# PASSWORD

## Working document : How to run a secure lottery

Michael Roe
Cambridge University Computer Laboratory
Computer Security Group

Version 0.1
January 1993

## 1 Rationale

Changing from the normal to a "security-enhanced" version of an application requires each user to expend a moderate amount of effort to learn how to operate the new program. Most people will (quite rightly) not make this effort if there is no benefit to be gained from doing so. On the other hand, the first large-scale tests of such an application cannot be carried out in an environment where there is a genuine need for security, as there is too great a risk of something going wrong.

To overcome this dilemma, we propose that security enhanced applications be introduced in the form of a game. If a flaw is discovered in the security of the system, the worst consequence this can have is that people will be able to cheat at the game. If the game has a single prize of negligible value, this is an acceptable risk. The intrinsic interest of playing the game will act as an inducement to read the manuals and work out how to run the software. (Each user's expected gain from playing the game will be the value of the prize multiplied by the probability of winning it. This will be extremely small, but human behaviour is well-known not to be rational in this respect).

## 2 Design Constraints

The design constraints upon the game were as follows:

- It should only make use of security facilities provided by both X.400(88) and Privacy Enhanced Mail, in order that the same game can be used to introduce either of these two secure e-mail systems.
- Given the above constraint, the game should make use of as many of the available security facilities as possible.
- It should be possible to play the game using only an implementation conforming to the relevant standards, without using any additional software. This will allow different vendors' implementations to be used with the same game. It would acceptable if the persons administering the game and awarding the prize need to make use of specially written software to do so.
- The game should not cause offence to any members of its target audience, which will be drawn from all EC member states. Various forms of historical simulation game, which were otherwise suitable, were rejected for this reason.
- The game should be easy to learn and simple to play.

# 3 Rules

The following game was devised, based on "Lotto" or "Bingo".

## 3.1 Identification of Participants

Before the game commences, the participants must be identified. Participants are divided into three classes:

- *players* who are eligible to win the prize. There may be arbitrarily many players, but the number chosen affects the length of the game.
- *adjudicators* who decide who has won and award the prize. There may be more than one adjudicator in order to reduce the opportunities for collusion between an adjudicator and a player. In case of dispute, more than half the adjudicators must agree for the prize to be awarded. The recommended number of adjudicators is 3, which by a fortunate co-incidence is also the number of national consortia involved in the PASSWORD project.
- *announcers* who periodically announce the value of "random" variables which determine the course of the game. There may be more than one announcer in order to reduce the opportunities for collusion between an announcer and a player. The same person may act as both an adjudicator and an announcer.

## 3.2 Communications Requirements

- There must be some means for people to indicate that they want to join in the game. This can be achieved by creating an electronic mail box to which requests to join can be sent.
- Each player must be able to send a message to all the adjudicators. This can be achieved by creating an e-mail distribution list that is sent to all the adjudicators.
- Each announcer must be able to send a message to all the players. This can be achieved by creating an e-mail distribution list that is sent to all the players.
- The adjudicators must know who the announcers are. This will usually be achieved by the adjudicators deciding who to appoint as announcers.
- The announcers must know who the players are.
- The players must know who the announcers are. (Strictly speaking, they must know which Distinguished Names each announcer will use for her messages. This may be a role identifier rather than a person's name, such as:

  ```
  C=GB@o=Cambridge University@ou=Computer Lab@cn=PASSWORD game announcer
  ```

- The players must know which announcer each message should come from. As the announcers take it in turns to send messages, the players must know the order in which turns are taken and who has the first turn.
- The players must be able to tell when a game has started and when a game has finished.

## 3.3 Separation of Duty

This game is vulnerable to many types of collusion attack, where several people conspire together in an attempt to cheat. The assignment of roles to people should be such that no person acting alone has sufficient access to subvert the system. In the Clark-Wilson model of computer security, this is known as the separation of duty requirement. The following table shows which roles are incompatible:

| | Adjudicator | Announcer | Notary | Player |
|---|---|---|---|---|
| Adjudicator | Y | Y | Y | N |
| Announcer | Y | Y | N | N |
| Notary | Y | N | Y | N |
| Player | N | N | N | Y |

| | Key |
|---|---|
| Y | Yes, the same person may occupy both roles. |
| N | No, the same person may not occupy both roles. |

The Clark-Wilson model assumes that two people are strictly more trustworthy than one. This is not necessarily the case. For the purposes of this game, we require in addition that there be separation of duty between *organisations*. That is, the three adjudicators should each be from different organisations, and similarly for the announcers and notaries.

## 3.4 Enrollment Phase

In the enrollment phase, the players identify themselves. This may be achieved by sending an e-mail message to the "join game" mail box.

For example:

```
To: pwd-game-request@cs.ucl.ac.uk
Subject: PASSWORD game

I'd like to join in the PASSWORD game; please put me on the mailing list.
My address is Fred.Bloggs@foobar.co.uk.
```

No security facilities are required at this point.

## 3.5 Key Distribution Phase

In the key distribution phase, each player, announcer and adjudicator must generate an RSA public key pair and be issued with a key certificate as described in PASSWORD report R2.5. This is part of the normal process of joining the PASSWORD pilot exercise, and is not specific to this game.

## 3.6 Confirmation Phase

In the confirmation phase, each player is sent an e-mail message containing the latest version of the rules of the game and the names of the announcer, including the order in which announcers will take turns and who will take the first turn. This message is electronically signed by the adjudicators.

In games of this type, the recipient of a message needs to know not only *who* a message came from, but also whether they were *authorised* to send that message. This first message, defining the rules of the game, is the only one for which the recipient has no evidence (internal to the system) that it was authorised. In game terminology, the recipient has no way of knowing whether or not the act of declaring what the rules are is itself a valid move. By choosing to believe that the message is valid, that the game is really being played, and that there will be a prize at the end of it (an act of pure faith) the recipient creates the structure within which moves can be determined to be either valid or invalid.

## 3.7 Card Distribution Phase

In the card distribution phase, each announcer chooses at random a list of $N$ integers in the range $1 \ldots M$ (a "card") for each player. This list is sent to the player in an e-mail message that uses the integrity, confidentiality and non-repudiation security services. That is:

- *Integrity:* The player can determine who sent the message. As the list of the authorised announcers was obtained in the previous phase, this allows the player to check that the originator is an authorised announcer.
- *Non-repudiation:* The player can prove to a third party (eg. the adjudicators) that the announcer sent them the message.
- *Confidentiality:* No-one except the announcer and the player knows which numbers were chosen. This helps protect against attempts to cheat involving other announcers and other players conspiring together.

This message should be self-identifying. That is, it should be obvious from its contents that it contains the player's card and is not a list of integers that was sent from the announcer to the player for some other reason. This protects against substitution attacks where a player takes some other message that was sent by an announcer and takes it to the adjudicators, claiming that it is a winning card.

This message should also contain the player's name, to prevent players from claiming the prize using someone else's card.

For example:

```
To: Fred.Bloggs@foobar.co.uk
Subject: PASSWORD Lotto Card, Part 1/3
From: game-announcer@darmstadt.gmd.de

This is part one of your personal PASSWORD Lotto card.

Your first line of numbers is:
 8 15 27 35 56 71 82 98

The next part will be sent by game-announcer@inria.fr.

Please keep this message, as you will need it to play the game.
```

The player should check that the source of message is one of the announcers listed in the "rules" message they received in the enrollment phase. Cards issued by other people, and cards in messages that are not integrity-protected (even if they *appear* to come from one of the announcers), are not valid and will be rejected by the adjudicators. Every e-mail user agent should indicate to the user whether or not the message is integrity-protected in a clear and unmistakable fashion. (eg. by drawing a special symbol on the screen beside the message).

### 3.8 Announcement Phase

In the announcement phase, the announcers take it in turns to pick a number at random in the range $1 \ldots M$ and send it to all the players. This message uses the integrity and non-repudiation services but does not use the confidentiality service.

Each player checks to see whether the announced number is on any of the cards they received from the announcers in the card distribution phase. If it is, they make a note that it has been called. If a player believes that all of the numbers on *all* of the lists they were given have been called, they may enter the claim phase and attempt to claim the prize.

For example:

```
To: game-players
From: game-announce@cl.cam.ac.uk
Subject: The first PASSWORD Lotto Number is 27

The first PASSWORD lotto number is 27. If the number 27 occurs on any of
your cards, please save this message. If ALL the numbers on ALL 3 of your
cards have been announced, you may have won a prize. If you think you have won,
forward ALL of your lotto cards to game-claims@cs.ucl.ac.uk.
```

### 3.9 Claim Phase

In the claim phase, a player attempts to prove to the adjudicators that she has won a prize. This is done by invoking the non-repudiation service on the messages containing the player's cards and the messages containing the numbers that were called. This can be achieved by forwarding all these messages (including the security protocol headers) to the adjudicators.

If the majority of the adjudicators are convinced that the player has won, the prize phase is entered and the game finishes. If the adjudicators determine that the claim is in error or an attempt to cheat, the announcement phase continues. The adjudicators may, at their discretion, award additional prizes for particularly ingenious attempts to cheat.

In reaching their decision, the adjudicators shall only make use of the evidence presented to them, and shall not make use of any additional information that they might have. For example, if a player presents ostensibly valid evidence that all their numbers have been called, but the adjudicators know that some of them were in fact not called (eg. if the announcers and adjudicators are the same people), then the player is entitled to win the main prize.

In the case of X.400(88), there is a technical problem with forwarding the messages to the adjudicators; it is possible to construct messages whose integrity protection will be broken by forwarding them. If this happens, the adjudicators can resolve the issue by either examining the copy of the message held by the notary (see section 4) or by using some means outside the X.400 standard to access the recipient's copy of the message. The first approach will probably be used for the purposes of this game, as it's easy. Serious applications of secure X.400 may use the latter method, as it is somewhat more reliable (consider, for example, the possibility that the notary might not tell the truth).

### 3.10 Prize Phase

In the prize phase, a prize is awarded to the winner.

The prize should have the following characteristics:

- It should be of relatively modest value (around 20 ECU).

- It should be typical of one of the participating EC countries. (eg. something that country is famous for exporting).
- It should be drinkable.

The adjudicators will send a message to the players, saying that the game has finished an a prize has been awarded. This message will be protected by the integrity and non-repudiation services.

# 4 Notarization

In order to provide a full non-repudiation service, each message must be *notarized*. That is, when the message is received it must be shown to a trusted third party who can later testify that the message existed at a particular time.

This is done in order to guard against an originator deliberately revealing her secret key in order to be able to deny that she signed a particular message. ("It wasn't me, it was a hacker who got access to my secret key.") In a scheme with notaries, users are held liable for everything that is done with their secret key until they report to a certification authority that it has been compromised. (This is similar to the procedures for stolen ATM cards). The notary can testify as to when the message was signed, and this be used to determine whether it was before or after the key was reported as being compromised. This relies on the assumption that everybody trusts the notary to tell the truth.

Within the PASSWORD project, we have chosen not to provide a general notary service, even though it would be desirable both for this game and for more serious applications.

For the purposes of this game, a restricted form of notary will be used. One or more notaries will be added to the e-mail distribution list that is used to send messages to the players. They will keep all messages sent to this list, and record the time at which messages were received (most e-mail user agents will do this automatically). Later on the adjudicators can ask the notaries for the times at which they received disputed messages. For simplicity, the notaries and the adjudicators may be the same people.

This form of notary is not perfect, as the players have no evidence that the notary has received any of the messages sent to the list.

# 5 Message Sequence Integrity

Each player will want to be sure that they have seen all the numbers that have been called, as their chance of winning the game is reduced if they miss some. Within the PASSWORD project we will not attempt to provide absolutely guaranteed *availability*. Normal failures of machines or malicious action (eg. by MHS administrators) can result in message loss.

We can, however, provide *message sequence integrity*. That is, a recipient of a sequence of messages from the same originator can be sure that no messages in the middle of the sequence have been lost. This is achieved by including an integrity-protected sequence number in each message. The message sequence number by itself is not sufficient to convince the recipient that she has received all the messages that were sent; the possibility remains that messages with higher sequence numbers were sent but not received. This is illustrated in the following diagrams:

Recipient knows she has received all messages up to number 5:

```
Sent       1  2  3  4  5
Received   1  2  3  4  5
```

Recipient can detect that message 3 was lost:

```
Sent        1  2  3  4  5
Received    1  2     4  5
```

Message 6 was lost, but the recipient cannot detect this:

```
Sent        1  2  3  4  5  6
Received    1  2  3  4  5
```

If messages are sent at a known constant rate, the recipient can also detect that messages with higher sequence numbers have been lost. For example, if PASSWORD lotto numbers are supposed to be called at the rate of one a day, and none have been received for a week, then the intended recipient has strong evidence that something has gone wrong.

X.400(88) has been only recently introduced at many of the sites involved in the PASSWORD project. It is therefore quite likely that it will occasionally stop working correctly. This game will have the useful side-effect of regularly exercising a large number of X.400 links and confirming that they are still operational.

For the purposes of the game, the sequence number will be included in the text of the messages so that they can be manually checked by the recipient. If X.400(88), rather than Privacy Enhanced Mail is being used, then the message sequence number can also be included in the message protocol header. Mail user agents could be programmed to check the X.400 sequence numbers automatically.

# 6 Other Attacks

This are several ways to cheat at this game which are not covered by this document. The details are left as an exercise for the reader.