Assessments

1) Parameters used for determining *TIME* and *SIZE* are sufficient for researching information security of objects and computer systems and networks for consumer, not governmental (corporate) needs.

2) Evaluation in regard to the selected objects, which were processed with methods of compression, is positive and the allowances do not affect the derived result.

3) In regard to the methods of compression we used the assessment is positive and the above mentioned experiments can be used and tailored to other methods of compression.

4) We can conclude, looking at the experiments, that with the decreasing size of an object after compression, time needed for an attack to complete its work over the object will increase.

5) As with the co-efficient of information security the best results were obtained from data objects, processed with dictionary methods of compression, and the worst results were obtained with the graphics objects processed with statistical methods of compression.

6) From all 59 methods of compression, 13 of them gave us the highest value of the co-efficient of information security of the object. They are from the group of dictionary methods and image methods of compression.

Bibliography

[1] Elena Ferrari, Bhavani M. Thuraisingham, *Web and Information Security*, IRM Press, 2006, ISBN: 1-59140-589-0, p. 215

[2] http://www.answers.com/file

[3] David Salomon, *Data Compression: The Complete Reference*, Springer, 2006, ISBN: 1846286026, p.1-9

[4] Polimirova, D., Nickolov, E., Nikolov, C., *Investigating The Relations Of Attacks, Methods And Objects In Regard To Information Security In Network TCP/IP Environment*, International Journal "Information Theories & Applications", vol. 1 / 2007, Number 1, ISSN 1313-0455, p. 85-92

[5] Hubert Hasenauer, *Sustainable Forest Management: Growth Models for Europe*, Springer 2006, ISBN: 9783540260981 p.267-269

Authors' Information

*PhD Student, **Dimitrina Polimirova**, Research Associate, National Laboratory of Computer Virology, Bulgarian Academy of Sciences, Phone: +359-2-9733398, E-mail: polimira@nlcv.bas.bg.*

*Prof. **Eugene Nickolov**, DSc, PhD, Eng, National Laboratory of Computer Virology, Bulgarian Academy of Sciences, Phone: +359-2-9733398, E-mail: eugene@nlcv.bas.bg.*

ICT SECURITY MANAGEMENT

Jeanne Schreurs, Rachel Moreau

***Abstract**: Security becomes more and more important and companies are aware that it has become a management problem. It's critical to know what are the critical resources and processes of the company and their weaknesses. A security audit can be a handy solution. We have developed BEVA, a method to critically analyse the company and to uncover the weak spots in the security system. BEVA results in security scores for each security factor and also in a general security score. The goal is to increase the security score Ss to a postulated level by focusing on the critical security factors, those with a low security score.*

***Keywords**: Security, Scan, Audit*

Introduction

As a consequence of the fast integration of technologies as Internet, Intranet, Extranet, Voice over IP and e-commerce, companies ICT-infrastructure will move to more openness to the outside world and as a consequence will become more vulnerable for security threats. This offers lots of new opportunities but also creates new threats. That's why focus and responsibility concerning security become even more and more important. The Computer Crime and Security Survey 2005 shows that these are the 10 most frequent attacks or misuses: Virus, insider abuse of net access, laptop/mobile theft, unauthorized access to information, denial of service, abuse of wireless network, system penetration, theft of proprietary info, telecom fraud and financial fraud. Figures show that attacks come from inside as well as from outside the organisation and bring along large costs. Especially unauthorized access and laptop and mobile theft becomes a enormous expense for the companies during the last years. Because of these large costs, companies became more and more aware that they not only deal with a technical problem but also with a management problem. To tackle this management problem, it is quite important to know the ICT-security state your company is in.

ICT security management

Spending each year a certain amount on security measures is not enough. A company needs a total security approach. It is a must to know what are the critical resources and processes of the company and their weaknesses so the can be protected in the right way.

A solution to this is a security audit. A security audit is ideal to detect the weak spots in the ICT security state of the company. Based on the results of the audit, a security policy can be developed, adjusted to the company situation. A security audit can be used to analyse and describe the security level.

1. Security audit checklist

We have developed a security audit, called BEVA. BEVA is a method to analyse critically the company and to uncover the weak spots of the security system. It positions the company on point of the security aspects in the different areas of business functions. We have developed a standard list that covers all aspects of security, structured in 10 domains being:

- Security policy
- Organization of information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development and maintenance
- Information secuirity incident management
- Business continuity management

Each of these areas consists of different security factors. The factors are in their turn tested on the basis of several subcriteia. Our list for the security factors is based on the standard ISO 17799. The 38 security factors are spread over the 10 domains, as set forward in the standard ISO17799 model.

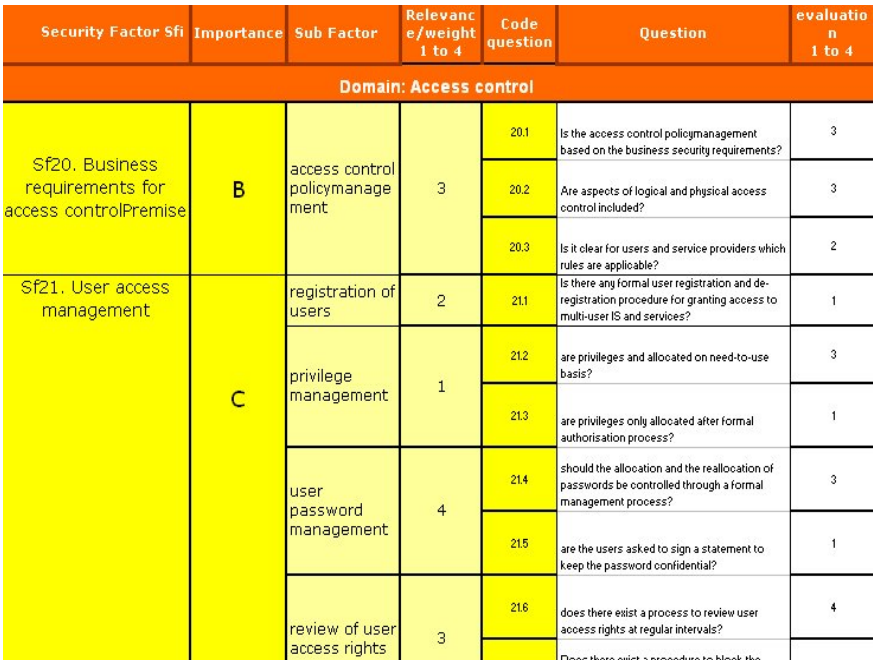
For example you have the domain "access control" and in this domain you have the factors: requirements for access, management of user access, user responsibility, control of network access, control access to OS, control of access to applications and information and use of mobile infrastructure.

For each of the 38 factors, a number of subcriteria are formulated. We developed a list of questions, covering the subcriteria we created. The questions are partly based on the "checklists in information management" SDU publishers. (www.riskworld.net/7799-2.htm).

2. The audit process and the calculation of security factor scores Sfi's and the security score Ss

To collect the information about the current security situation of the company, we start with the questioning of the key persons in the company using the audit checklist questionnaire.

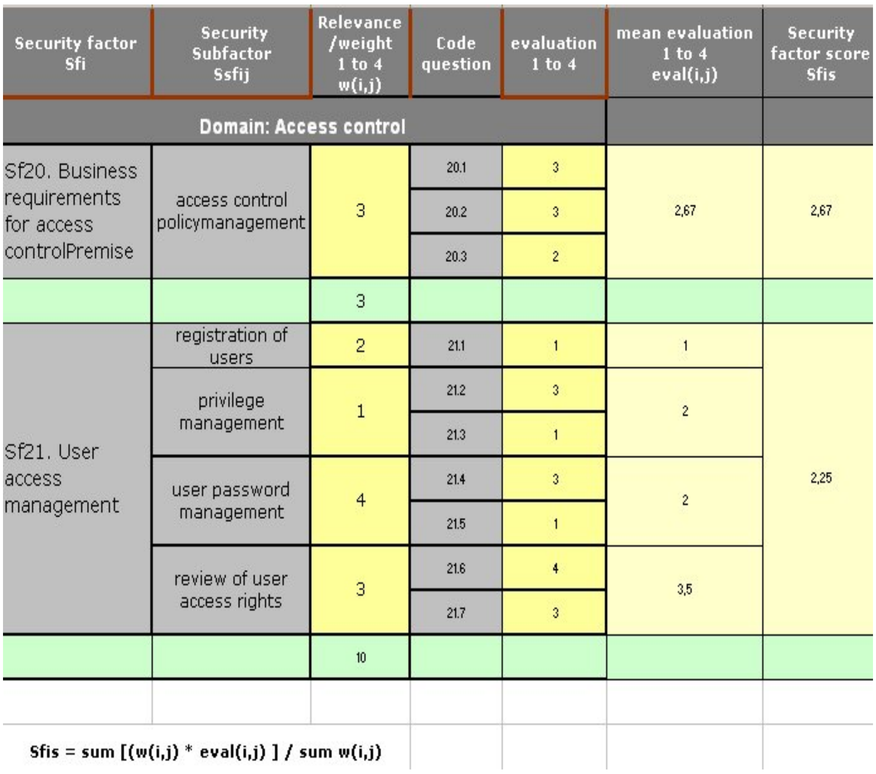
The company determines which systems or processes are critical for them and connected with it, which security factors are important or relevant. An importance rate is given to the security factors from A (low importance) to E (high importance) (see figure 1).



Security Factor Sfi	Importance	Sub Factor	Relevance/weight 1 to 4	Code question	Question	evaluation 1 to 4
Domain: Access control						
Sf20. Business requirements for access controlPremise	B	access control policymanagement	3	20.1	Is the access control policymanagement based on the business security requirements?	3
				20.2	Are aspects of logical and physical access control included?	3
				20.3	Is it clear for users and service providers which rules are applicable?	2
Sf21. User access management	C	registration of users	2	21.1	Is there any formal user registration and de-registration procedure for granting access to multi-user IS and services?	1
		privilege management	1	21.2	are privileges and allocated on need-to-use basis?	3
				21.3	are privileges only allocated after formal authorisation process?	1
		user password management	4	21.4	should the allocation and the reallocation of passwords be controlled through a formal management process?	3
				21.5	are the users asked to sign a statement to keep the password confidential?	1
		review of user access rights	3	21.6	does there exist a process to review user access rights at regular intervals?	4
					Does there exist a procedure to block the	

Figure 1: Questions audit checklist

In BEVA, we express the state of security into scores of the security factor (Sfi's). We do this for all the factors and in the end we give a general security score (Ss) over all security factors. We based our security analysis partly on the Marion-AP method.



Security factor Sfi	Security Subfactor Ssfij	Relevance /weight 1 to 4 w(i,j)	Code question	evaluation 1 to 4	mean evaluation 1 to 4 eval(i,j)	Security factor score Sfis
Domain: Access control						
Sf20. Business requirements for access controlPremise	access control policymanagement	3	20.1	3	2,67	2,67
			20.2	3		
			20.3	2		
		3				
Sf21. User access management	registration of users	2	21.1	1	1	2,25
	privilege management	1	21.2	3	2	
			21.3	1		
	user password management	4	21.4	3	2	
			21.5	1		
	review of user access rights	3	21.6	4	3,5	
			21.7	3		
		10				

Sfis = sum [(w(i,j) * eval(i,j)] / sum w(i,j)

Figure 2: Calculation of the Sf i's

To evolve to a security factor score, the key persons is asked to allocate a weight from 0 to 4 to the subcriteria of the security factors to indicate the relevance. Subsequently the evaluation starts and the list of questions is asked. Each question is given a score between 1 and 4. (see figure 2). The management team evaluates the company for all aspects on a one to four scale and at the same time measures the importance or relevance of all subfactors.

When the questionnaire is completed, BEVA now calculates the security factor scores (Sf) being:

Sfi s = sum [eval (i,j) * w(i,j)] / sum w(i,k)

If all the factor scores are calculated also a general security score Ss is given:

Ss= sum [eval (1,38) * w(1,38)] / sum w(1, 38)

For example see factor 21 in the example: Sf21:[2*1 + 1*2 + 4*2 + 3*3,5]/10 = 2.25

Ss= in this example 2.66

Based on the evaluated questionnaire and the allocated weights, a realistic picture of the security situation of the company can be created as well general as by factor. The system BEVA creates a graphical output of the correlation diagram between these two variables measured for all aspects. Figure 3 shows the scores of all the security factors.

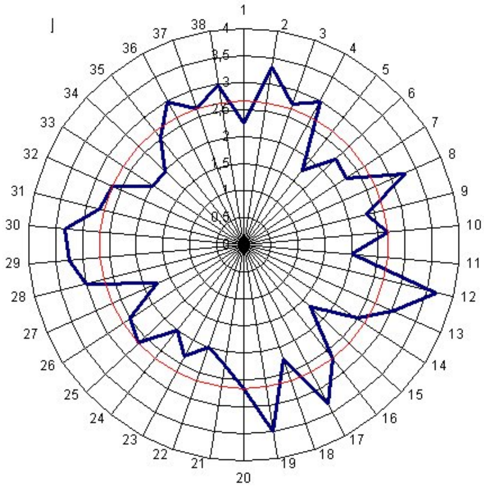


Figure 3: Graph of the security scores

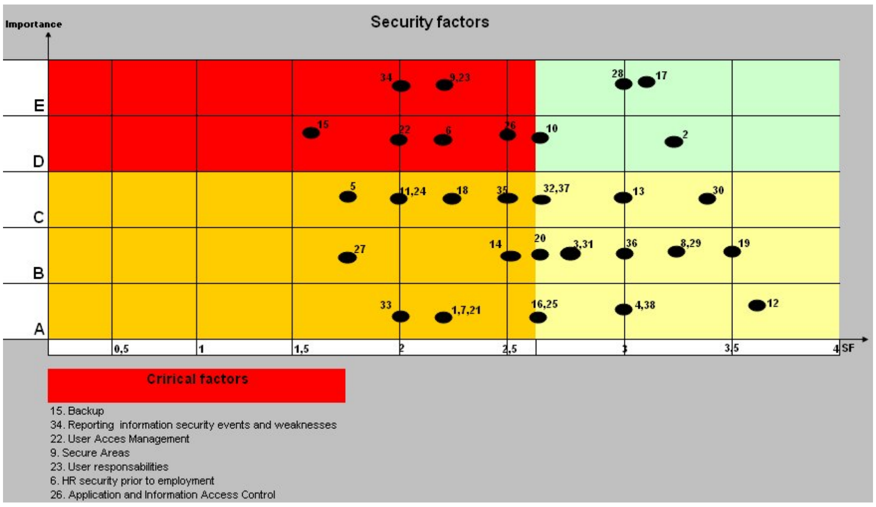
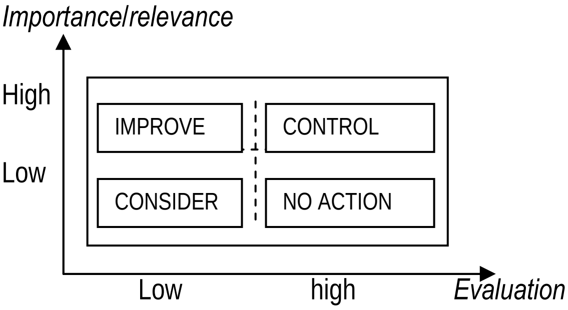


Figure 4: Graph of security factors and their importance

The red line states Ss the general security score. The blue line connects the individual scores of the security factors. Security factors 1, 5, 6, 7, 9, 11, 14, 15, 18, 21, 22, 24, 26, 27, 33 and 34 score beneath the general security score.

Figure 4 combines the scores of the security factor with its importance. For example factor 33 scores low namely 2 but has importance A, low importance. Factor 34 scores also 2 but had importance E, high importance. These differences are well stressed in this graphic. As you can see the ***red*** area highlights the security factors that score low and have a high importance. The factors lying in this area are critical and need immediate attention.

The ***green*** area is important and good secured. It is important to continue these actions and follow up these factors well. The *yellow* zone scores good but isn't that important, no action needs to be taken here. The less important factors that don't score well are situated in the *orange* zone. These factors need to be considered but probably with a small piece of the budget.



Now a clear view of the security situation is obtained. Feedback is given to the company and the evaluation states immediate points of action.

3. The occurrence of threats

The yearly organised CSI/FBI-study delivers the following probabilities for the threats (see fig. 5).

Our final goal is to influence the occurrence of the threats, or the probability of the occurrence of them, by implementing selective security measures in the company. This will impact in the long run the security situation.

We must concentrate on the critical security factors, following the results of the audit. If the security factor is critical, than the threats linked with it have a critical risk too.

In figure 6 we figured out the relations between the threats and the security factors

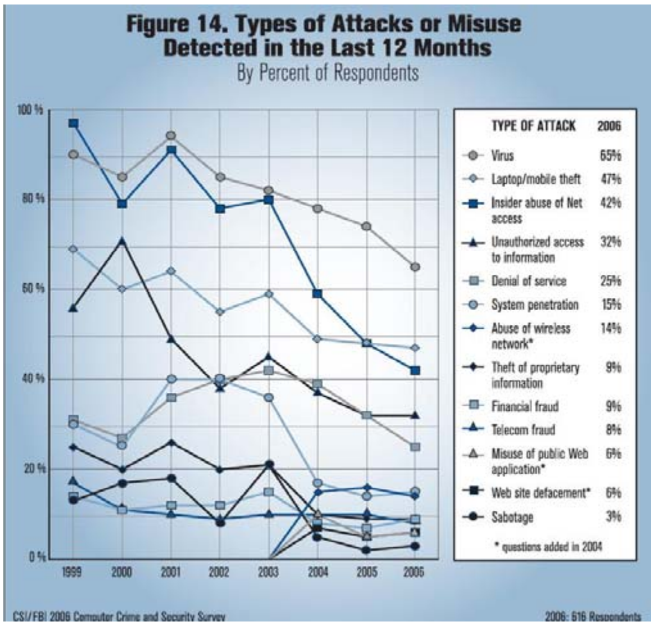


Figure 5: Threats and their occurance

Threat	Virus	Laptop/Mobile theft	Insider abuse of net access	Unauthorized access to information	Denial of Service - aanval	System penetration	Abuse of wireless network	Theft of proprietary information	Financial fraud	Telecom fraud	Misuse of public web application	Website defacement	Sabotage	Illegal software applications on the system (bots, Trojan horses,...)	Phishing	Misuse of the chat	Password sniffing	Exploiting the DNS server of the organization
1.1 Information security aspects of continuity mgt					x								x					
2.1 Business requirements for access control				x		x	x	x				x					x	
2.2 User access management				x		x	x	x	x			x					x	
2.3 User responsibilities				x		x											x	
2.4 Network access control			x				x		x							x		
2.5 OS access control													x					
2.6. Application en information access control											x					x		
2.7 Mobile computing and telenetworking		x					x			x								
3.1 Security requirements of IS				x		x												
3.2 Correct processing in applications				x		x												
3.3 Crypto-graphic controls			x	x		x	x	x										
3.4 Security of system files				x		x												
3.5 Security in development and support processes				x									x	x				
3.6 Technical vulnerability management				x		x							x					
4.1 Secure areas		x						x					x					
4.2 Equipment security		x						x					x					
5.1 Compliance with legal requirements									x									
5.2 Compliance with security policies and standards				x		x												
5.3 Information Systems audit considerations			x															
6.1 Prior to employment									x	x						x		

6.2 During employment			x				x			x	x					x		
6.3 Termination of change of employment		x	x	x		x	x	x	x	x		x						
7.1 Information security policy		x	x	x							x		x			x		
7.2 Internal organization			x															
7.3 External parties				x		x		x	x	x		x	x	x			x	
8.1 Operational Procedures and Operations mgt				x		x		x	x	x					x		x	
8.2 Third party service delivery management				x				x	x	x								
8.3 System planning and acceptance																		
8.4 Protection against malicious and mobile code	x											x		x	x		x	x
8.5 Back-Up management								x										
8.6 Network security management			x	x	x	x	x					x					x	x
8.7 Media Handling								x										
8.8 Exchange of information		x		x				x					x					
8.9 E-commerce					x	x		x	x	x	x				x		x	x
8.10 Monitoring			x	x		x	x		x	x						x		
9.1 Responsibility for assets		x											x					
9.2 Information classification								x					x					
10.1 Information incident management									x	x								

Figure 6: Relation between threats and security factors

4. Security measures and follow up

A next step is to create a list of action points. Taking into account the stated security budget and the factors and their importance, an action plan is suggested. In the CSI study we can find the most used measures. A table is created were the most used measures are related with the threats they prevent.

Measures	Virus	Laptop/Mobile theft	Insider abuse of net access	Unauthorised access to information	Denial of Service - aanval	System penetration	Abuse of wireless network	Theft of proprietary information	Financial fraude	Telecom fraude	Misuse of public web application	Website defacement	Sabotage	Illigal software applications on the system (bots, trojan horses,...)	Phishing	Misuse of the chat	Pasword sniffing	Exploiting the DNS server of the organisation
Firewall				x	x	x					x	x		x				
AntiVirus Software	x													x			x	
AtiSpyware Software														x			x	
Server Based Acces control list				x		x		x										
Intrusion detection system				x		x		x			x	x						
Ecryption for data				x				x									x	
Reusable account system																	x	
Intrusion prevention system				x		x		x			x	x						
Log management software			x						x	x						x		
Application level firewall	x				x									x				
Smart card/ one time password token				x		x		x										
Specialized wireless security							x											
Training personeel		x					x						x					
Endpoint security client software	x													x				
Update server	x			x		x		x				x		x				

Figure 7: Relation between measures and threats

The action plan concerning security will be implemented, taking into account the weakest security factors and of course considering the budget.

After a period of approximately 3 months after implementing the security measures, a new security audit should be taken. The new security score Ss is calculated and compared to the stated aimed Security score using the security measures. If there are security factors that score too low, these should be investigated and adjusted.

Conclusion

The awareness that security is a management problem is everywhere present. It's critical to know what are the critical resources and processes of the company and their weaknesses. Our security audit is a handy solution. We have developed BEVA, a method to critically analyse the company and to uncover the weak spots in the security system. BEVA results in security scores for each security factor and also in a general security score. The goal is to increase the security score Ss to a postulated level by focusing on the critical security factors, those with a low security score. The results of the audit are an ideal start to do risk analysis.

Bibliography

[Shannon, 1949] C.E.Shannon. The Mathematical Theory of Communication. In: The Mathematical Theory of Communication. Ed. C.E.Shannon and W.Weaver. University of Illinois Press, Urbana, 1949.

[Jean-Marc Lamère] la sécurité informatique; Dunod : La méthode MARION (Méthodologie d'Analyse de Risques Informatiques Orientée par Niveaux) www.eisti.fr/~bg/COURSITACT/TXT/m_marion.txt

[Val Thiagarajan B.E, 2005] Information Security Management; BS ISO/ IEC 17799:2005; SANS Audit Check List: author:., M.Comp, CCSE, MCSE, SFS, ITS 2319, IT Security Specialist.

Security Management: A New Model to Align Security with Business Needs; Sumner Blount, CA Security Solutions; August 2006

[Schreurs J, Moreau R.] ICT security management- ECEC 2007 (www.riskworld.net/7799-2.htm)

[Lawrence A. Gordon, Martin P. Loeb, William Lucyshyn and Robert Richardson] 2006 CSI/FBI-study about cybercrime: COMPUTER CRIME AND SECURITY SURVEY

https://event.on24.com/eventRegistration/EventLobbyServlet?target=registration.jsp&eventid=27372&sessionid=1&key=42F39B89EE0B30BA951711A5E7A98EDD&sourcepage=register

http://mediaproducts.gartner.com/gc/webletter/computerassociates/vol3issue3_risk/index.html

Authors' Information

Jeanne Schreurs – prof. Business informatics, Universiteit Hasselt; gebouw D, Agoralaan, 3590 Diepenbeek, Belgium; e-mail: jeanne.schreurs@uhasselt.be

Rachel Moreau - Universiteit Hasselt; gebouw D, Agoralaan, 3590 Diepenbeek, Belgium; e-mail: Rachel.moreau@uhasselt.be

COMPLEX PROTECTION SYSTEM OF METADATA-BASED DISTRIBUTED INFORMATION SYSTEMS

Denis Kourilov, Lyudmila Lyadova

Abstract: A description of architecture and approaches to the implementation of a protection system of metadata-based adaptable information systems is suggested. Various protection means are examined. The system described is a multilevel complex based on a multiagent system combining IDS functional abilities with structure and logics protection means.

Keywords: adaptable information systems, protection mechanisms, metadata, multiagent systems.

ACM Classification Keywords: D.2 Software Engineering: D.2.0 General – Protection mechanisms; K.6 Management of Computing and Information Systems: K.6.5 Security and Protection – Authentication, Insurance, Invasive software (e.g., viruses, worms, Trojan horses), Unauthorized access (e.g., hacking, phreaking); I.2 Artificial Intelligence: I.2.11 Distributed Artificial Intelligence – Multiagent systems.