Who sent the e-mail?*

Angel Corberán[1], Ricard Martínez[2], Francisco Montes[1†] and Salvador Roca[3]

[1] Department of Statistics and O. R.

[2] Data Protection Law Assessor

[3] Computer Center

Universitat de València. Spain.

Abstract

In mid October 2001, a number of lecturers at the University of Valencia received insulting, threatening and anonymous electronic mails. An investigation about this fact is only permitted under very restricted conditions, stipulated by the Spanish law of the Secrecy of Communications. Only one judicial authority is able to lift these restrictions and authorize information to be checked in order to obtain enough evidence to unveil who was responsible for the messages. The authors propose in this paper a study for quantifying the weight of certain evidence with a view to show to the judge that the relevance of the said weight would justify such a measure.

1 Introduction

The University of Valencia provides computer services to a wide community of around 60000 people. This number of users generates, on a regular basis, several conflicts associated with an incorrect use of the computer systems. One of the more frequent conflicts is the anonymous e-mail in which insults or even threatens can be sent.

Considering that each user presents, on average, a minimum use of 5 hours, and that different free-access computer rooms are available at our university, it is possible that some of these e-mails were sent from the university computers. Therefore, it can be assumed that a user in one session and in a short period of time performs several activities under an anonymous identity. On the other hand, it is possible to establish a connection between the anonymous sender and the receiver of the e-mail (for instance, a student that has failed an exam or that has been scolded by a teacher). Moreover, it is possible that the sender sent an e-mail under its "real" identity in the same or in another session.

*A first version of this paper was presented in the Fifth International Conference on Forensic Statistics. Venice 2002.

†E-mail: francisco.montes@uv.es

Under these circumstances, and in a LAN net (as it is the case of the University of Valencia), there are different ways to establish and trace an identity during a given session. However, the legal limits of this investigation must be previously defined in order to avoid a possible invasion of privacy. In the Spanish Law (considering also the specific norms about communications), it is clearly stated that the investigation through the Internet traffic of a person, requires a court order.

In mid October 2001, a number of lecturers at the University of Valencia (UV from now on) received insulting and threatening electronic mails. All the mails had been sent from the same server, the same day and with a difference of hardly 20 minutes between the first and the last. The server was reached via a web page that only demanded the user's name and a password in order to use its services. The messages were anonymous and arrived together with other *normal* messages whose sender was a student enrolled in subjects given by the lecturers who received the aforementioned mails. This circumstance made the insulted lecturers think that the said student could be the author of the messages and communicated the fact to the academic authorities.

The academic authorities started an investigation into the facts, which involved having access to the information contained in the mail servers and the UV Internet. However, as we said before this access is only permitted under very restricted conditions, stipulated by the Spanish law of the Secrecy of Communications. Only one judicial authority is able to lift these restrictions and authorize information to be checked in order to obtain enough evidence to unveil who was responsible for the messages.

A judge can pose lifting secrecy if it justifies the benefits obtained. Here is a study to quantify the weight of certain evidence with a view to show to the judge that the relevance of the said weight would justify such a measure.

2 Facts and reasonable evidences

The type of message received, the one that arrived accompanied by a *normal* message, sent by a student that was taught by all the lecturers involved, and for whom a previous incident had been recorded, led the lecturers to suspect this student, who from now on will be denoted X.

How do we think X has acted and what evidence can we hope to find? It would seem reasonable to think that the student has acted as follows:

A1: in an instant of time t_0, he has connected to the web page that holds the external mail server from one of the computers available in the UV Computer Labs,

A2: he has sent messages to the lecturers,

A3: he has gone through, at some moment of the process, a step that demands identification. For instance, connecting to his own mail address at the UV,

A4: he has closed down his connection with the Internet, once the interval of time t has passed since the beginning of the process.

If this is what he has done, the previous steps should have left the following traces:

R1: a register in the *proxy* of the UV Internet server for each of the connections to the web page that holds the external mail server and, particularly, one for each of the occasions on which a mail was sent. We shall designate M_i and tr_i as the emission of the mail and the time it took place, respectively,

R2: a register in the *log* of the UV incoming mail server, which took place in the time interval $te_i > tr_i$,

R3: a register in the *log* of the UV distributor of incoming mail, which took place in the time interval $td_i > te_i > tr_i$.

R4: a register of the type of action in A3, in the case that it took place.

3 The value of the evidence

In the following we shall suppose that just one insulting mail has been sent to just one lecturer.

If we are able to express, in the form of evidence, the information associated to the steps that X has carried out, and we can also estimate the probabilities of the derived occurrences, we will be in a position to obtain (Aitken [1]) the value of this evidence from

$$\frac{P(Ev|G_X)}{P(Ev|G_X^c)}, \tag{1}$$

and use the corresponding value in the following expression which, from the prior odds in favour of the guilt of X, give us the posterior odds in favour of the guilt of X.

$$\frac{P(G_X|Ev)}{P(G_X^c|Ev)} = \frac{P(Ev|G_X)}{P(Ev|G_X^c)} \times \frac{P(G_X)}{P(G_X^c)}, \tag{2}$$

where G_X represents the event *X is guilty*, in the sense that he really sent the insulting mail.

The evidence demonstrated by the previous steps is the following:

> Ev={*during the time interval* $[t_0, t_0+t]$*, from a computer at the UV, an insulting e-mail message has been sent through the external server and an action has been carried out using the identity X; some time later the lecturer has received the message from the same mail server*}.

This evidence involves the events,

> E_1={*the insulting message has been sent through a computer at the UV during the interval* $[t_0, t_0 + t]$},
>
> E_2={*whoever is using the computer at the UV during the interval* $[t_0, t_0 + t]$ *is always the same person*},

E_3=$\{$*whoever takes the aforementioned step A3 identifies himself as X is really X*$\}$,

in such a way that

$$Ev = E_1 \cap E_2 \cap E_3.$$

Given its definition it seems reasonable to assume the independence of these three events, in such a way that (1) would stay in the form

$$\frac{P(Ev|G_X)}{P(Ev|G_X^c)} = \frac{P(E_1|G_X)}{P(E_1|G_X^c)} \times \frac{P(E_2|G_X)}{P(E_2|G_X^c)} \times \frac{P(E_3|G_X)}{P(E_3|G_X^c)}. \quad (3)$$

We will now look at how to estimate each of the factors of the second member of (3).

Probabilities related to E_1.- Any knowledge we wish to have about E_1 demands an analysis of the aforementioned traces and accede, therefore, to the protected information. As we have already said this, a priori, is not possible.

This difficulty can be got around via the following simulation process:

1. We registered as users of the external mail server.
2. During the five working days of a week and different hours we crossed each other messages through the external mail server.
3. We requested from the Computer Center of the UV, the information that the aforementioned messages had generated in the *proxy* of the UV Internet server and in the *log* of the server and of the distributor of mail entering the UV.

The objective of this process is to obtain a random sample of the variable T_D=$\{$*time elapsed between the dispatch of the message and its delivery to the destination by the distributor of mails entering the UV*$\}$. Table 1 summarises the characteristics of the sample obtained, the histogram of which we display in figure 1.

N	**Min.**	**Max.**	$\mathbf{p_{05}}$	$\mathbf{p_{95}}$	**mean**	**median**	**sd**
81	2	119	2	83.50	40.57	43	20.80

Table 1.- Summary of the random sample of T_D (values are expressed in seconds).

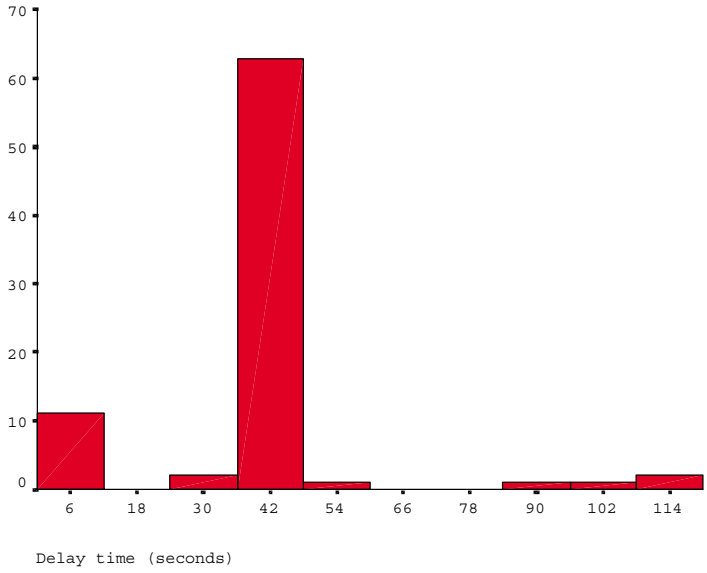

Figure 1.- Histogram of the random sample of T_D.

It is difficult to adjust a theoretical distribution to the observed data. In the absence of this, we will focus our attention on t_{max}, the maximum observed value of T_D .

If by t_R we designate the time taken for the message to arrive to the Lecturer's e-mail address, we will consider the interval $I = [t_R - t_{max}, t_R]$ and the random variable N_I=$\{$*the number of users at the UV who are connected to the external mail server in the interval* I$\}$. In accordance with the definition of E_1 we will have $E_1|G_X = \{N_I \geq 1\}$ and $E_1|G_X^c = \{N_I \geq 2\}$, and

$$\frac{P(E_1|G_X)}{P(E_1|G_X^c)} = \frac{P(N_I \geq 1)}{P(N_I \geq 2)} = r \geq 1. \tag{4}$$

Now the problem is how to find out the distribution of N_I, because any estimation procedure requires access to protected information. We have, therefore, to conjecture about the value of r.

Probabilities related to E_2.- If the variable T_{t_0} designates the uninterrupted time that a student, who has connected in the instant t_0, using one of the computers available in the in the UV Computer Labs, we have $E_2 = \{T_{t_0} \geq t\}$, and

$$\frac{P(E_2|G_X)}{P(E_2|G_X^c)} = \frac{P(T_{t_0} \geq t|G_X)}{P(T_{t_0} \geq t|G_X^c)} = 1, \tag{5}$$

given that the variable T_{t_0} behaves in the same way for all the users.

Probabilities related to E_3.- It seems clear that $P(E_3|G_X) = 1$. To estimate the probability $P(E_3|G_X^c)$ we observe that $E_3|G_X^c$=$\{$*somebody has supplanted the electronic personality of* $X\}$. For this to happen the impostor must know the login and the password of X who, without doubt, would change the latter on becoming aware of it. It must be that knowing the number of time the password has changed supplies us with an estimation, without doubt in excess, of $P(E_3|G_X^c)$.

Throughout the year 2001, 3896 changes took place in the 41685 available mail accounts in the UV mail server, therefore,

$$\frac{P(E_3|G_X)}{P(E_3|G_X^c)} = \frac{1}{\frac{3896}{41685}} = \frac{41685}{3896} = 10{,}70. \tag{6}$$

Substituting (4), (5) and (6) in (3) we obtain for, V, the value of the evidence

$$V = \frac{P(G_X|Ev)}{P(G_X^c|Ev)} = 10{,}70\ r \tag{7}$$

4 Regarding X's guilt

It is difficult to quantify the three lecturer's suspicion regarding X. We can assign to G_X the probability $1/K$, with K being the number of students in the group common to the three lecturers. This way of assigning probabilities implies confusing unknowns with equiprobability and has received deserved criticism (Isaac [2], page 40), but in this case we think it is justifiable as we are dealing with a lower bound for $P(G_X)$ which gives rise therefore, to a lower bound for (2).

Then,

$$\frac{P(G_X)}{P(G_X^c)} = \frac{1}{K-1}. \tag{8}$$

Substituting (7) and (8) in (2) we obtain for the posterior odds, PO, in favour of the guilt of X,

$$PO = \frac{P(G_X|Ev)}{P(G_X^c|Ev)} = \frac{10{,}70\ r}{K-1}.$$

From this expression we have constructed tables 2 and 3. In the first one we show the values that r would have to take so that, above certain values of K, we would obtain the values of PO that head the columns. In table 3, which shows the value of PO for certain values K and r, we highlighted in black the values of $PO \geq 1$.

	PO=1	***PO=15***	***PO=10***	***PO=15***
K=10		4.21	8.41	16.82
K=20	1.78	8.88	17.76	35.51
K=50	4.58	22.90	45.79	91.59
K=100	9.25	46.26	92.52	185.05

Table 2.- Values of r for some values of PO and K.

	r=1	***r=3***	***r=9***	***r=99***
K=10	**1.19**	**3.57**	**10.70**	**117.70**
K=20	0.56	**1.69**	**5.07**	**55.75**
K=50	0.22	0.66	**1.97**	**21.62**
K=100	0.11	0.32	0.97	**10.70**

Table 3.- Values of PO for some values of K and r.

5 Conclusions

1. The evidence that Ev represents allows us to conclude, (4) and (7), that its value is at least 10,70. But remember that Ev assumes that the message has been sent from a computer at the UV, which is, without doubt, the first and most important objection to our result. The first step to carry out is, therefore, to check up to what point this hypothesis is reasonable. To do this we can study the variables T_D and N_I.

   Better knowledge of the behaviour of T_D would allow us to choose the percentile with which to fix the interval I that defines N_I. The probability that the connection to the external mail server has not been carried out from a computer at the UV is closely related to $P(N_I = 0)$, for the estimation of which we need, as we have already said, to have access to protected information.

2. The facts that have motivated this study happen, fortunately, very infrequently. Moreover, if we trust in the correct behaviour of the great majority of the students at the UV, we can expect the value of r to be high and, in accordance with table 3, the value of PO will be also high.

Taking these comments into account, the final conclusion would be that the judge should allow the analysis of protected information, given the indisputable help that this would represent in order to evaluate the guilty of X.

References

[1] C.G.G. Aitken (1995). *Statistics and the Evaluation of Evidence for Forensic Scientists.* John Wiley, Chichester.

[2] R. Isaac (1995). *The Pleasures of Probability.* Springer Verlag, New York.