

Franklin University

## FUSE (Franklin University Scholarly Exchange)

---

All Faculty and Staff Scholarship

---

2005

### ISRAM: information security risk analysis method

Bilge Karabacak

Franklin University, bilge.karabacak@franklin.edu

Ibrahim Sogukpinar

Gebze Institute of Technology, ispinar@bilmuh.gyte.edu.tr

Follow this and additional works at: <https://fuse.franklin.edu/facstaff-pub>



Part of the [Information Security Commons](#)

---

#### Recommended Citation

Karabacak, B., & Sogukpinar, I. (2005). ISRAM: information security risk analysis method. *Computers & Security, 24* (2), 147-159. <https://doi.org/10.1016/j.cose.2004.07.004>

This Journal Article is brought to you for free and open access by FUSE (Franklin University Scholarly Exchange). It has been accepted for inclusion in All Faculty and Staff Scholarship by an authorized administrator of FUSE (Franklin University Scholarly Exchange). For more information, please contact [fuse@franklin.edu](mailto:fuse@franklin.edu).



ELSEVIER

# 3 ISRAM: information security risk 4 analysis method

5 **Bilge Karabacak<sup>a,\*</sup>, Ibrahim Sogukpinar<sup>b</sup>**

6 <sup>a</sup>National Research Institute of Electronics & Cryptology (UEKAE), P.O Box 74, 41470 Gebze,  
7 Kocaeli, Turkey

8 <sup>b</sup>Gebze Institute of Technology, 41400 Gebze, Kocaeli, Turkey

9 Received 24 December 2003; revised 27 July 2004; accepted 27 July 2004

## 10 KEYWORDS

11 Information security;  
12 Risk analysis;  
13 Quantitative risk  
14 analysis;  
15 Paper-based risk  
16 analysis;  
17 Risk model  
18

**Abstract** Continuously changing nature of technological environment has been 27  
enforcing to revise the process of information security risk analysis accordingly. A 28  
number of quantitative and qualitative risk analysis methods have been proposed 29  
by researchers and vendors. The purpose of these methods is to analyze today's 30  
information security risks properly. Some of these methods are supported by 31  
a software package. In this study, a survey based quantitative approach is proposed 32  
to analyze security risks of information technologies by taking current necessities 33  
into consideration. The new method is named as Information Security Risk Analysis 34  
Method (ISRAM). Case study has shown that ISRAM yields consistent results in 35  
a reasonable time period by allowing the participation of the manager and staff of 36  
the organization. 37

© 2004 Published by Elsevier Ltd. 38

## 19 Introduction

20 The structure and type of information technologies  
21 have changed enormously over last decade. The  
22 simple stand-alone batch applications evolved into  
23 distributed computing environments, including real-  
24 time control, multitasking and distributed process-  
25 ing. The process of information security risk analysis  
26 has also been affected by these enormous changes.

39 It is claimed to be "inconsistent, long lasting and  
40 difficult to apply" (Gerber and Solms, 2001). Due to  
41 the difficulties of applying complex risk analysis  
42 tools into today's information systems, researchers  
43 have studied to develop new methods. 44

45 Because the success and continuity of organ-  
46 izations vastly depend on the availability of infor-  
47 mation technologies, the task of protection of  
48 information technologies have become more crit-  
49 ical than ever. In 1980s, the head of information  
50 technologies (IT) department of organization was  
51 the responsible staff to protect information sys-  
52 tems. Nowadays, some of the company managers

\* Corresponding author.

E-mail addresses: bilge@uekae.tubitak.gov.tr (B. Karabacak),  
ispinar@bilmuh.gyte.edu.tr (I. Sogukpinar).

54 are taking over this responsibility from the head of  
55 IT department (Owens, 1998). Thus, managers of  
56 organizations should understand the risk analysis  
57 process that directly affects the protection of  
58 information technologies. Moreover, managers  
59 may desire to participate in risk analysis process.  
60 The structure of new risk analysis methods allows  
61 the participation of managers (Bilbao, 1992; Kailey  
62 and Jarratt, 1995; Jenkins, 1998; C&A Systems  
63 Security Limited, 2000; Toval et al., 2002; Jacobson,  
64 2002; Coles and Moulton, 2003).

65 In this study, a new method named Information  
66 Security Risk Analysis Method (ISRAM) is proposed  
67 for information security risk analysis by taking  
68 today's needs into account. ISRAM is designed for  
69 analyzing the risks at complex information systems  
70 by allowing the participation of managers and  
71 staff. Proposed method consists of seven steps.  
72 These steps are exemplified in a case study in  
73 order to explain ISRAM clearly. To verify the results  
74 of the same case study, a risk model is set up with  
75 Arena simulation software. The collected real-life  
76 statistical data are introduced into the risk model.

77 This paper is organized as follows: risk analysis  
78 methods for information security are introduced  
79 briefly after the Introduction. Then the risk model  
80 of ISRAM, explanations and experimental results  
81 are presented. The section following that contains  
82 some ideas on the verification, comparison and the  
83 results of the application. The last section is the  
84 conclusion.

## 85 Risk analysis methods for information 86 security

87 Basically there are two types of risk analysis  
88 methods. Quantitative risk analysis methods use  
89 mathematical and statistical tools to represent  
90 risk. In qualitative risk analysis methods, risk is  
91 analyzed with the help of adjectives instead of  
92 using mathematics. Risk analysis methods that use  
93 intensive quantitative measures are not suitable  
94 for today's information security risk analysis. In  
95 contrast to the past decades, today's information  
96 systems have a complicated structure and a wide-  
97 spread use. Therefore, intensive mathematical  
98 measures used to model risk for complex environ-  
99 ments make the process more difficult. Calcula-  
100 tions performed during the risk analysis process  
101 are also very complex. Quantitative methods may  
102 not be able to model today's complex risk scenar-  
103 ios. Risk analysis methods based on qualitative  
104 measures, are more suitable for today's complex  
105 risk environment of information systems. However,

one important drawback for qualitative risk anal- 106  
ysis methods is their nature that yields inconsis- 107  
tent results. Because qualitative methods do not 108  
use tools like mathematics and statistics to model 109  
the risk, the result of method is vastly depended 110  
on the ideas of people who conduct the risk 111  
analysis. There is a risk of giving subjective results 112  
while using qualitative risk analysis methods. 113  
Following examples can be given for two types of 114  
risk analysis tools which are based on quantitative 115  
and qualitative methods. TUAR is a quantitative 116  
tool, which uses fault trees and fuzzy logic to 117  
express the risk (Bilbao, 1992). RaMEX is a qualita- 118  
tive tool, which does not use mathematical or 119  
statistical instruments (Kailey and Jarratt, 1995). 120

Both qualitative and quantitative risk analysis 121  
methods may be supported by software. On the 122  
contrary, risk analysis methods that are executed 123  
without assistance of software are referred as 124  
paper-based methods (Gordon, 1992). There are 125  
a number of risk analysis methods that are sup- 126  
ported by software (Spinellis et al., 1999). Soft- 127  
ware-based risk analysis methods may have some 128  
disadvantages. First, the cost of such methods is 129  
usually high. Second, the main frame of risk 130  
analysis process is drawn by software. Thus, some 131  
necessary variations of the risk analysis process 132  
would not be achieved. Paper-based risk analysis 133  
methods consist of meetings, discussions and work- 134  
ing sheets. One important drawback for paper- 135  
based method is their duration. Because of the 136  
nature of the meetings, paper-based methods may 137  
take a long time to give the risk results. 138

The Buddy System (Jenkins, 1998) and Cobra 139  
(C&A Systems Security Limited, 2000) are examples 140  
of risk analysis methods that are supported by 141  
software. The Buddy System is quantitative, and 142  
Cobra is qualitative. SPRINT is an example of 143  
paper-based risk analysis method (ISF, 1997). 144

Both quantitative and qualitative risk analysis 145  
methods may be supported by standards and 146  
guides like Common Criteria Framework (ISO, 147  
1999), ISO 13335 (ISO, 1996–2001), ISO 17799 148  
(ISO, 2000), NIST 800-30 Special Publication (NIST, 149  
2001) and the other standards and guides related 150  
to information technologies (Toval et al., 2002). As 151  
an example, CRAMM (CCTA, 2001) is a quantitative, 152  
software-based risk analysis method that is com- 153  
patible with standards. CORA is another risk 154  
analysis tool, which is quantitative, software 155  
based and compatible with NIST 800-30 guide 156  
(Jacobson, 2002). A risk manager can use CORA 157  
to perform risk analysis process described in NIST 158  
800-30 guide. These standards put forward robust 159  
and well-defined risk analysis methods. However, 160  
these methods may require the participation of 161

162 expert risk analysts because of complexity and  
163 formality of methods.

164 BPIRM, business process information risk man-  
165 agement, is an approach for risk management,  
166 which is suggested to close the major gaps found at  
167 some risk management practices conducted by  
168 organizations (Coles and Moulton, 2003). Under-  
169 standing the real risks by the business process  
170 owner and defining their control requirements are  
171 recommended by the method of BPRIM. Also this  
172 method is useful for establishing who is responsible  
173 for implementing and managing the controls re-  
174 lated to these risks throughout all aspects of the  
175 business process.

176 The driving force for changes to information  
177 security risk analysis is not just the technology.  
178 Information security risk analysis has been affected  
179 by the new legal requirements. Therefore, risk  
180 management is required novel governance ap-  
181 proaches. To overcome this issue, a governance  
182 approach is proposed to provide a better frame-  
183 work to manage risks (Moulton and Coles, 2003).

## 184 ISRAM: information security risk 185 analysis method

186 By taking today's information technology environ-  
187 ment into consideration, risk analysis method  
188 should allow effective participation of manager  
189 and staff into the process. In today's technological  
190 environment, if the risk analysis method contains  
191 complicated mathematical and statistical tools, it  
192 may require the expert participation and it may  
193 last for a long time. Also, the risk analysis process  
194 should not contain pure qualitative measures. This  
195 may cause subjective results. Risk analysis meth-  
196 ods that do not possess these properties may not  
197 meet the requirements of organizations. ISRAM is  
198 a quantitative, paper-based risk analysis method  
199 that is designed to have these properties.

## 200 Risk model of ISRAM

201 The underlying risk model of ISRAM is based on the  
202 following formula, which is the fundamental risk  
203 formula (NIST, 2001; McEvoy and Whitcombe,  
204 2002; USGAO, 1999).

$$\begin{aligned} \text{Risk} = & \text{Probability of occurrence of security breach} \\ & \times \text{Consequence of occurrence of security breach} \end{aligned} \quad (1)$$

208 The risk model of ISRAM, which is deduced from  
209 formula (1), is given by formula (2). Formula (2)

consists of two main parts, which are the projec- 210  
tions of two fundamental parameters in formula (1). 211

$$\text{Risk} = \left( \frac{\sum_m [T_1(\sum_i w_i p_i)]}{m} \right) \left( \frac{\sum_n [T_2(\sum_j w_j p_j)]}{n} \right) \quad (2)$$

where

*i*: the number of questions for the survey of prob- 216  
ability of occurrence, determined at Step-2; 217  
*j*: the number of questions for the survey of 218  
consequences of occurrence, determined at 219  
Step-2; 220  
*m*: the number of participants who participated 221  
in the survey of probability of occurrence, 222  
becomes definite at Step-5; 223  
*n*: the number of participants who participated 224  
in the survey of consequences of occurrence, 225  
becomes definite at Step-5; 226  
*w<sub>i</sub>*, *w<sub>j</sub>*: weight of the question "i" ("j"), 227  
determined at Step-2; 228  
*p<sub>i</sub>*, *p<sub>j</sub>*: numerical value of the selected answer 229  
choice for question "i" ("j"), determined at 230  
Step-3; 231  
*T<sub>1</sub>*: risk table for the survey of probability of 232  
occurrence, constructed at Step-4; 233  
*T<sub>2</sub>*: risk table for the survey of consequences of 234  
occurrence, constructed at Step-4; 235  
Risk: single numeric value for representing the 236  
risk. Obtained at Step-6. 237

ISRAM is basically a survey preparation and 239  
conduction process to assess the security risk in 240  
an organization. Two separate and independent 241  
survey processes are being conducted for two risk 242  
parameters in formula (2). The preparation and 243  
conduction of survey, so as the analysis of its 244  
results are defined according to the well-defined 245  
steps to yield the risk. Formula (2) represents 246  
these steps mathematically. 247

Annual Loss Expectancy (ALE) value may be 248  
required for some company managers after risk 249  
analysis. ISRAM does not make Single Loss Expec- 250  
tancy (SLE) or ALE calculations during the calcula- 251  
tion of "risk". The unit of "risk" is not in dollars. 252  
Rather, it is a single numerical value between 1 253  
and 25, which will be defined later in Table 9. 254

However, while presenting the survey result to 255  
senior management, the risk value may be con- 256  
verted to an ALE value by the risk analyst. ISRAM 257  
supports an easy conversion from the risk value to 258  
the ALE value. A sample conversion for the result 259  
of case study is given in the section 'Verification, 260  
comparison and the results of the application'. 261



## 262 The method in detail

263 The aim of ISRAM is to assess the risk caused by the  
 264 information security problems. To achieve this  
 265 goal, ISRAM is performed by using public opinion  
 266 on the problem. Public opinion is obtained by  
 267 conducting a survey. A survey is composed of  
 268 questions and answer choices related to the infor-  
 269 mation security problem. Manager, directors, tech-  
 270 nical personal and common users of computer may  
 271 be candidates for answering the survey questions.  
 272 The aim of the survey is to understand the effect  
 273 of information security problem on the system or  
 274 organization. In other words, conducting a survey  
 275 is somewhat making an as-is analysis. ISRAM makes  
 276 a structured as-is analysis to assess the risk caused  
 277 by information security problem.

278 ISRAM consists of seven main steps as shown in  
 279 Fig. 1. Of these seven steps, first four steps belong  
 280 to the survey preparation phase, fifth step is the  
 281 conduction of the survey and the last two steps  
 282 are the phase in which results are obtained and  
 283 assessed. In the survey preparation phase of  
 284 ISRAM, the questions, the number of the questions,

the weight values of the questions, the number of  
 answer choices and the numerical values of answer  
 choices are determined. Finally, the risk tables are  
 prepared.

The existence of information security problem is  
 detected in the first step. After the first step,  
 ISRAM process is divided into two parallel sub-  
 processes. One of these sub-processes is performed  
 for the probability of occurrence of security breach  
 parameter and the other is performed for the  
 consequences of occurrence of security breach  
 parameter. Hereafter, only the sub-process for  
 the probability of occurrence of security breach  
 will be explained according to Fig. 1.

In the second step, all the factors that may  
 affect the probability of occurrence of security  
 breach are listed. After listing all possible factors  
 for the risk parameter, weight values are desig-  
 nated to the factors. One factor may have more  
 effect on the probability of the occurrence than  
 the other. That's why weight values for factors are  
 designated. Weight values of the factors are in fact  
 weight values for the questions. (Factors are con-  
 verted into survey questions in the third step.)  
 Step-2 is a vital part of ISRAM to obtain the realistic  
 and objective results. To achieve this step, people  
 who have general security perspective and prefer-  
 ably company workers should participate in. These  
 staff should have enough knowledge and aware-  
 ness on the information security problem, its  
 effects and its probable causes. Also, staff should  
 have enough knowledge on the information system  
 that is affected by the problem.

In the third step, the factors are converted into  
 the survey questions and the answer choices are  
 determined for each question. Each question may  
 have different number of choices. The number of  
 choices should be selected by the risk analyst  
 according to the questions and the case being  
 analyzed. Because certain differentiations have to  
 be supplied among the answer choices of a ques-  
 tion, answer choices represent different levels.  
 After the answer choices are determined, numer-  
 ical values are designated to the answer choices.  
 The answer choices and their numerical values  
 have to be selected carefully, because, the ans-  
 wers selected by survey participants will be the  
 main assessment components for the risk. In Step-  
 6, risk amount will be calculated quantitatively  
 according to the answer choices selected by  
 participants. The team who lists the factors should  
 work carefully on the selection of the choices and  
 assignment of numerical values.

In the fourth step, two risk tables are prepared.  
 Risk tables are vital for the quantitative analysis of  
 the survey results. A risk table converts bulk survey

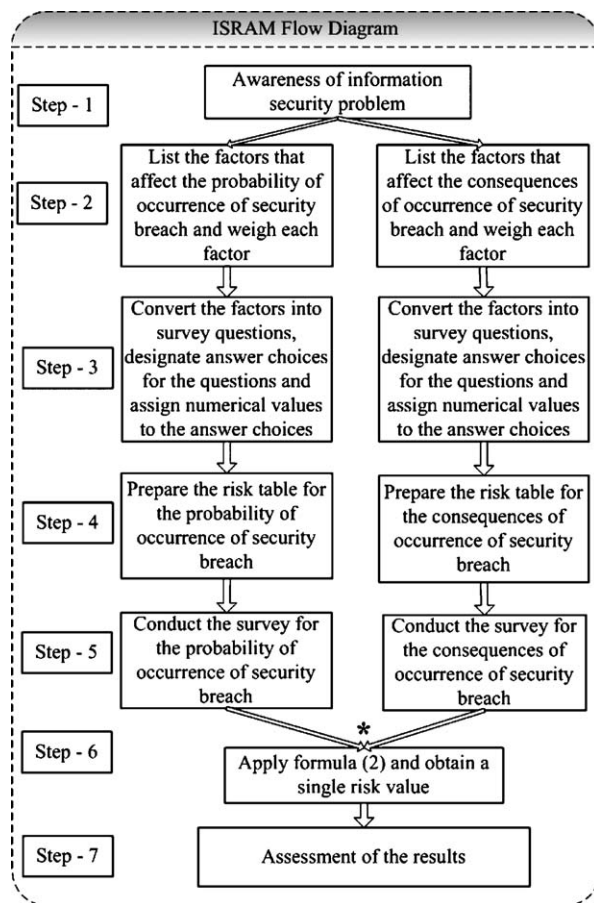


Figure 1 Basic flow diagram of ISRAM.

341 result to meaningful, quantitative and scaled  
342 values. To do this, a risk table scales all possible  
343 survey results that can be obtained from a single  
344 survey. Risk tables are the main reference points  
345 for the evaluation of the survey results. They  
346 prevent confusions while quantitatively assessing  
347 the survey results. The content of a risk table  
348 changes according to the surveys conducted. A risk  
349 table forms a connection between the result of  
350 survey and the quantitative value of the risk  
351 parameter under consideration.

352 Survey is conducted after the preparation of risk  
353 tables is over. This is the fifth step of ISRAM. This  
354 step is the most peculiar part of ISRAM in which  
355 ordinary information system users participate ac-  
356 tively into the risk analysis process. At Step-5,  
357 the survey questions can be distributed to the relevant  
358 staff as hard copy or it can be answered electron-  
359 ically. The questions for two risk parameters can  
360 be delivered in one survey or it is possible to  
361 deliver separate surveys for two risk parameters.  
362 In this case, the number of participants may be  
363 different for two surveys. It is important to note  
364 that the answers to the survey questions are  
365 valuable information for risk analysis process. But  
366 the main purpose of ISRAM is to convert these  
367 answers into numeric values.

368 In the sixth step, formula (2) is applied to get  
369 single quantitative risk result from answered sur-  
370 veys. An example of application of formula (2) is  
371 given in Table 10, which shows the calculations for  
372 our case study.

373 Step-7 is the assessment phase of ISRAM. In the  
374 assessment phase, not only the numerical survey  
375 result, which is obtained in Step-6, is assessed  
376 but also the answers to the survey questions are  
377 analyzed.

378 All of these phases allow the active participa-  
379 tion of managers and staff into the risk analysis

380 process. Among these seven steps, addition, multi-  
381 plication and division operations are used only in  
382 Steps 4 and 6. Other complicated mathematical  
383 and statistical calculations are not used in these  
384 steps.

385 Steps 2–4 are the most vital parts of ISRAM for  
386 an objective risk analysis. Company staff must  
387 work carefully during these steps to vanish any  
388 subjectivity and incompleteness.

## Practice of ISRAM

389

390 In the case study, ISRAM was used to analyze the  
391 risk arising from computer viruses. Our environ-  
392 ment for risk analysis was composed of 20 com-  
393 puters on a Local Area Network (LAN) as shown  
394 in Fig. 2. These computers belong to a research  
395 institute and are used by staff to connect to  
396 Internet. Every computer has a dedicated user.  
397 However, any of the computers in the network can  
398 be used by any user. Twenty institute workers took  
399 action in the survey to obtain the public opinion on  
400 computer viruses.

### Step-1: awareness of the problem

401

402 As it has been already said in the previous  
403 paragraph, the information security problem is  
404 caused by computer viruses. Computers which  
405 are used in the case study do not have appropriate  
406 antivirus software installed. Personal firewall  
407 products are installed in a few computers. It is  
408 apparent that there is a strong requirement for  
409 a structured risk analysis in which the probability  
410 of a virus infection and the consequences of an  
411 incident is estimated.

412 Technically oriented people of the institute  
413 realize the information security problem and de-  
414 cide to make a risk analysis. The first step of ISRAM  
415 is completed.

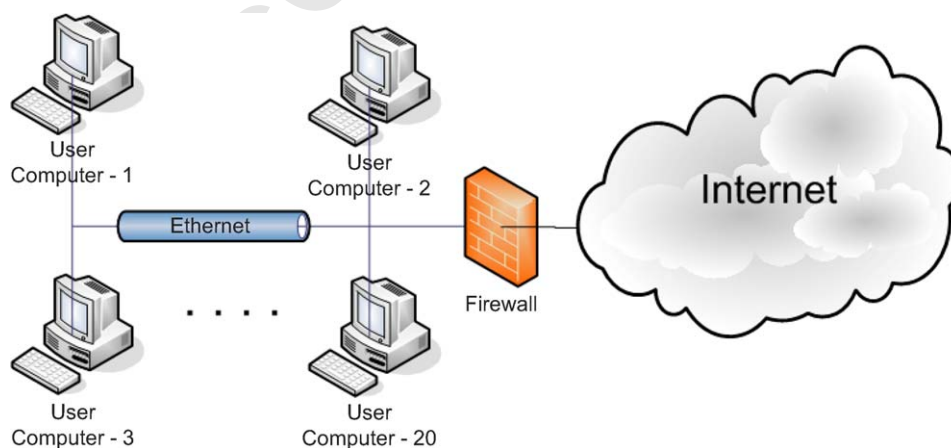


Figure 2 Environment of ISRAM.

### 416 **Step-2: listing and weighing the factors**

417 At Step-2, separate analyses are made for two risk  
418 parameters to determine the factors, which affect  
419 these parameters.

420 After determining and listing all the factors,  
421 weight factors are assigned to the factors by using  
422 Table 1. The value of assets, the strength of  
423 already existing countermeasures, and the level  
424 of vulnerabilities are all considered during the  
425 assignment of weight factors.

426 After the discussions among risk analysis team, 21  
427 factors are determined that affect the probability  
428 of a virus infection. Fifteen factors that affect the  
429 consequences of infection are determined. Among  
430 these factors, six of them affect both parameters.

431 Three of the factors are directly associated with  
432 vulnerabilities of operating system and patch level  
433 (these three factors affect both risk parameters).

434 Some of the factors that affect the probability  
435 of a virus infection and their equivalent weight  
436 values are shown in Table 2. (Because of the space  
437 constraints, all the factors could not be written.)

438 Some of the factors that affect the consequen-  
439 ces of a virus infection and their equivalent weight  
440 values are shown in Table 3.

441 Six factors that affect both the probability and  
442 the consequences of a virus infection and their  
443 equivalent weight values are shown in Table 4.

444 First three factors in Table 4 are directly  
445 associated with vulnerabilities of systems. Note  
446 that these factors affect both the probability and  
447 the consequences of infection. These factors have  
448 also considerable weight values.

### 449 **Step-3: converting factors into questions, 450 designating answer choices and assigning 451 numerical values**

452 At Step-3, all the factors are converted into survey  
453 questions and answer choices are designated. The

**Table 2** Some of the factors that affect the probability

Factor	Weight value
The type of attachment of e-mails	3
The number of e-mails per day	1
The number of different websites entered per day	1
The source of floppies	2
The number of files downloaded per day	1

number of answer choices can change according to 454  
the type and structure of survey question. In our 455  
case study, there are a total number of 30 survey 456  
questions. Ten of these questions have only two 457  
answer choices (six of them are yes/no questions). 458  
Sixteen of the questions have four answer choices. 459  
Four of the questions have three answer choices. 460  
Apart from yes/no questions, all questions have an 461  
answer choice, named "Other:" If a participant can- 462  
not find an appropriate answer among dedicated 463  
choices, he/she is expected to write his/her answer 464  
there. 465

After designation of answer choices, Table 5 is 466  
used to convert answer choices into numerical 467  
values. 468

Some of the questions and their answer choices 469  
are shown in Table 6. The weight values of 470  
questions and the numerical values of answer 471  
choices are also given in parenthesis. In questions 472  
column, "p" in parenthesis means that the factor 473  
affects the probability of infection and "c" in 474  
parenthesis means that the factor affects the con- 475  
sequences of infection. Note that, if the question 476  
(factor) affects both parameters (probability 477  
and consequences), then first numerical weight 478  
value in next parenthesis is for the probability of 479

**Table 1** Reference table for the weight values of the factors

Weight value	Explanation
3	The factor is directly associated with a severe vulnerability and/or the factor is directly associated with a critical asset and/or there is no countermeasure in place. Because of these reasons, the factor is most effective factor that affects the probability of infection or the consequences of infection. The factor contributes directly to the value of the risk parameter.
2	The factor is somewhat associated with a vulnerability and/or the factor is directly associated with an important asset and/or there is a few countermeasure in place. Because of these reasons, the factor is slightly/normally effective factor that affects the probability of infection or the consequences of infection. The factor contributes somewhat directly to the value of the risk parameter.
1	The factor is a little associated with vulnerability and/or the factor is indirectly associated with an important asset and/or there are enough countermeasures in place. Because of these reasons, the factor is least effective factor that affects the probability of infection or the consequences of infection. The factor contributes indirectly to the value of the risk parameter.

**Table 3** Some of the factors that affect the consequences

Factor	Weight value
The backup condition of files	3
The place of files	2
The importance of files in a computer	3
The dependence to files and applications	2

480 infection and the other one is for the consequences  
481 of infection.

482 For a participant, more than one choice may be  
483 applicable. In this case, the most effective choice

501 each of the answer choices, numerical values  
502 between 0 and 4 are determined.

503 To construct a risk table, firstly, minimum and  
504 maximum numerical values that can be obtained  
505 from the survey of risk parameter are found.  
506 Formula (3) is applied in order to find the minimum  
507 and maximum survey results of the probability of  
508 infection parameter. For our case study, the value  
509 of “ $i$ ” is 21, “ $w_i$ ” is the weight of “ $i$ th” question,  
510 and “ $p_i$ ” is the value of the answer choice for  
511 question- $i$ . Maximum value for a survey is found  
512 out by assuming that a participant chooses the  
513 most influential answer choice for all questions (so  
514 that “ $p_i$ ” has its maximum possible value). In this  
515 case, “maximum output” equals to 128.

$$\sum_i w_i p_i \left\{ \begin{array}{l} i: \text{the number of the questions} \\ w: \text{the weight of the } i\text{th question} \\ p: \text{the value of the selected answer choice of the } i\text{th question} \end{array} \right\} \quad (3)$$

484 (the choice which has the largest numerical value)  
485 is used during calculations.

#### 486 Step-4: preparation of risk tables

487 Two risk tables are constructed for our case study  
488 (one for the probability of infection parameter and  
489 one for the consequences of infection parameter).  
490 Each of the tables has five levels to represent the  
491 level of risk parameter. These dynamic tables  
492 scale the possible results of the surveys of the  
493 fundamental risk parameters both quantitatively  
494 and qualitatively.

495 For the probability of infection parameter,  
496 there were 21 factors, so 21 survey questions are  
497 applied. Until now, each of these questions was  
498 weighted. Answer choices were designated to each  
499 of these questions. Different number of answer  
500 choices was designated for survey questions. For

516 Minimum value for a survey is found by assuming  
517 that a participant chooses the least influential  
518 answer choice for all the questions (so that “ $p_i$ ”  
519 has its maximum possible value). The “minimum  
520 output” is 29 for our case study.

521 One hundred and twenty-eight points, which is  
522 the maximum possible value for a survey result  
523 present the highest probability of infection by  
524 a virus. Twenty-nine points, which is the minimum  
525 possible value for a survey result present the  
526 lowest probability of infection by a virus. In  
527 Table 7, the values between 29 and 128 are  
528 arranged to represent risk levels. Possible survey  
529 results presented in Table 7 are scaled and  
530 matched to quantitative and qualitative values.

531 While building the risk table, the possible survey  
532 values are grouped evenly and scaled to represent  
533 the level of risk parameter. It may not be possible

**Table 4** Factors that affect both the probability and the consequences

Factor	Weight value for probability	Weight value for consequences
The operating system of computer	3	3
The update against vulnerabilities	3	3
The type of user account	2	3
The frequency of update	1	2
Access to the shared folders of other computers	1	2
The number of computers which are accessed by sharing	1	2



**Table 5** Numerical values of answer choices

Numerical value of answer choice	Explanation
4	Most effective answer choice. Affect enormously the probability of occurrence or consequences of occurrence.
3	Rather effective answer choice. Affect highly the probability of occurrence or consequences of occurrence.
2	Somewhat effective answer choice. Affect considerably the probability of occurrence or consequences of occurrence.
1	Least effective answer choice. Affect slightly the probability of occurrence or consequences of occurrence.
0	No effect on the probability of occurrence or consequences of occurrence.

534 for all intervals to be divided evenly. In this case,  
 535 interval of excess should be assigned to the most  
 536 critical value. Table 7 is the risk table constructed  
 537 for the probability of infection parameter. In the  
 538 case study, the interval of "very high probability"  
 539 is 20. The intervals of other four scales are 19.

The other risk table is for the consequences of 540  
 infection. The same calculations for maximum and 541  
 minimum values of survey output were made for 542  
 the consequences of infection variable during our 543  
 case study. To find these values, formula (4) is 544  
 used. This is the same as formula (3), except "j" is 545

**Table 6** Some of the questions and their respective answer choices

Questions	Answer choices				
	a	b	c	d	e
What do you do at Internet? (p) (2)	Download (4)	Sending and receiving e-mails (3)	Chat (2)	Reading newspapers and articles (0)	Other:
How many different sites do you visit? (p) (1)	More than 10 (4)	7–9 (3)	5–7 (2)	Less than four (1)	Other:
What type of files do you download? (p) (2)	Executables (4)	Scripts (3)	Documents (1)	No download (0)	Other:
What is the importance of files present at your computer? (c) (3)	Very important and only at my computer (4)	Important, there are copies at other computers (3)	Not important (0)	Other:	—
What is the operating system of your computer? (p) (c) (3) (3)	Belongs to Windows family (4)	Linux/Unix (0)	Other:	—	—
In what account do you use your computer? (p) (c) (2) (3)	Administrator/root (4)	Normal user (1)	Other:	—	—
Do you update your computer against vulnerabilities? (p) (c) (3) (3)	No (4)	Yes (0)	—	—	—

**Table 7** Risk table for the survey of probability of infection parameter

Survey result	Qualitative scale	Quantitative scale
29–48	Very low probability	1
49–68	Low probability	2
69–88	Medium probability	3
89–108	High probability	4
108–128	Very high probability	5

546 used to represent the questions of the consequen-  
547 ces of occurrence parameter.

$$\sum_j w_j p_j \left\{ \begin{array}{l} j: \text{the number of the question} \\ w: \text{the weight of the } j\text{th question} \\ p: \text{the value of the selected answer choice of the } j\text{th question} \end{array} \right\} \quad (4)$$

548 According to formula (4), “maximum output” is  
549 found to be 160 and “minimum output” is calcu-  
550 lated as 47.

551 Table 8 is constructed for the consequences of  
552 infection parameter. For this risk table, interval of  
553 excess is 26, which is for “very serious consequen-  
554 ces”. The interval values of other scales are all 21.

555 A final risk table, Table 9, is prepared by using  
556 Tables 7 and 8 according to the fundamental risk  
557 formula. The final risk table prevents confusions in  
558 the last step of ISRAM, which is the assessment  
559 phase. This final risk table is static. The uppermost  
560 row of the final risk table shows the quantitative  
561 values of probability of infection parameter. The  
562 leftmost column shows the quantitative values of  
563 consequences of infection parameter. The multi-  
564 plication of these two values according to formula  
565 (1) gives the various risk values between 1 and 25.

566 The number of survey questions, the types of  
567 questions and the structures of risk tables are  
568 changeable according to the information security  
569 problem. The flexibility of the method allows

**Table 8** Risk table for the survey of consequences of infection parameter

Survey result	Qualitative scale	Quantitative scale
47–68	Negligible consequences	1
69–90	Minor consequences	2
90–111	Important consequences	3
112–133	Serious consequences	4
134–160	Very serious consequences	5

ISRAM to apply to diverse information security 570  
571 problems effectively.

To obtain consistent and accurate results from 572  
573 a survey, it is important to carefully list the factors  
574 and prepare the questions and answers. According  
575 to the nature of problem, the number and type of  
576 staff that participate in a survey may change. All  
577 staff may participate in a survey that plans to  
578 express the risk that arises from viruses.

#### Step-5: conduction of the survey 579

After preparation of risk tables for two risk 580  
581 parameters and the final risk table, the survey is  
582 ready for the distribution to the related staff.

Thus, the preparation phase of the survey process 583  
584 is over. At Step-5, the survey questions are  
585 distributed to the relevant staff as hard copy. In  
586 our case study, one survey, which contains the  
587 questions of both risk parameters are submitted to  
588 the user. Twenty people participated in the survey.

#### Step-6: application of formula (2) and obtaining 589 590 a single risk value

After Step-5 is finished, formula (2) is applied. In 591  
592 our case study, the probability for a computer to  
593 be infected by a virus is found to be 3.8, which is  
594 close to “high probability” at qualitative scale.  
595 The consequence of a virus infection is found to be  
596 4.05, which is approximately “serious consequen-  
597 ces” at qualitative scale. As a result, the value of  
598 risk is found to be 15.39, which is high level risk  
599 according to the final risk table, Table 9.

Detailed survey results are given in Table 10. In 600  
601 this table, the bulk survey results, simplified  
602 survey results (after risk conversion tables) for all  
603 participants, values of risk parameters and the  
604 final risk value are given. The detail of application  
605 of formula (2) is clearly seen in Table 10.

#### Step-7: assessment of the results 606

The most important output of ISRAM is the single risk 607  
608 value obtained at Step-6. This risk value is obtained  
609 after performing considerable amount of prelimi-  
610 nary work including listing the factors, designat-  
611 ing answer choices, weighting the factors, giving  
612 numerical values to answer choices and preparing  
613 risk tables. The quality of this preliminary work  
614 definitely affects the accuracy of single risk value.

**Table 9** The final risk table prepared from risk tables (Tables 7 and 8)

Risk = (1) × (2)	1: Very low	2: Low	3: Medium	4: High	5: Very high
1: Negligible	1: Very low	2: Very low	3: Very low	4: Low	5: Low
2: Minor	2: Very low	4: Low	6: Low	8: Medium	10: Medium
3: Important	3: Very low	6: Low	9: Medium	12: Medium	15: High
4: Serious	4: Low	8: Medium	12: Medium	16: High	20: Very high
5: Very serious	5: Low	10: Medium	15: High	20: Very high	25: Very high

615 On the other hand, not only these calculations  
616 and the final numerical result are considered but  
617 also answers given for questions are examined in  
618 detail by the risk analysts while assessing the  
619 survey results.

620 By examining the answers to the survey ques-  
621 tions in the case study, some important results  
622 are obtained. Some of the users have adminis-  
623 trative privileges while using their computers,  
624 which increases both the probability and con-  
625 sequences. USB storage devices and CD-ROMs  
626 (not floppies) widely used in the network. Most  
627 of the users do not backup their data. A small  
628 group of the users download programs. Half of

the participants do not patch their computer. 629  
This is a great vulnerability for virus infection. In 630  
general, user security awareness should reduce 631  
somewhat the probability and consequences of 632  
infection. 633

The structure of ISRAM allows the gross risk and 634  
net risk calculations. After user security awareness 635  
program is held, the same survey is performed to 636  
obtain the net risk value. In our case study, after 637  
user security awareness program, risk value is 638  
found to be 14.3, which is between medium and 639  
high risk but very close to the high risk level. 640

The assessment of survey results is an important 641  
part of ISRAM. Managers and staff can easily 642

**Table 10** Survey results

Participant- <i>m</i> ( <i>m</i> is equal to <i>n</i> in our case study)	Probability of infection (bulk result) $\sum w_i p_i$ where $i = 1 \dots 21$	$T_1$	Consequences of infection (bulk result) $\sum w_j p_j$ where $j = 1 \dots 15$	$T_2$
Participant-1	94	4	103	3
Participant-2	100	4	124	4
Participant-3	74	3	95	3
Participant-4	73	3	112	4
Participant-5	110	5	121	4
Participant-6	97	4	113	4
Participant-7	89	4	129	4
Participant-8	88	3	118	4
Participant-9	99	4	105	3
Participant-10	85	3	135	5
Participant-11	93	4	136	5
Participant-12	124	5	156	5
Participant-13	69	3	98	3
Participant-14	95	4	123	4
Participant-15	96	4	145	5
Participant-16	90	4	119	4
Participant-17	118	5	135	5
Participant-18	71	3	129	4
Participant-19	94	4	113	4
Participant-20	71	3	123	4

$$\left( \frac{\sum_m [T_1 (\sum_i w_i p_i)]}{m} \right) = 3.8 \quad \left( \frac{\sum_n [T_2 (\sum_j w_j p_j)]}{n} \right) = 4.05$$

$$\text{Risk} = \left( \frac{\sum_m [T_1 (\sum_i w_i p_i)]}{m} \right) \left( \frac{\sum_n [T_2 (\sum_j w_j p_j)]}{n} \right) = 15.39$$

643 participate into this step like other steps and  
644 express their opinions.

645 The survey results are assessed and suggestions  
646 are put forward for the risk mitigation process.  
647 The outcome of ISRAM is a risk report, which  
648 clearly puts forward the survey results and as-  
649 sseses these results.

## 650 Verification, comparison and the results 651 of the application

652 In order to verify the results of ISRAM case study,  
653 we have gathered statistical data and run simula-  
654 tion based on statistical data obtained. Arena  
655 simulation software has been used to model the  
656 risk environment and simulate on the real statisti-  
657 cal data.

658 By making analyses on the pilot network, it is  
659 seen that, three main sources of virus are e-mails,  
660 downloads (or USB storage devices) and floppy  
661 diskettes (or CD-ROMs). So, the gathered statisti-  
662 cal data are composed of the number of received  
663 e-mails, downloads and storage media usage  
664 per day, per computer and per user basis. The  
665 statistical data were gathered for one month.  
666 During this month, virus incidents were carefully  
667 noted. The sources and number of infections were  
668 written down.

669 After the completion of gathering of the statis-  
670 tical data, three independent risk models were  
671 constructed at Arena software because of the  
672 independency of sources of data, which come to  
673 computers.

674 In the risk models, data were generated by the  
675 entities represented by exponential probability

distribution function. Mean value of the probabili- 676  
ity distribution function was determined according 677  
to the gathered statistical data for e-mail traffic, 678  
number of downloads and storage media usage. 679  
The generated data were passed through the 680  
probability of infection and the consequences of 681  
infection entities for all three risk models. The 682  
probability of infection was constructed according 683  
to the statistical data. Consequences of infection 684  
entities were constructed after the discussion with 685  
experts. 686

The gathered statistical data were imported 687  
into the risk model and based upon the real 688  
statistical data, Arena software simulated the 689  
situation of the test network as if one year of 690  
period had passed. Table 11 shows the final result 691  
of this simulation. 692

The simulation results revealed the similar 693  
results as ISRAM application. As it is seen in Table 694  
11, there are a number of virus infections in one 695  
year, which can correspond to the high level of 696  
probability. Also, as it can be easily seen from the 697  
last five rows of table, most of the infected viruses 698  
have serious consequences. These two results are 699  
compatible with the results obtained at the Step-6 700  
of ISRAM. At Step-6 of ISRAM, formula (2) was 701  
applied and single values for probability of in- 702  
fection and consequences of infection were found. 703  
The value for the first parameter was close to high 704  
probability level and the value for the second 705  
parameter was approximately equal to serious 706  
consequences level. 707

"As-if" analyses are also performed during 708  
simulation. If the users perform updates and 709  
backup operations, the probability and consequen- 710  
ces of virus infections decrease dramatically. But it 711

**Table 11** Simulation results

Risk report 1	Date: 17 May 2004
E-mail virus model	Time: 2:34:51PM
Model parameter	Average
Total e-mails	25342.1000
The number of e-mails that contain viruses	42.6000
The number of e-mails that contain viruses, which infect	32.5000
Total downloads	5245.1200
The number of downloads that contain viruses	12.0732
The number of downloads that contain viruses, which infect	10.0200
Total storage media usage	17445.3400
The number of storage media that contain viruses	8.334
The number of storage media that contain viruses, which infect	6.5300
The number of infections that cause very serious consequences	3.0000
The number of infections that cause serious consequences	19.0500
The number of infections that cause important consequences	5.0450
The number of infections that cause minor consequences	12.9550
The number of infections that cause negligible consequences	9.0000



712 should not be expected from users to perform  
713 these operations.

714 Consequently, the results of simulation based on  
715 gathered statistical data are compatible with the  
716 results of ISRAM case study. ISRAM gives the similar  
717 results in a much shorter time period without  
718 struggling with statistical data and by allowing  
719 participation of staff.

720 An important advantage of ISRAM is its appro-  
721 priateness to ALE calculations. In order to present  
722 the survey result to the senior management, ALE  
723 calculations can be performed. Some managers  
724 may desire to see monetary losses rather than  
725 single numerical values.

726 Calculation of ALE can be achieved as in  
727 formula (5).

Annual Loss Expectancy

$$\begin{aligned} &= \text{Threat Occurrence Rate per Year} \\ &\quad \times \text{Single Loss Expectancy} \end{aligned} \quad (5)$$

731 where, the unit of Annual Loss Expectancy is  
732 "dollars per year". Similarly the unit of Single Loss  
733 Expectancy is "dollars per worst case occur-  
734 rence". "Threat Occurrence Rate per Year" can  
735 be characterized as "the probability of virus  
736 infection" and "Single Loss Expectancy – SLE"  
737 can be characterized as "the consequences of  
738 virus infection"

739 For ALE calculation, it is necessary to convert  
740 the numerical values of two risk parameters to  
741 threat occurrence per year and SLE values. In our  
742 case study, the probability of virus infection was  
743 found to be 3.8 – high probability, the conse-  
744 quence of a virus infection was found to be 4.05 –  
745 serious consequences. Risk analysts can convert  
746 these results to "Threat Occurrence Rate per  
747 Year" and "Single Loss Expectancy" values by  
748 taking companies situation into consideration.  
749 For our case study, "Threat Occurrence Rate per  
750 Year" is designated as 50 occurrences per year and  
751 "Single Loss Expectancy" is designated as 40\$.  
752 Therefore, ALE is equal to 2000\$. This is more than  
753 the cost of an antivirus software package for an  
754 institute. Thus, it is easily said that the lack of  
755 antivirus software exposes high risk to institute.

## 756 Conclusion

757 In this study, a novel method, ISRAM, is proposed  
758 for information security risk analysis. The pro-  
759 posed method is based on a quantitative approach  
760 that uses survey results to analyze information  
761 security risks.

Quantitative tools included in ISRAM are simple  
762 numbers related with the survey, risk tables,  
763 addition, multiplication and division operations.  
764 The main advantage of ISRAM over other risk  
765 analysis methods is its ease of use. There are no  
766 complicated mathematical and statistical instru-  
767 ments in ISRAM.  
768

769 Previously, it was mentioned that qualitative  
770 methods might give subjective results. ISRAM is  
771 a quantitative tool with well-defined steps and  
772 mathematical measures. With a careful operation,  
773 ISRAM gives objective risk results. The comparison  
774 of the case study and simulation results proves this  
775 statement.

776 Software-based risk analysis methods have a rigid  
777 frame. During risk analyses in which software is  
778 used, necessary variations may not be achieved.  
779 This is not the case for ISRAM. ISRAM does not have  
780 rigid frames. The number of questions and answer  
781 choices, risk tables, weight values and the other  
782 values may be changed from one analysis to  
783 another. ISRAM has well-defined steps, and there-  
784 fore it is deterministic. There is no risk of long  
785 period of analysis like the paper-based methods.

786 Because ISRAM is a quantitative method which  
787 does not contain complicated mathematical and  
788 statistical instruments, manager and the staff may  
789 effectively participate in the risk analysis process.  
790 It is suggested that information security risk anal-  
791 ysis should be more business oriented. Thus, less  
792 technology and more culture and organization  
793 should be used in order to succeed (McEvoy and  
794 Whitcombe, 2002; Sommer, 1994; Reid and Floyd,  
795 2001). ISRAM fulfills both the business and tech-  
796 nology requirements by taking today's needs into  
797 consideration.

798 ISRAM may be used for a wide range of prob-  
799 lems. From technical problems like the one in our  
800 case study, to procedural and political issues like  
801 to find out the risk arises from the weaknesses of  
802 information security policies.

## References

- Bilbao A. TUAR. A model of risk analysis in the security field, CH3119-5/92. IEEE; 1992. 804  
805  
C&A Systems Security Limited. COBRA consultant products for 806  
windows. Evaluation & user guide; 2000. 807  
Coles RS, Moulton R. Operationalizing IT risk management. 808  
Computers & Security 2003;22(6):487–93. 809  
Gerber M, Solms RV. From risk analysis to security requirements. 810  
Computers & Security 2001;20(7):577–84. 811  
Gordon J. Security modelling, risk analysis methods and tools. 812  
IEE colloquium; 1992. p. 6/1–6/5. 813  
Information Security Forum (ISF). Simplified practical risk 814  
analysis methodology (SPRINT) user guide; 1997. p. 43–57. 815

- 816 ISO. Evaluation criteria for IT security ISO15408, Parts 1 thru 3. 846  
817 Geneva: ISO; 1999. 847
- 818 ISO. Guidelines for the management of IT security ISO 13335, 848  
819 Parts 1 thru 5. Geneva: ISO; 1996–2001. 849
- 820 ISO. Code of practice for information security management ISO 850  
821 17799. Geneva: ISO; 2000. 851
- 822 Jacobson RV. Using CORA to implement the NIST risk manage- 852  
823 ment guide Available from: <[http://www.ist-usa.com/  
824 Downloads/UsingCORA with NISTSP800-30.zip](http://www.ist-usa.com/Downloads/UsingCORA%20with%20NISTSP800-30.zip)>; 2002. 853
- 825 Jenkins BD. Security risk analysis and management White Paper, 854  
826 Countermeasures Inc. Available from: <[http://www.cs.  
827 kau.se/~albin/Documents/RA\\_by%20Jenkins.pdf](http://www.cs.kau.se/~albin/Documents/RA_by%20Jenkins.pdf)>; 1998. 855
- 828 Kailey MP, Jarratt P. RAMEX: a prototype expert system for 856  
829 computer security risk analysis and management. *Computers & Security* 1995;14(5):449–63. 857
- 830 McEvoy N, Whitcombe A. Structured risk analysis InfraSec 2002. 858  
831 LNCS 2437; 2002. p. 88–103. 859
- 832 Moulton R, Coles RS. Applying information security governance. 860  
833 *Computers & Security* 2003;22(7):580–4. 861
- 834 National Institute of Standards and Technology (NIST). Risk 862  
835 management guide for information technology systems 2001. Special Publication 800-30. 863
- 836 Owens S. Information security management: an introduction. 864  
837 British Standards Institution; 1998. 865
- 838 Reid RC, Floyd SA. Extending the risk analysis model to include 866  
839 market-insurance. *Computers & Security* 2001;20(4):331–9. 867
- 840 Spinellis D, Kokolakis S, Gritzalis S. Security requirements, risks 868  
841 and recommendations for small enterprise and home–office 869  
842 environments. *Information Management & Computer Security* 1999;7(3):121–8.
- Sommer P. Industrial espionage: analysing the risk. *Computers & Security* 1994;13(7):558–63. 846
- Toval A, Nicolas J, Moros B, Garcia F. Requirements reuse for 848  
improving systems security: a practitioner’s approach. 849  
*Requirements Engineering* 2002;6:205–19. 850
- United Kingdom Central Computer and Telecommunication 851  
Agency (CCTA). Risk analysis and management method, 852  
CRAMM user guide, Issue 2.0 2001. 853
- United States General Accounting Office (USGAO). Information 854  
security risk assessment, <[http://www.gao.gov/cgi-bin/  
855 getrpt?GAO/AIMD-00-33](http://www.gao.gov/cgi-bin/getrpt?GAO/AIMD-00-33)>; 1999. 856
- Bilge Karabacak** received his B.Sc. degree in Electronic 855  
Engineering from Bilkent University in 1999, and his M.Sc. 856  
degree in Computer Engineering from Gebze Institute of 857  
Technology in 2003. Currently he is pursuing Ph.D. degree in 858  
Computer Engineering at Gebze Institute of Technology. His 859  
interested areas are risk management, network security and 860  
application security. 861
- İbrahim Soğukpınar** received his B.Sc. degree in Electronic and 860  
Communications Engineering from Technical University of 861  
İstanbul in 1982, and his M.Sc. degree in Computer and Control 862  
Engineering from Technical University of İstanbul in 1985. He 863  
received his Ph.D. degree in Computer and Control Engineering 864  
from Technical University of İstanbul in 1995. Currently he is the 865  
Assistant Professor at Computer Engineering Department in 866  
Gebze Institute of Technology. His interested areas are in- 867  
formation security, networking, information systems applica- 868  
tions and computer vision. 869

Available online at [www.sciencedirect.com](http://www.sciencedirect.com)

SCIENCE @ DIRECT®