users of computer-based systems, where these systems consist of client and server computers, gain access to secure services:

A. Authentication of the user (and/or client computer) making use of the secure service. This allows the server to confirm the identity of the user (and/or client computer).

B. Authentication of the server providing the secure service. This allows the user to confirm the identity of the server.

C. Encryption (or secrecy) of the communication channel between the server and the client computer. This may be necessary when a high degree of confidentiality is required such as during a private transaction, or when messages need to be digitally signed.

The first of the above three concerns, authentication of the user (A), is the most challenging, particularly where there are many users who are widely distributed. For practical and economic reasons, password-based authentication, although the weakest authentication mechanism, is widely used for authenticating users for secure Internet services.

This paper introduces a novel authentication mechanism called Cell-ID. The Cell-ID system provides strong user authentication in a practical way by using mobile telephones as identity authentication tokens. It solves the token rollout problem by using the existing mobile communication infrastructure, and assumes that the majority of users who need to be authenticated are already in possession of a mobile telephone.

Strong user authentication

Users may identify themselves to servers usually by providing a “username” or “user number”. Since usernames and numbers are not secrets, it would be easy for an intruder to pose as a user and gain access to that person’s secure services. To prevent this from happening, the identity of the user must be authenticated. User authentication (proof of identity) can commonly be done in three ways:

What you know: Secrets

> If the user can show that he or she is in possession of a secret such as a password, PIN, cryptographic key or certificate that only the real user is supposed to know, it may act as proof of identity.

What you have: Hardware Tokens

> If the user can show that he or she is in possession of a hardware device, such as a magnetic card, smart card, cryptographic token or calculator, that only the real user is supposed to have, it may act as proof of identity.

What you are: Bio-metric Measurements

> If the user can show that a measurement of part of his or her body (such as a fingerprint, retina scan, photograph, etc.) matches that of the registered user, it may act as proof of identity.

User authentication based on a secret, particularly where this secret is a password or PIN that is managed by the user, is generally considered a **weak** authentication mechanism because

- users are known to choose weak (short, easy-to-guess) passwords that can easily be remembered;
- users may write down or share passwords;
- passwords are static; users do not usually change their passwords on a frequent basis, and if the secret “leaks out”, the user can never sure that his or her secret is not known by a third party unless this is changed on a frequent basis.

Authentication based on a secret such as a suitably long cryptographic key (i.e. where decipherment is infeasible) is considered a **strong** user authentication mechanism.

Authentication mechanisms based on hardware tokens are **strong** authentication mechanisms because identity of the user cannot be verified by guessing a secret. Furthermore, the user can be assured that as long as she is in possession of the hardware token, access to her secure services by a third party is impossible.

Authentication mechanisms using bio-metric measurements are also **strong**, since these are not based on a secret that the user knows, and therefore has to remember. However, bio-metric measurements of a particular user do not change (i.e. they are static, since there is an intrinsic association with “what” the user is), and hence, when the measurement is encoded into some electronic format that is transmitted over open communication channels, this information must be kept secret. Hence, these measurements must be encrypted to preserve their secrecy and integrity to prevent unauthorised use by an impostor. In this sense, due to the static nature of bio-metric measurements and their transmission over open channels, these are essentially no different from authentication mechanisms based on secrets.

Hence, authentication credentials can either be

- **Static**, such as cryptographic keys that must be installed on computing equipment (both client and server); passwords that users must remember; measurements of bio-metric entities such as fingerprints, retinas, voice, etc;

- **Dynamic**, such as one-time passwords (OTP) generated by some hardware token, where possession of the token, and hence identity, is proved by offering the OTP. One-time passwords may either be generated by algorithmic processes based on some cryptographic key, or generated by random processes.

Dynamic credentials provide a significant advantage over static credentials: with dynamic authentication credentials, the validity of a one-time password for a particular authentication session expires after some time, and even if the password does "leak out" it cannot be used for future authentication sessions. Furthermore, depending on the authentication protocol, it may even be infeasible for an impostor to use a "leaked-out" password for a current authentication session: the session must be hijacked since a different password is generated for each new authentication session.

Cell-ID: Practical, strong user authentication

Strong user authentication methods are, in many cases, impractical and expensive. This impracticality (or the *distribution problem*) refers to the difficulty of "rolling out" the user authentication technology. In all cases, either secret keys, hardware tokens such as cryptographic tokens and calculators, software programs or devices such as smart cards, card readers and bio-metric scanners must be distributed to all the users. Usually there are many more users than servers, and where the servers may be centrally located, users are usually widely distributed. This is particularly the case where the user base is large, for example, where users from among the general public make use of online Internet subscription services. Hence, password-based authentication, although fundamentally weak, is often the most practical and cost-effective way of authenticating large numbers of users.

This paper introduces a novel authentication mechanism called Cell-ID. The Cell-ID system provides strong user authentication in a practical way by using mobile telephones as identity authentication tokens. It solves the token rollout problem by using the existing mobile communication infrastructure. It assumes that the majority of users who need to be authenticated are already in possession of a mobile telephone. Furthermore, Cell-ID could also make use of existing trusted databases containing username and mobile telephone number pairs during the authentication process.

Cell-ID uses possession of a GSM SIM card (effectively the mobile telephone) as an authentication token to authenticate the identity of a person trying to gain access to a secure computer/network service. When a user logs into a computer-based system protected by Cell-ID, a random one-time passcode is sent to the user's mobile telephone. This passcode is valid for a limited period of time for only a single and unique authentication session. Cell-ID can also be combined with a password or a PIN for a stronger two-factor authentication mechanism.

The procedure that is performed each time a user logs into a Cell-ID protected system or makes use of a Cell-ID protected service is shown in Figure 1. The following terms will be used in the explanation of Figure 1 that follows:

IP Server

The computer system which provides a secure service over an IP (Internet Protocol) network to which users want to gain access.

Cell-ID Authentication Server

A centralised computer system that performs most of the Cell-ID authentication process. The Cell-ID Authentication Server may provide an authentication service to many IP Servers.

Cell-ID User Database

The Cell-ID User Database contains information matching username (or number) and mobile telephone number pairs. The Cell-ID User Database can be populated by an administrator, or by the users themselves. When users are allowed to register on the Cell-ID User Database, the correctness of the information must be confirmed from third party sources such as databases of mobile communication network service providers, banks or any other trustworthy source of information.

Thin Cell-ID Authentication Clients

Software installed on every IP Server that makes use of the Cell-ID authentication Service. The Thin Client redirects the authentication process (which otherwise may have taken place on the IP server itself) to the Cell-ID Authentication Server.

Cell-ID One-Time Passcode

A random number that is sent from the Cell-ID Authentication Server to the user's mobile telephone. The user reads the one-time passcode received by his mobile telephone and offers it as a pass-phrase to gain access to secure service(s) offered by the IP Server. The random number is cryptographically strong (generated in hardware), and is used once only for a single, unique login session. The one-time passcode is valid for a limited period of time.

Session Number

Every authentication session is numbered with a (pseudo unique) number, the Session Number. When the Cell-ID Authentication Server sends a message containing the passcode via the mobile communication network to the user's mobile telephone, it also includes the Session Number. The Thin Authentication Client uses the same session number when prompting the user for the One-Time Passcode. This enables the user to match the received One-Time Passcodes with the correct login session.

Confidence Level

A value associated with each user in the Cell-ID User Database that reflects the integrity of the procedure used to register the user's details in the database. This value may be updated from time-to-time whenever the user's registration details are re-confirmed. This value may or may not be used during the authentication process.

The procedures shown in Figure 1 are explained as follows (numbers correspond to those in the figure; lines in red represent encrypted communication channels):

1. The user requests access to a secure Internet service provided by an IP Server (e.g. a Web server) by sending a username or number to identify herself.

2. The IP Server runs a Thin Cell-ID Authentication Client that re-directs the authentication request to the Cell-ID Authentication Server by sending the username and server name or address to the Cell-ID Authentication Server.

3. The Cell-ID Authentication Server generates a random number (the Cell-ID One-Time Passcode) and Session Number, queries the Cell-ID Database for the user's mobile telephone number and sends a message to the user's mobile telephone containing the passcode and session number. The message can be sent via SMS, USSD, GPRS or any other suitable mechanism. The One-Time Passcode, Session Number, as well as a Confidence Level are sent to the IP server (also referred to as the Cell-ID Authentication Client).

4. The user reads the random number from her mobile telephone and offers it via the IP network to the IP Server as a passcode. Note that the Session Number is used to link every Cell-ID message that arrives on the mobile telephone to a specific authentication session.

5. The IP Server compares the random number received from the Cell-ID Authentication Server to the passcode submitted by the user for that particular authentication session. If the two numbers match, the user is granted access. If the numbers do not match, or if a response is not received within a certain time interval, access is denied. The server may also use the Confidence Level (which reflects the confidence of correctness of the user's data in the Cell-ID database) from the Cell-ID Database to determine whether or not the user is granted access.

6. The outcome of the access attempt is sent back to the Cell-ID Authentication Server and logged in the Cell-ID Database.

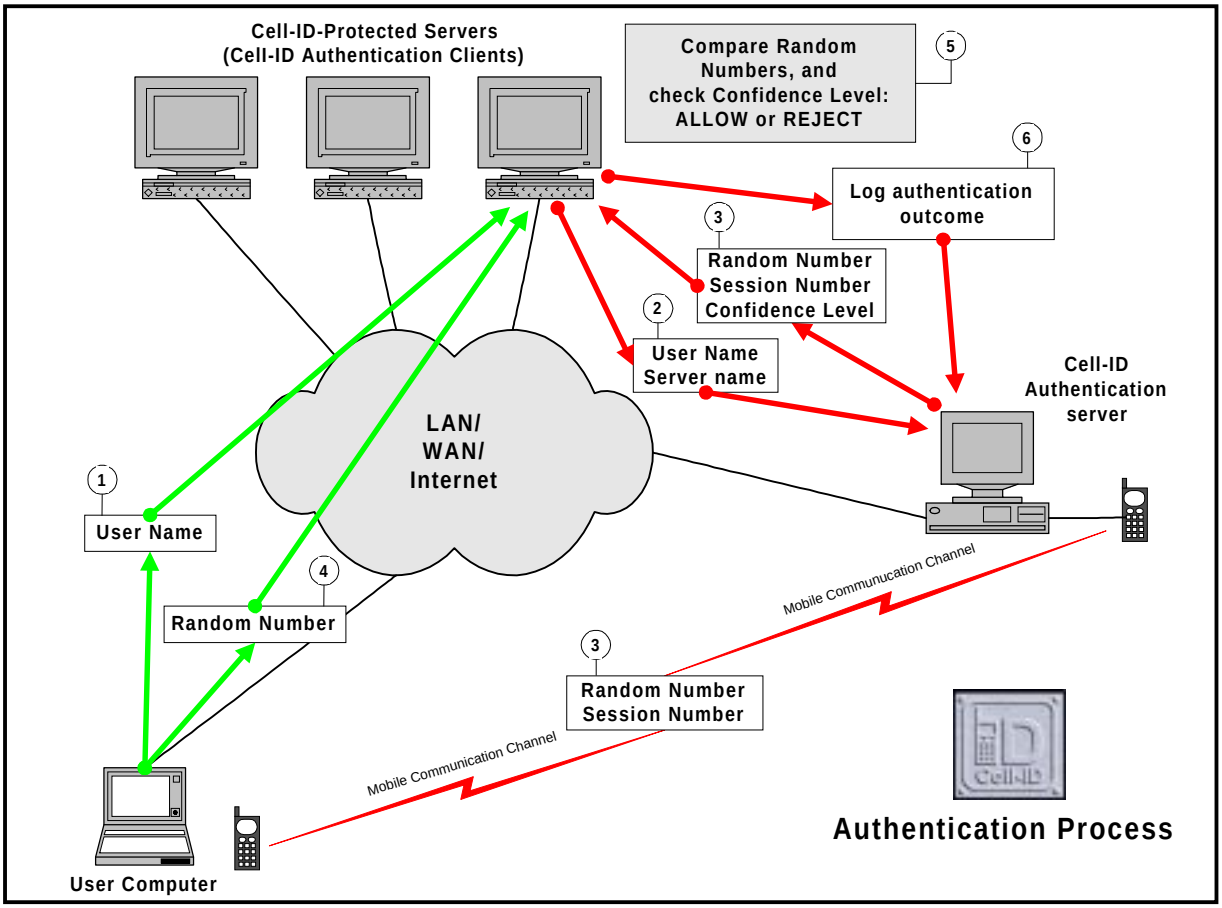

Figure 1: Cell-ID authentication procedure

The Cell-ID system currently uses SMS to deliver the passcode message to the user's mobile telephone. In Figure 1, it is suggested that SMS messages are sent from a GSM modem directly connected to the Cell-ID server. However, it is preferable to deliver the SMS via a direct IP link to the SMS server (SMSC) of the GSM network service provider. This increases reliability and total throughput (up to 10 SMS messages per second per IP link).

The most critical component affecting the performance of the Cell-ID authentication system is the performance of the GSM message delivery channel between the Cell-ID authentication server and the user. The Cell-ID authentication system is a real-time authentication mechanism, and hence, rapid and reliable delivery of SMS messages is essential. This implies both the throughput of SMS delivery between the Cell-ID authentication server and the SMSC, and the SMS delivery time to the user.

Throughput of SMS messages via the IP link is up to 10 messages per second per link (multiple links can be utilized if necessary). The median for SMS message delivery is 6.8 seconds (taken over 300 samples, as shown in Figure 2). Further statistics that can be derived from these trials are (in the graph below, an error is the case where an SMS is delivered after 45 seconds):

Median:	6.82 sec
Average:	7.6 sec
Standard Deviation:	3.47 sec
Maximum:	32.62 sec
Minimum:	5.33 sec
Errors:	2.7 %

Table 1: SMS delivery statistics for direct IP link to SMSC

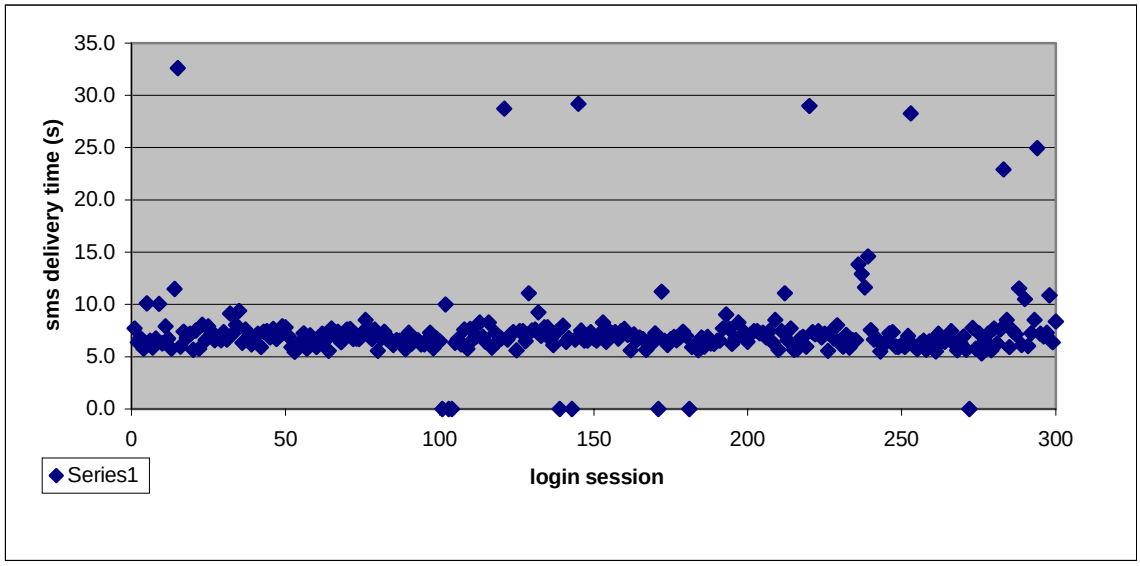

Figure 2: SMS delivery time via direct IP link to SMSC (zero value indicates network error)

Throughput of SMS messages from the GSM modem is approximately five messages per minutes per modem (one every 12 seconds), where multiple modems can be configured if necessary. The median for SMS message delivery is 13.7 seconds (taken over 110 samples, as shown in Figure 3). Further statistics that can be derived from these trials are:

Median:	13.67 sec
Average:	13.9 sec
Standard Deviation:	1.90 sec
Maximum:	26.09 sec
Minimum:	11.37 sec
Errors:	4.5 %

Table 2: SMS delivery statistics for GSM modem

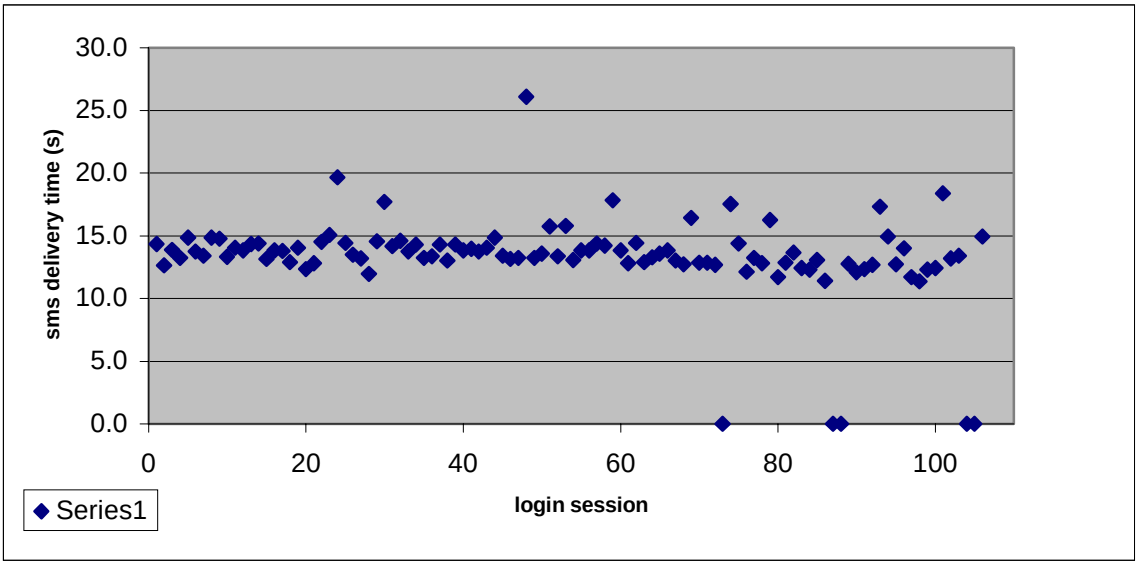

Figure 3: SMS delivery time from GSM modem (zero value indicates network error)

It is clear from the above statistics that the SMS delivery mechanism provides acceptable performance, with an average delivery time of about 7 seconds and an error rate of less than 3 percent.

Conclusion

Cell-ID is a practical, strong user authentication mechanism for authenticating large numbers of users for access to secure Internet subscription services. Cell-ID solves the rollout problem associated with conventional token-based mechanisms by using the existing mobile telephone infrastructure as hardware authentication tokens, and the SMS delivery mechanism to deliver random one-time passcodes to the users. SMS can be shown to provide acceptable performance metrics so that Cell-ID can be used as a feasible real-time authentication mechanism.

Cell-ID is secure

A separate, authenticated (GSM) communication channel is used to deliver cryptographically strong one-time passcodes to a user's mobile telephone when logging into a secure service over an IP network. The user is alerted (by an SMS on her mobile telephone) whenever someone else tries to gain access to her account. All actions are logged.

Cell-ID is affordable

Cell-ID needs a significantly lower capital investment than competing token-based authentication products (important in an environment where technology is rabidly changing). The total running cost of Cell-ID is less than that of other strong authentication products. Cell-ID spreads the cost of authentication much more evenly over the years of operation, thus limiting the "peak budget"-effect for the first year of operation.

Cell-ID is simple to roll out

No extra authentication tokens for users to carry and no software or hardware to install on client computers. The existing mobile telephone infrastructure is used to manage the "tokens". No costly Public Key Infrastructure (PKI) to roll out and manage.

Cell-ID is simple to use

Cell-ID uses familiar technology that users are already comfortable with. The user logs in as usual, followed by a prompt to type in the Cell-ID passcode which is received on his mobile telephone about 7 seconds after initiating the authentication process.