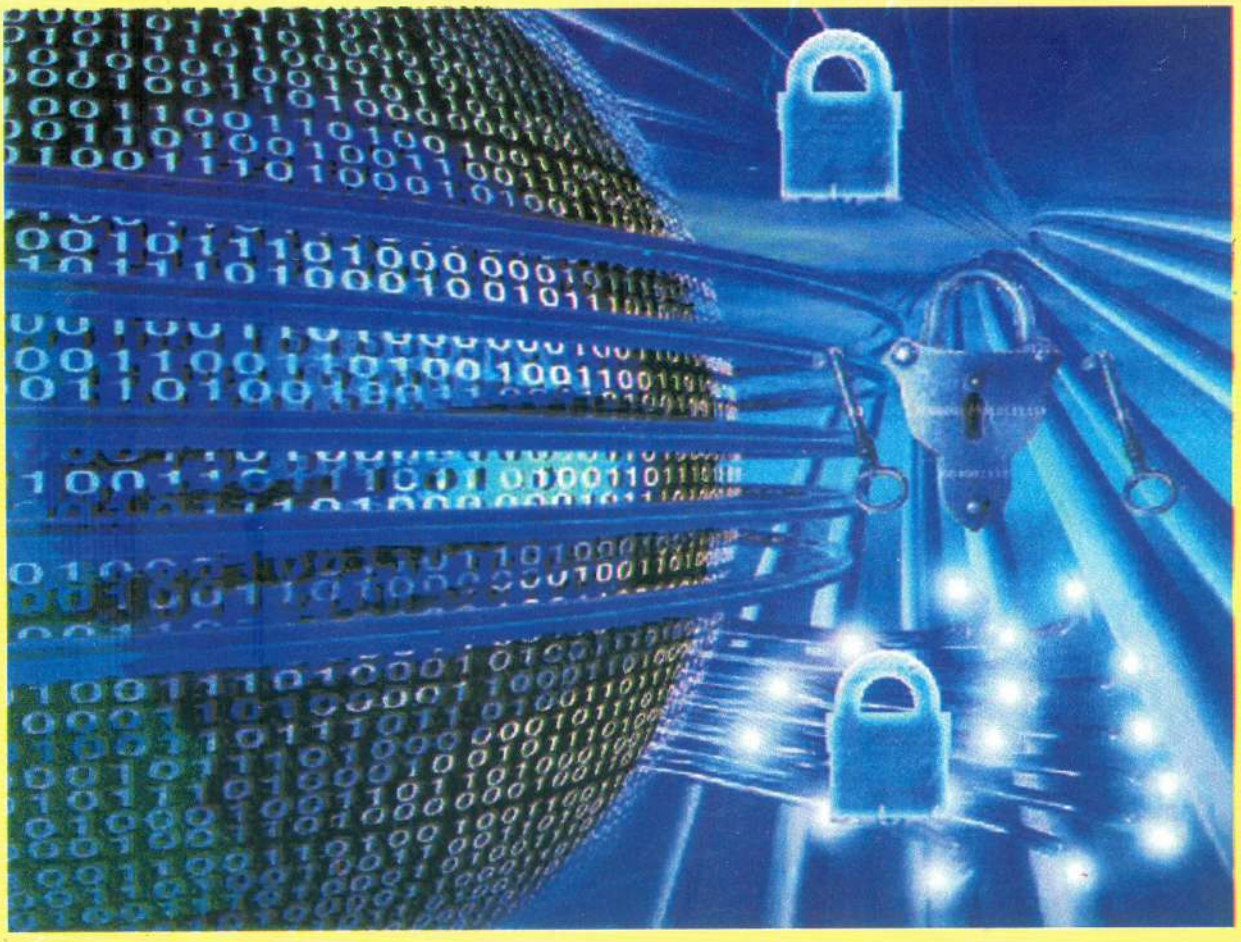
ignou
THE PEOPLE'S
UNIVERSITY

Indira Gandhi National Open University
School of Vocational Education and Training

MSE-024
Policy, Standards and Laws



SECURITY STANDARDS

1

"शिक्षा मानव को बन्धनों से मुक्त करती है और आज के युग में तो यह लोकतंत्रा की भावना का आधार भी है। जन्म तथा अन्य कारणों से उत्पन्न जाति एवं वर्गगत विषमताओं को दूर करते हुए मनुष्य को इन सबसे ऊपर उठाती है।"

- इन्दिरा गांधी

"Education is a liberating force, and in our age it is also a democratising force, cutting across the barriers of caste and class, smoothing out inequalities imposed by birth and other circumstances."

- Indira Gandhi

ignou
THE PEOPLE'S
UNIVERSITY
Indira Gandhi National Open University
School of Vocational Education and Training

Block

1

SECURITY STANDARDS

Programme Expert/ Design Committee of Post Graduate Diploma in Information Security (PGDIS)

Prof. K.R. Srivathsan
Pro Vice-Chancellor, IGNOU

Mr. B.J. Srinath, Sr. Director & Scientist 'G',CERT-In, Department of Information Technology, Ministry of Communication and Information Technology Govt of India

Mr. A.S.A Krishnan, Director, Department of Information Technology, Cyber-Laws and E-Security Group, Ministry of Communication and Information Technology, Govt of India

Mr. S. Balasubramony, Dy. Superintendent of Police, CBI, Cyber Crime Investigation Cell Delhi

Mr. B.V.C. Rao, Technical Director National Informatics Centre, Ministry of Communication and Information Technology

Prof. M.N. Doja, Professor, Department of Computer Engineering, Jamia Milia Islamia New Delhi

Dr. D.K. Lobiyal, Associate Professor School of Computer and Systems Sciences, JNU New Delhi

Mr. Omveer Singh, Scientist, CERT-In Department of Information Technology Cyber-Laws and E-Security Group Ministry of Communication and Information Technology Govt of India

Dr. Vivek Mudgil, Director, Eninov Systems Noida

Mr. V.V.Subrahmanyam, Assistant Professor School of Computer and Information Science IGNOU

Mr. Anup Girdhar, CEO, Sedulity Solutions & Technologies, New Delhi

Prof. A.K. Saini, Professor, University School of Management Studies, Guru Gobind Singh Indraprastha University, Delhi

Mr. C.S. Rao, Technical Director in Cyber Security Division, National Informatics Centre, Ministry of Communication and Information Technology

Prof. C.G. Naidu, Director, School of Vocational Education & Training, IGNOU

Prof. Manohar Lal, Director, School of Computer and Information Science, IGNOU

Prof. K. Subramanian, Director, ACIIL IGNOU Former Deputy Director General National Informatics Centre, Ministry of Communication and Information Technology Govt of India

Prof. K. Elumalai, Director, School of Law IGNOU

Dr. A. Murali M Rao, Joint Director Computer Division, IGNOU

Mr. P.V. Suresh, Sr. Assistant Professor School of Computer and Information Science IGNOU

Ms. Mansi Sharma, Assistant Professor School of Law, IGNOU

Ms. Urshla Kant
Assistant Professor, School of Vocational Education & Training, IGNOU
Programme Coordinator

Block Preparation

Unit Writers

Mr. Vikas Rao Vadi
HOD (Computer Science), Kalka Institute for Research and Advanced Studies (Affiliated to Guru Gobind Singh Indraprastha University), Alaknanda, New Delhi (Unit 1)

Ms. Shalini Chawla
M.Tech (Computer Science), Assistant Professor, Northern India Engineering College (NIEC), (Affiliated to Guru Gobind Singh Indraprastha University), Delhi (Unit 2)

Mr. Arun Bakshi
Sr. Assistant Professor (Information Technology)
Gitarattan International Business School (giBS)
Madhuban Chowk, Delhi (Unit 3)

Mr. Rohit Verma
Assistant Professor, Apeejay Institute of Management
Jalandhar (Unit 4)

Block Editor

Adv. Vaishali Kant
B.A.LL.B, LLM
National Law School of India University Bangalore

Ms. Urshla Kant
Assistant Professor, School of Vocational Education & Training, IGNOU

Proof Reading

Ms. Urshla Kant
Assistant Professor, School of Vocational Education & Training, IGNOU

PRODUCTION

Mr. B. Natrajan	Mr. Jitender Sethi	Mr. Hemant Parida
Dy. Registrar (Pub.)	Asstt. Registrar (Pub.)	Proof Reader
MPDD, IGNOU	MPDD, IGNOU	MPDD, IGNOU

August 2011

ISBN : 978-81-266-7522-3

Further information on the Indira Gandhi National Open University courses may be obtained from the University's office at Maidan Garhi, New Delhi-110 068 or the website of IGNOU www.ignou.ac.in

Printed and Published on behalf of the Indira Gandhi National Open University, New Delhi, by the Registrar, MPDD.

Printed At :- Print Pack (India),215/21,Ambadker Gali Moujpur Delhi - 53 .

COURSE INTRODUCTION

This course talks about the policy, standards and law relating to information security. Cyber law is now emerging which refers to a code of safe and responsible behaviour for the internet community. Accordingly practicing good cyber policy, standards and law involve:-

1. Understanding the risk of harmful and illegal behaviour online.
2. Learning how to protect ourselves and other internet users from such behaviour
3. Teaching young people who may not realize the potential for harm to themselves and others
4. How to use the internet safely and responsibly.

However internet should not merely be perceived as a new media, comparable to mass media but most rather be seen as a new communicative sphere encompassing both system and the world and there is a need for positive state obligations in order to protect individual's right to express themselves and to seek information free from interference by third parties.

This course elaborates about the security protocols. There are a variety of security protocols from which programmers can choose. Each has its own particular advantages and disadvantages. A protocol is an agreed upon format for transmitting data between two devices. The protocol determines the following:

1. What type of error checking is to be used?
2. What data compression technique, if any, to be used?
3. How the sending device will indicate that it has finished sending a message?
4. How the receiving device will indicate that it has received a message?

This course elaborates in detail the various types of cyber crimes. This cyber crime is the collective encompassing both cyber offences and cyber contraventions. The word cyber is synonymous with computer, computer system or computer network. Thus, cyber crime may be defined as any illegal act that involves a computer, computer system or computer network.

This course explains the relevance of cyber laws in place. It emphasizes on the updating of the laws with the rapid change in technology. Today, we need highly effective laws for the providing information security. The IT Act has undergone numerous changes in the year 2008. But still it requires more amendments and changes which can run parallel with the technology. Lets hope for the comprehensive and effective cyber laws to be in force.

This course includes the following blocks:

Block 1 – Security Standards
Block 2 – ISO Standards
Block 3 – Cyber Laws
Block 4 – Cyber Crimes and Regulation

BLOCK INTRODUCTION

Whether a business manufactures goods or provides services, when it meets standards relevant to its industry, it ensures that positive characteristics such as quality, durability, efficiency, safety and environmental friendliness are reinforced. Cyber Security standards are security standards which enable organizations to practice safe security techniques to minimize the number of successful cyber security attacks. These guides provide general outlines as well as specific techniques for implementing cyber security. For certain specific standards, cyber security certification by an accredited body can be obtained. There are many advantages to obtaining certification including the ability to get cyber security insurance. This block comprises of four units and is designed in the following way;

The **Unit One** introduces security policies and standards. Policy is both the starting point and the touchstone for information security in any company. Policy provides evidence of the company's stance on security and provides a living tool for every employee to help build and maintain that level of security. It is therefore essential that security policy is accurate, comprehensive, and useable.

The **Unit two** is an attempt to explain how you should support the information security awareness activities that are essential for compliance with ISO27k and particularly for certification against ISO/IEC 27001.

Unit three is all about the security mechanism standards. After studying this unit students will be able to understand security concerns. The techniques like encryption, cryptography and their role to provide security to the data and information are also covered. The role of algorithm is very important in security concern. The digital signature are very important in the security measurements in business world, thus are covered very well.

Unit four explains, about the security protocol standards. It covers entity authentication protocol, key establishment and time stamping technique. The entity authentication protocols are responsible for identifying the correct entity to whom and by whom the information is sent or received. At the same time with the help of these protocols a sender could not deny later, that the information was not send by him which was actually send by him. Using the concept of time stamping an eye can be kept at the time of development of a document.

Hope you benefit from this block.

ACKNOWLEDGEMENT

The material we have used is purely for educational purposes. Every effort has been made to trace the copyright holders of material reproduced in this book. Should any infringement have occurred, the publishers and editors apologize and will be pleased to make the necessary corrections in future editions of this book.

UNIT 1 INTRODUCTION TO SECURITY POLICIES AND STANDARDS

Structure

1.0 INTRODUCTION

Security policy is a definition of what it means to be secure for a system, organization or other entity. For an organization, it addresses the constraints on behavior of its members as well as constraints imposed on adversaries by mechanisms such as doors, locks, keys and walls. For systems, the security policy addresses constraints on functions and flow among them, constraints on access by external systems and adversaries including programs and access to data by people.

In business, a security policy is a document that states in writing how a company plans to protect the company's physical and information technology (IT) assets. A security policy is often considered to be a "living document", meaning that the document is never finished, but is continuously updated as technology and employee requirements change. A company's security policy may include an acceptable use policy, a description of how the company plans to educate its employees about protecting the company's assets, an explanation of how security measurements will be carried out and enforced, and a procedure for evaluating the effectiveness of the security policy to ensure that necessary corrections will be made.

Security policy can be:

1. Information security
2. Computer security policy
3. Information protection policy
4. User account policy

1.1 OBJECTIVES

After studying this unit, you should be able to learn about:

- need of security;
- Policy types;
- Policy Development Process;
- Policy Development Team;

- Policy Development Lifecycle;
- Policy Document Outline;
- Cyber security standards; and
- IT Security policy standard : ISO 27001.

1.2 SIGNIFINANCE OF SECURITY POLICY

If it is important to be secure, then it is important to be sure all of the security policy is enforced by mechanisms that are strong enough. There are organized methodologies and risk assessment strategies to assure completeness of security policies and assure that they are completely enforced. In complex systems, such as information systems, policies can be decomposed into sub-policies to facilitate the allocation of security mechanisms to enforce sub-policies. However, this practice has pitfalls. It is too easy to simply go directly to the sub-policies, which are essentially the rules of operation and dispense with the top level policy. That gives the false sense that the rules of operation address some overall definition of security when they do not. Because it is so difficult to think clearly with completeness about security, rules of operation stated as "sub-policies" with no "super-policy" usually turn out to be rambling ad-hoc rules that fail to enforce anything with completeness. Consequently, a top level security policy is essential to any serious security scheme and sub-policies and rules of operation are meaningless without it.

Information Security

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

The terms information security, computer security and information assurance are frequently incorrectly used interchangeably. These fields are interrelated often and share the common goals of protecting the confidentiality, integrity and availability of information; however, there are some subtle differences between them.

These differences lie primarily in the approach to the subject, the methodologies used, and the areas of concentration. Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms.

Computer security can focus on ensuring the availability and correct operation of a computer system without concern for the information stored or processed by the computer.

Governments, military, corporations, financial institutions, hospitals, and private businesses amass a great deal of confidential information about their employees, customers, products, research, and financial status. Most of this information is now collected, processed and stored on electronic computers and transmitted across networks to other computers.

Should confidential information about a business' customers or finances or new product line fall into the hands of a competitor, such a breach of security could lead to lost business, law suits or even bankruptcy of the business. Protecting confidential information is a business requirement, and in many cases also an ethical and legal requirement.

For the individual, information security has a significant effect on privacy, which is viewed very differently in different cultures.

The field of information security has grown and evolved significantly in recent years. There are many ways of gaining entry into the field as a career. It offers many areas for specialization including: securing network(s) and allied infrastructure, securing applications and databases, security testing, information systems auditing, business continuity planning and digital forensics science, etc.

Computer Security Policy

A computer security policy defines the goals and elements of an organization's computer systems. The definition can be highly formal or informal. Security policies are enforced by organizational policies or security mechanisms. A technical implementation defines whether a computer system is secure or insecure. These formal policy models can be categorized into the core security principles of: Confidentiality, Integrity and Availability. For example the Bell-La Padula model is a confidentiality policy model, whereas Biba model is an integrity policy model.

Information Protection Policy

Information protection policy is a document which provides guidelines to users on the processing, storage and transmission of sensitive information. Main goal is to ensure information is appropriately protected from modification or disclosure. It may be appropriate to have new employees sign policy as part of their initial orientation. It should define sensitivity levels of information.

User Account Policy

User Account Policy is a document which outlines the requirements for requesting and maintaining an account on computer systems or networks, typically within an organization. It is very important for large sites where users typically have accounts on many systems. Some sites have users read and sign an Account Policy as part of the account request process

1.3 NEED OF SECURITY POLICY

1.3.1 Basic Purpose of Policy

A security policy should fulfill many purposes. It should:

1. Protect people and information
2. Set the rules for expected behavior by users, system administrators, management, and security personnel
3. Authorize security personnel to monitor, probe, and investigate
4. Define and authorize the consequences of violation
5. Define the company consensus baseline stance on security
6. Help minimize risk
7. Help track compliance with regulations and legislation

Information security policies provide a framework for best practice that can be followed by all employees. They help to ensure risk is minimized and that any security incidents are effectively responded to. Information security policies will also help turn staff into participants in the company's efforts to secure its information assets, and the process of developing these policies will help to define a company's information assets. Information security policy defines the organization's attitude to information, and announces internally and externally that information is an asset, the property of the organization, and is to be protected from unauthorized access, modification, disclosure, and destruction.

1.3.2 Policy and Legislative Compliance

In addition to the purposes described above, security policies can be useful in Ways that go beyond the immediate protection of assets and policing of Behavior. They can be useful compliance tools, showing what the company's stance is on best practice issues and that they have controls in place to comply with current and forthcoming legislation and regulations. In today's corporate world it is essential for companies to be able to show compliance with current legislation and to be prepared for forthcoming legislation. Recent laws such as HIPAA (Health Insurance Accountability and Portability Act), GLB (Gramm-Leach-Bliley Act) and Sarbanes Oxley have had major implications for policy makers in the U.S. and farther a field. Policy can be used to help companies ensure they have the controls in place to work towards compliance by mapping policy statements to legislative requirements. In this way they can provide evidence that their baseline security controls are in line with regulations and legislation. This type of stance will also give companies an indication based on legal requirements of what they need to protect and to what extent. This will

help to ensure that they target security controls only where they are needed, a benefit from both a financial and personnel resourcing perspective.

1.3.3 Policies as Catalysts for Change

It is also possible to use policies to drive forward new company initiatives, with policy acting as the catalyst for future projects which move towards better security and general practices. For example, a policy stating that a certain type of encryption is required for sensitive information sent by E-mail may (with prior consultation with the appropriate technical experts) help to promote the need to develop such a capacity in the future. The presence of this requirement in policy has made sure the impetus to develop the E-mail encryption project has remained strong. In short, security policy should be a useful tool for protecting the security of the Enterprise, something that all users can turn to in their day-to-day work, as a guide and information source. All too often however, security policies can end up simply as "shelfware" , little read, used, or even known of by users and disconnected from the rest of company policy and security practice.

1.3.4 Policies Must be Workable

The key to ensuring that your company's security policy is useful and useable is to develop a suite of policy documents that match your audience and marry with existing company policies. Policies must be useable, workable and realistic. In order to achieve this it is essential to involve and get buy-in from major players in policy development and support (such as senior management, audit and legal) as well as from those people who will have to use the policies as part of the daily work (such as subject matter experts, system administrators and end users).

In order to achieve this, one important element is to communicate the importance and usefulness of policies to those who have to live by them. Often users seem to think that policy is something that is going to stand in the way of their daily work. An important element of policy development, and to ensure policies are put into practice and not rejected by the users, is to convey the message that policies are useful to users: to provide a framework within which they can work, a reference for best practice and to ensure users comply with legal requirements. Once users realise that policy is something that may actually help them as they do about their work, they are much more likely to be receptive to both helping you develop it and living up to it to ensure compliance. Similarly, once senior management realise that policy is a tool they can leverage to help ensure adherence to legislative requirements and to move forward much needed new initiatives, they are much more likely to be supportive of policy in terms of financial and resourcing support as well as becoming policy champions themselves.

1.4 USER OF POLICIES

1.4.1 Audience Groups

Your audience is of course all your company employees, but this group can be divided into audience sub-categories, with the members of each sub-category likely to look for different things from information security policy. The main audiences groups are:

1. Management – all levels
2. Technical Staff – systems administrators, etc
3. End Users

All users will fall into at least one category (end-user) and some will fall into two or even all three.

1.4.2 Audience and Policy Content

The audience for the policy will determine what is included in each policy document. For example, you may not always want to include a description of why something is necessary in a policy - if your reader is a technical custodian and responsible for configuring the system this may not be necessary because they are likely to already know why that particular action needs to be carried out. Similarly, a manager is unlikely to be concerned with the technicalities of why something is done, but they may want the high-level overview or the governing principle behind the action. However, if your reader is an end-user, it may be helpful to incorporate a description of why a particular security control is necessary because this will not only aid their understanding, but will also make them more likely to comply with the policy. Allow for the fact that your readers will want to use the policies in a number of ways, possibly even in more than one way at one time. For example, when first reading a policy document, an end-user may be interested in reading the entire document to learn about everything that they need to do to help protect the security of the company. On another later occasion however, the user may reference the document to check the exact wording of a single policy statement on a particular topic. Given the variety of issues, readers, and uses for policy, how can we hope to address them in one document? The answer is that we can't. Companies must ensure that their information security policy documents are coherent with audience needs and to do this it is often necessary to use a number of different document types within a policy framework. Which type of document you use will be determined in large part by the audience for that document. For example, an overall Acceptable Use Policy will be in the form of a higher level document, while a document that describes how to configure the instant messaging system to ensure it complies with the Acceptable Use Policy may be in the form of a job aid or guidelines document. Manager and

end users are likely to be interested the former, while administrative staff is more likely to use the latter.

1.5 POLICY TYPES

1.5.1 Policy Hierarchy Overview

The diagram below outlines a hierarchical policy structure that enables all policy audiences to be addressed efficiently. This is a template for a policy hierarchy and can be customized to suit the requirements of any company:

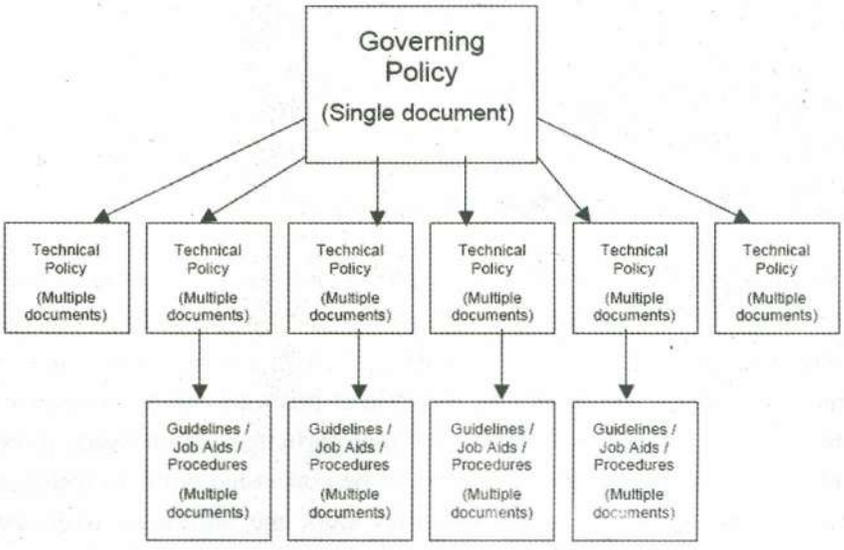


Fig. 1

The diagram above shows a hierarchy for a fairly mature, developed process, probably aligned to that possible in a large company where policy development has been underway for several years. For smaller companies or for those just starting to develop policy, it is possible to use this basic framework, but to initially have a smaller number of Technical Policies and possibly no guidelines or job aids early in the process. Rather than trying to develop a large hierarchy all at once, it is more realistic to develop a Governing Policy and a small number of Technical Policies initially, then increase the number of policies and supporting documents, as well as the complexity of the policies as you move forward. As we have seen, in large companies there will be several audiences for your policy, and you will want to cover many different topics on different levels. For this reason, a suite of policy documents rather than a single policy document works better in a large corporate environment.

The proposed scheme provides for all levels of audience and for all topics by using two policy types supported by procedural documents:

1. Governing Policy

2. Technical Policy
3. Job Aids / Guidelines

1.5.2 Governing Policy

Governing Policy should cover information security concepts at a high level, define these concepts, describe why they are important, and detail what your company's stand is on them. Governing Policy will be read by managers and end users. By default it will also be read by technical custodians (particularly security technical custodians) because they are also end users. All these groups will use the policy to gain a sense of the company's overall security policy philosophy. This can be used to inform their information security-related interaction with business units throughout the company.

Governing Policy should be closely aligned with existing and future HR (Human Resources) and other company policies, particularly any which mention security- related issues such as E-mail or computer use, etc. The Governing Policy document will be on the same level as these company-wide policies. Governing Policy is supported by the Technical Policies which cover topics in more detail and add to these topics be dealing with them for every relevant technology. Covering some topics at the Governing Policy level may help obviate the need for a detailed technical policy on these issues. For example, stating the company's governing password policy means that details of specific password controls can be covered for each operating system or application in the relevant technical policy, rather than requiring a technical policy on password controls for all systems. This may not be the case for a smaller company, where fewer systems/applications are used and where a single technical password policy would therefore be sufficient. For a larger company however, the former method provides a more efficient process for users to follow because they will have to reference fewer documents – simplifying this process raises the odds that users will comply with the policy, thereby improving security. In terms of detail level, governing policy should address the "what" in terms of security policy.

1.5.3 Technical Policies

Technical Policies will be used by technical custodians as they carry out their security responsibilities for the system they work with. They will be more detailed than Governing Policy and will be system or issue specific, e.g., an AS-400 Technical Policy or a Technical Physical Security Policy. Technical Policies will cover many of the same topics as Governing Policy, as well as some additional topics specific to the overall technical topic. They are the handbook for how an operating system or a network device should be secured. They describe what must be done, but not how to do it - this is reserved for procedural documents which are the next detail level down from Governing and Technical Policy. In terms of detail level, Technical Policy should address

the "what" (in more detail), "who", "when" and "where" in terms of security policy.

1.5.4 Job Aids / Guidelines

Procedural documents give step-by-step directions on the 'how' of carrying out the policy statements. For example, a guide to hardening a Windows server may be one or several supporting documents to a Technical Windows Policy. Procedures and guidelines are an adjunct to policy, and they should be written at the next level of granularity, describing how something should be done. They provide systematic practical information about how to implement the requirements set out in policy documents. These may be written by a variety of groups throughout the company and may or may not be referenced in the relevant policy, depending on requirements. Procedural documents may be written where necessary in addition to and in support of the other types of policy documents, to aid readers in understanding what is meant in policy through extended explanations. Not all policies will require supporting documents. Beware however, if you find yourself getting requests for job aids for every policy document you write, your original documents may be too complex or hard to understand. Save you and your readers time by ensuring everything you write is clear, concise, and understandable in the first place.

The development of these supporting documents need not necessarily be undertaken by the policy development team who develop the Governing and Technical policies. It may be more efficient to have the individual business unit develop their own supporting documents as needed, both because of the availability of resources on the policy development team and because the technical staff in the business units is likely to have the most complete and up-to-date technical knowledge in the company, better enabling them to write such documents. The policy gives them the framework to follow (the "what", "who", "when", and "where" in terms of security policy) and they simply need to follow these controls and sketch out the "how". Job aids and guidelines will also act as a backup facility if a staff member leaves, ensuring their knowledge isn't lost and that policy requirements can still be carried out.

Check Your Progress 1

Note: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

1) What is IT security?

.....

.....

.....

.....

2) What are policy types?

.....

.....

.....

.....

1.6 POLICY DEVELOPMENT PROCESS

1.6.1 Development Approach

1.6.1.1 Development Process Maturity

The major consideration behind any company's policy development process will be the level of process maturity. It is important that companies (especially larger ones) don't aim too high initially and try to develop a comprehensive and complex policy program straight away. This isn't likely to be successful for a number of reasons including lack of management buy-in, unprepared company culture and resources and other requirements not in place. In this situation it is advisable to start off small, perhaps developing checklist–style policies initially and only a skeleton policy framework with essential policies developed first. As the process grows in maturity, companies will be able to develop the full range of policies with more detail included in each as well as accompanying procedural documentation as needed. Education, awareness and communication processes will also grow in maturity to cope with promoting an ever-growing range of policies. This should coincide with the growing corporate strength of the policies themselves. The corporate culture will start to appreciate that the policies must be followed and may actually start to use them to push through much needed changes throughout the company.

1.6.1.2 Top-Down versus Bottom-Up

There are many starting points for developing policy. New or forthcoming legislation can often be a powerful impetus to develop policy, as can recent security incidents or enthusiastic administrators recently returned from the latest training course. All these provide great inputs to policy but the key is to be balanced. Relying solely on the 'top-down' approach of using only legislation, regulations and best practice to write your policy will leave you with unrealistic, artificial policy that won't be workable in the real world. Similarly, relying only on a 'bottom-up' method based only on system administrator knowledge can result in policy that is too specific to a given environment (perhaps just one part of a large company), possibly based too much on local current practice or on the latest training suggestions, making it too unrealistic. The best policy will come from a combination of these approaches, both top-down and bottom-up. In order to achieve this it is

something that must be considered from the outset and must be reflected in the diversity of areas involved in policy development and the types of review policy undergoes. This balanced approach is likely to result in a more mature policy development process. It can work for both small companies (where there is little space between top and bottom) and big companies where the breadth of knowledge is needed to ensure a realistic and workable resulting policy.

1.6.1.3 Current Practice versus Preferred Future

Policy development must also take into account to what extent the policy should reflect current practice versus preferred future. Writing a policy that reflects only precisely what is done today may be out-of-date even by the time it is published, while a policy that includes controls which cannot yet be feasibly implemented may be impossible to comply with for technical reasons and may therefore be ignored as unrealistic and unworkable. It is important that this is discussed at an early stage as if it is not discussed and the policy develops too far towards the unworkable, preferred future model, this may only then show up at the policy gap identification stage, when a lot of time and effort will then have been wasted developing something which is of little value. The best policy strikes a balance between current practice and preferred future and this is what the policy development team should aim for.

1.6.1.4 Consider All Threat Types

Finally when considering what should be included in an initial draft, make sure to consider all the types of threats your company faces. While those from malicious external attackers in the form of viruses and worms attract much media attention and accordingly deserve to be considered when writing policy, other considerations that are at least as important include natural disasters, disgruntled current and former employees and ignorance leading to accidental security exposures. Policies should consist of controls to combat all these threat types.

1.7 POLICY DEVELOPMENT TEAM

It is important to determine who is going to be involved in the actual development phase of policy at an early stage. The group who develops the policy should ideally also be the group who will own and enforce the policy in the long-term; this is likely to be the information security department. The overall composition of the policy development team will vary according to the policy document being developed, but the following is a list of individuals or groups who may be involved.

1.7.1 Primary Involvement

1. Information Security Team – A team or part of a team from this group should be assigned the overall responsibility for developing the policy documents. Overall control may be given to one person with others in a supporting role. This team will guide each policy document through development and revision and should subsequently be available to answer questions and consult on the policy.

2. Technical Writer(s) – Your company or security department may already have a technical writer on staff that can assist in writing security policies. Even if they are not able to take primary responsibility for the information security policy project, an in-house technical writer can be a valuable resource to help with planning your policy project, determining an appropriate style and formatting structure for your documents, and editing and proof-reading your policy drafts.

1.7.2 Secondary Involvement

The following groups may (and in some cases, should) have input during the development of the policy in reviewing and/or approval roles.

- **Technical Personnel** – In addition to staff on the security team, you may need to call upon the expertise of technical staff that have specific security and/or technical knowledge in the area about which you are writing. They will be familiar with the day-to-day use of the technology or system for which you are writing policy and you can work with them to balance what is good security with what is feasible within your company.

- **Legal Counsel** – Your Legal department should review the policy documents once they are complete. They will be able to provide advice on current relevant legislation such as HIPAA and Sarbanes- Oxley, etc that requires certain types of information to be protected in specific ways, as well as on other legal issues. The Legal department should also have input into the policy development process in terms of letting the policy development team know about forthcoming legislative requirements and helping to decipher these for the team.

- **Human Resources** – The Human Resources department may need to review and/or approve your policy depending on how you have determined that your policy will relate to existing company policies. Where your policy touches on topics covered by existing HR policy, e.g., E-mail usage, physical security, you must make sure that both sets of policy say the same thing.

- **Audit and Compliance** – The Internal Audit department in your company are likely to be involved in monitoring company-wide compliance with the policy once it is in force. It is therefore useful if they are involved in the development and review processes for policy to ensure that it is enforceable in terms of their procedures and current best practice. If there are other compliance groups additional to the main internal audit department, these groups should also be consulting as needed.

- **User Groups** – During revision of policy documents, it can be useful to work with users to determine how successful current policy is, and thereby determine how the policy may need to be changed to make it more useable for your target audiences. Issues such as the style, layout, and wording of your policy documents may seem minor issues compared to their content, but remember that if your documents are off-putting or hard to understand; users may not read them fully or may fail to understand them correctly, thereby needlessly risking security compromise.

1.8 POLICY DEVELOPMENT LIFECYCLE

Once you have determined who will be involved in writing the policy, you can begin the policy development process.

1.8.1 Senior Management Buy-in

Developing a suite of policy documents will require a high level of commitment, not just from the primary developer and development team, but also from a number of other information security personnel in the company. In order to make sure that these resources are available to you for the time you need to get the information you need, management buy-in must be sought at the beginning of the policy project. Management must be made aware of both the importance and size of the task ahead so that they will not baulk at resource allocation in the later stages. Senior management also supports the policy development and maintenance process by championing the resulting policies throughout the company and putting their weight behind them so that the policy is seen to have "teeth". Further, they should be prepared to support projects that result from policy to ensure compliance. These two types of support are essential to the ongoing viability of the policy program.

1.8.2 Determine a Compliance Grace Period

At the beginning of your overall policy development project, you should work with the Internal Audit group to determine how soon after policy publication they will audit based on the policy. By allowing a grace period for compliance, you are helping to ensure that the policies will be enforceable. This grace

period will ensure those users who have to live by the policies have enough time to review them and implement any project, processes or internal communications necessary to make sure they are in compliance. Depending on the size of the company, the grace period can be anything from a few months to around one year.

1.8.3 Determine Resource Involvement

At this point you should identify who you will need to talk to in order to determine and agree on the content of the policy. You must give all team members an estimate of how much of their time they can expect to allocate to the project. Policy projects held up because subject-matter experts (SMEs) are busy can mean that the policy risk being out of date before it is finished. If necessary, get buy-in directly from line managers. In most cases, people will see the value of policy and will be happy to help you develop something that will help them in their jobs, but you need to make sure they are on board before going any further.

1.8.4 Review Existing Policy

If your company has any existing security policy, review it to determine if it can be used as part of the new suite of policy documents. Collect all related procedures and guidelines as well as any high level policy documents. These can all be used to get an idea of current company stance on a given issue or technology, or simply to show that a certain technology is secured differently in different areas of the company. This is something that will need to be reflected in the new policy document. Even existing guidelines or job aids can become the starting point for a policy document on the same topic.

1.8.5 Determine Research Materials

As well as talking to SMEs and other experts and drawing on your own knowledge of information security, you may need to do research for some policy topics. This is particularly the case for 'new' technologies such as instant messaging, smartphones, or topics that your company has not previously had an official security policy on. In these cases, you will need to research industry best practices, and there are a number of sources you can use for this - we have listed some below:

- **Internet** – As well as visiting information security websites, (e.g., www.securityfocus.com) use web search engines to find information on security topics. However, stick to reliable sources and be aware that some of the information may not be current.
- **SANS** – The papers in the SANS reading room provide excellent information on security topics which can be used as research material for policy topics.

- **Journals, books, white papers** – Again, by aware of how up to date these sources are. In the fast-moving infosec world, books may soon get out of date; journals may be a better source in these cases.

1.8.6 Interview SMEs

Before the interview itself, there are things you can do to ensure you get the best from your SMEs.

- **Define your objectives** – know as much about the topic as you can, and determine what level of detail and information you require from the SME. The detail you require will depend on what type of policy document you are working. Let your SME(s) know what your objectives are so that they too can be prepared.
- **Prepare for the meeting** – arrange a suitable meeting place or book a conference bridge. Compile a list of questions or an outline of topics you want to cover.
- **Control the interview** – listen actively, ask open-ended questions and control the flow of the interview. Where SMEs disagree or go off on tangents, aim to bring them back to the focus of the discussion without getting into arguments about opinions. Take notes and write everything down. Ask questions if you are not clear on any points.
- **Sum up and confirm** – sum up what you have understood from the interview and what your next steps are. Iterate anything that is expected from the SME before or in time for the next meeting. Thank them for their time.
- **Post-interview review** – organize your materials, and review your notes while they are still fresh in your mind and on paper.

1.8.7 Write Initial Draft

Determining the right pitch or level for the policy can make the difference between a feasible security policy and one that is merely shelfware. Make the policy too rigid and it will be unenforceable, but make it too weak and it will provide insufficient protection. Be aware that there may well be exceptions to some of the policy statements. In these cases, it is acceptable to leave the statements in the policy, but to refer the exceptions to the deviations process. This ensures that the company policy is clearly stated and enforced according to risk assessment and best practices, while at the same time providing a mechanism for dealing with occasional exceptions without weakening the policy. Even if you don't have fully formed policy statements at this point, it is a good idea to get something down on paper before your first review meeting with the rest of the project team. Even a list of topic headings and questions is easier to work from than a blank page.

1.8.8 Style Considerations

The following style guidelines will help to ensure your policies are useable:

- Consult your corporate style guide. If one exists, this will be an easy way to ensure all your policies have the same look and feel and will also help them to be more quickly accepted as corporate documents. If you don't have a style guide, consider developing one to ensure consistency throughout your policies. This will also make them easier to update and review.
- Ensure you have a consistent style throughout. There is much debate about the passive voice versus the active voice; whichever you use, chose one and stick to it throughout to aid comprehension.
- Be clear and use concrete rather than abstract language, e.g., say "log files must be reviewed at a minimum annually" rather than "log files must be reviewed regularly". What is considered "regular" will differ from person to person and your policy must mean the same to everyone so that it can be followed consistently?
- Avoid using very negative statements such as "never". Using overly strong negatives sets up gradations of prohibition that are unhelpful when you want to present clear, useable policy that either allows or disallows actions, or presents exceptions clearly. In the following example, the first policy statement weakens the second because of the statement that one action "must never" be done while the other is prohibited with the, by comparison softer, "must not": "Passwords must never be shared. Passwords must not be written down."
- Use simple, easy to understand language and pare it down to a minimum. All your readers must be able to understand your policy, and they shouldn't have to wade through reams of information to get to the point.
- Use "must" for "shall" and "will", where "must" is what you mean. You will therefore avoid inconsistencies in using "shall" and "will" and will not be mistaken for talking about the future.
- Don't include anything that isn't policy in the policy statements section of the document. Background information, for example, should go in a section of its own, either at the start of the document or in an appendix. You will weaken your policy statements by mixing them with informational statements. Similarly, procedural information should go in separate guidelines documents.
- Where you use bulleted lists in policy, ensure that all items in the list are grammatically similar. For example, if the list starts out as a list of nouns with modifiers, it shouldn't include any items that are verb phrases.

- Don't include the names of individuals in policy. People are likely to change job rile more frequently than you will change the policy. Instead use job role names or department names, e.g., "the DBA team manager".

1.8.9 Review Cycles

Review the draft with the project team as often as you need to ensure it is complete and correct and they are happy with it. Then make a final check of your document to ensure that you have followed the style guides outlined above. In addition, carry out a final spelling and grammar check and have your document proof-read by someone who wasn't involved in its development – this will help ensure that it is understandable and clear.

1.8.10 Review with Additional Stakeholders

During this review phase the policy should be reviewed by any groups who have an interest in the policy. This includes any groups who will be expected to work with the policy, which may have knowledge that needs to be taken into account when developing with the policy, or who are able to help ensure that the policy is enforceable and effective. Such groups include the legal and internal audit departments. In addition, regional offices should be considered here, they will have to comply with the policy, but their requirements may be different from those of the central office and this should be considered in this review phase.

1.8.11 Policy Gap Identification Process

Before publishing policy, it is a good idea to determine which (if any) policy statements are not currently in force in your organization. These are known as gaps. Document any such gaps and determine which groups or individuals are responsible for closing them. Include these groups in the discussion and let them know that this policy will shortly be published and will have an impact on their working practice. This will ensure that people are prepared for the publication of the policy and no one will be deluged with enquiries upon publication. You will need to inform any groups identified during the gap identification process for each policy of the time-scale of the grace period for compliance so that they can plan towards future compliance.

If you've pitched your policy correctly, you shouldn't find a very large number of gaps. Finding that every statement in the policy is actually a gap indicates that it is pitched too far towards a preferred future state and you may need to rethink some or all of the content. Once you have identified any gaps, it is a good idea to keep a record of the gaps for each policy somewhere (e.g., in a database or even simply a spreadsheet).

This should be checked regularly to see if any of the gaps are now closed or if any have passed the compliance grace period and need to be revisited. This

record will also be a useful resource when you come to revise the policy in the future. Maintenance of this record may be the responsibility of the policy development team, the wider information security team or other areas such as Internal Audit. Make it clear where this responsibility lies at the outset.

1.8.12 Develop Communication Strategy

Although the policy will be constantly available for company employees, you will initially need to make them aware of new or updated policy. Work with your communications or security awareness group to do this. Ensure that all appropriate management groups are informed, so that they can filter down information in their area.

It stands to reason that if policy is not read it will not be adhered to, so don't underestimate the importance of successfully communicating policies to the various audience groups. Depending on the size of the company and the maturity of the policy development process this will be more or less complex. Smaller companies have an easier job in one way in that it is logistically easier for them to reach all employees and let them know what they should be reading and following. It is also likely that smaller companies will have fewer policies for their employees to read since they will usually have fewer technologies in use. However, even getting employees to read the Governing Policy can be a challenge, especially existing employees when the policy changes. Here are a few suggestions for how to tackle this:

- Make it a contractual requirement: This is usually reserved for HR-owned policies which employees must adhere to as part of their employment contract. However, because of the growing importance of information security in the corporate world, there is a growing argument for having employees sign up to information security policies as well as general HR policies.

- Make policy part of required training: Incorporating information security policies into a training course (or courses) and making it a requirement for employees to complete these courses annually is another way to ensure policies get read and hopefully adhered to following course completion.

- Use a subscription-based communication method: One more advanced method of getting policies right under the noses of the employees who need to read them, and ensuring that the employees actually want to read them rather than considering them a nuisance, is to offer a subscription- based service where employees sign up to receive whichever policies are most appropriate for them. This 'sign up for security' method is something that could be activated when employees join the company, but could include a facility for employees to update their subscription options When ever they want to, for example if they move departments or change job role. While for larger firms this solution would require building a subscription service

and maintaining it, smaller firms may be able to use a manual system that could provide this sort of service fairly easily.

1.8.13 Publish

Policy documents should be published so that they are available to all company employees. This usually means putting them on a company intranet site, possibly the information security team's own intranet site. The documents should be easily accessible and available for download, printing, and saving. Determining the most appropriate policy delivery method is a particular issue for large companies or those with large numbers of policies that don't apply to all employees. System of policy delivery would mean that an employee would receive directly only those policies they needed to comply with to do their job. This would make it much more likely that the employee will read and comply with the policy versus a conventional system where they have to seek out the relevant policies from a larger policy bucket.

1.8.14 Activate Communication Strategy

E-mail is probably the best way to inform employees about policy changes quickly and effectively, although you may also want to include information about policy in other forms of company communication and through your company's security awareness program. Ensure policy is reflected in awareness strategies. An effective security awareness strategy will ensure that all your audiences are aware of your security policies, know where to find them and how to comply with them, as well as the consequences of non-compliance. Through a security awareness program, it should be possible to teach policy stakeholders about the policy and their role in maintaining it. This will help make the policy an integral part of their jobs. It is through using communication and education programs that you will be better able to foster a positive attitude in your company towards information security. There is evidence to show that users of the information security systems would be more willing to adhere to better security practices if they were knowledgeable (i.e., better trained and better informed) about what good practice actually involved .

A major part of ensuring policies have value is to ensure the employees who are supposed to follow them are aware of them and perhaps even more importantly, are aware of the value of adhering to them. This can be a big cultural shift in any organization. People often say things like: "but we've always done it that way" or "it doesn't matter if those SSNs go missing because we have stored them elsewhere". What security awareness campaigns must reflect is that the world has changed and it isn't about protecting the information just well enough so that it can be used for whatever purpose the company needs it for. There are now laws requiring companies to protect information at all times and to inform customers where security breaches occur. Therefore it isn't enough just to do things as they have always been

done or not to keep records of what customer information is stored where. This may have been enough previously, but what your security awareness campaigns need to reflect is that things have changed and the front line in ensuring information is protected are the employees. Once employees realize that even relatively small security breaches can have potentially devastating (and job jeopardizing) consequences, they are much more likely to be willing to act as your first line of defense and to pick up your policies and start adhering to them. Awareness, education and policy go hand in hand, each strengthening the other.

1.8.15 Regularly Review and Update

Each policy document should be updated regularly. At a minimum, an annual review strikes a good balance, ensuring that policy does not become out of date due to changes in technology or implementation, but is more feasible than a review every six months which would require a very quick turnover of a large number of policies for a large company. There should also be a provision for ad hoc updates that are necessary when fundamental changes in technology or process render existing policies, or parts of them, redundant. The review process should mirror the initial development process, but should be shorter, with the initial drafting phase telescoped into fewer meetings, or carried out over E-mail. The time for review phases by groups outside the information security team can also be shortened by having all groups review the draft at the same time.

When reviewing existing policies, a number of factors should be taken into account in addition to those included during the initial development. The experience of working with the existing policy by users, systems administrators, or anyone else who has seen the policy in action is valuable here. These people should be interviewed on how they think the policy worked and what could be changed in the future. They will also provide valuable insights into changes in technology or industry best practices that may need to be reflected by a change in the policy. Any security violations, deviations, and relevant audit information should also be reviewed when reviewing existing policy. This information will highlight any areas where the policy was difficult to enforce or where frequent deviations from policy were noted. It may be that elements of the policy are infeasible or need to be tweaked slightly to ensure that extra and unnecessary work on deviations is not created. This must as always be balanced with good security practice. Policy must primarily reflect what is necessary for good security. From a due diligence viewpoint, it is not acceptable to change good policy to inadequate policy just because there were a number of requests to deviate from that policy by certain groups within the company.

1.9 POLICY DOCUMENT OUTLINE

In addition to the policy statements that will form the main body of your policy documents, each policy should include the following sections.

Introduction

This section should introduce the policy by name and locate it within the hierarchy of other existing information security and company policy documents.

Purpose

State the main goals of the policy; this will explain the reason for the policy and will help readers understand how the policy should be used. Legal and compliance issues should also be mentioned in here. Include statements on any specific legislation the policy is designed to adhere to.

Scope

The scope is a statement of the infrastructure and information systems to which the policy applies, and the people who are stakeholders in it. Stakeholders would typically include anyone who is a user of the information or systems covered by the policy.

Roles and Responsibilities

This is a statement of the structures through which the responsibilities for policy implementation are delegated throughout the company. Job roles may be specified in this section, e.g., Database Administrators (DBAs), Technical Custodians, Field Office employees, etc.

Sanctions and Violations

This section details to what extent breaking policy is considered a violation (e.g., it is HR-related and therefore related to an employee's contract, or is it an information security department matter?) This section should also detail how violations should be reported, who to and what actions should be taken in the event of a violation. It should also include information on what sanctions will be carried out resulting from a violation (for example, verbal or written warnings, etc).

Revisions and Updating Schedule

This section defines who is responsible for making updates and revisions to the policy and how often these will take place. It may be useful to include a reference to the document as a "living document" which can be updated as determined by those responsible for updates and revisions. This will ensure

that any ad hoc revisions are accounted for as well as scheduled updates. Information should also be included detailing where the policy will be published and how employees can access it.

Contact Information

Details who should be contacted in connection with policy. A group or mailbox rather than an individual is preferable here as these are less likely to change.

Definitions/Glossary

Define any terms that may be unfamiliar to the reader. The necessity for this will depend on the audience, e.g., the readership of a Technical Policy for Linux are likely to already be familiar with the Linux technical terms, therefore it will not be necessary to spell these out. The cryptography section of the user policy however may include terms with which readers are not familiar and these should be defined in footnotes or a glossary to aid comprehension.

Check Your Progress 2

Note: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

1) Explain the policy development process?

.....

.....

.....

.....

2) Explain Top-Down Versus Bottom-Up Approach.

.....

.....

.....

.....

3) Explain Policy Development Lifecycle.

.....

.....

.....

.....

1.10 CYBER SECURITY STANDARDS

Cyber security standards are security standards which enable organizations to practice safe security techniques to minimize the number of successful cyber security attacks. These guides provide general outlines as well as specific techniques for implementing cyber security. For certain specific standards, cyber security certification by an accredited body can be obtained. There are many advantages to obtaining certification including the ability to get cyber security insurance.

History

Cyber security standards have been created recently because sensitive information is now frequently stored on computers that are attached to the Internet. Also many tasks that were once done by hand are carried out by computer; therefore there is a need for Information Assurance (IA) and security. Cyber security is important in order to guard against identity theft. Businesses also have a need for cyber security because they need to protect their trade secrets, proprietary information, and personally identifiable information (PII) of their customers or employees. The government also has the need to secure its information. One of the most widely used security standards today is ISO/IEC 27002 which started in 1995. This standard consists of two basic parts. BS 7799 part 1 and BS 7799 part 2 both of which were created by (British Standards Institute) BSI. Recently this standard has become ISO 27001. The National Institute of Standards and Technology (NIST) has released several special publications addressing cyber security. Three of these special papers are very relevant to cyber security: the 800-12 titled "Computer Security Handbook;" 800-14 titled "Generally Accepted Principles and Practices for Securing Information Technology;" and the 800-26 titled "Security Self-Assessment Guide for Information Technology Systems". The International Society of Automation (ISA) developed cyber security standards for industrial automation control systems (IACS) that are broadly applicable across manufacturing industries. The series of ISA industrial cyber security standards are known as ISA-99 and are being expanded to address new areas of concern.

ISO 27002

ISO 27002 incorporates both parts of the BS 7799 standard. Sometimes ISO/IEC 27002 is referred to as BS 7799 part 1 and sometimes it refers to part 1 and part 2. BS 7799 part 1 provides an outline for cyber security policy; whereas BS 7799 part 2 provides a certification. The outline is a high level guide to cyber security. It is most beneficial for an organization to obtain a certification to be recognized as compliant with the standard. The certification once obtained lasts three years and is periodically checked by the BSI to ensure an organization continues to be compliant throughout that three year period.

ISO 27001 (ISMS) replaces BS 7799 part 2, but since it is backward compatible any organization working toward BS 7799 part 2 can easily transition to the ISO 27001 certification process. There is also a transitional audit available to make it easier once an organization is BS 7799 part 2-certified for the organization to become ISO 27001-certified. ISO/IEC 27002 states that information security is characterized by integrity, confidentiality, and availability. The ISO/IEC 27002 standard is arranged into eleven control areas; security policy, organizing information security, asset management, human resources security, physical and environmental security, communication and operations, access controls, information systems acquisition/development/maintenance, incident handling, business continuity management, compliance.

Standard of Good Practice

In the 1990s, the Information Security Forum (ISF) published a comprehensive list of best practices for information security, published as the Standard of Good Practice (SoGP). The ISF continues to update the SoGP every two years; the latest version was published in February 2007.

Originally the Standard of Good Practice was a private document available only to ISF members, but the ISF has since made the full document available to the general public at no cost.

Among other programs, the ISF offers its member organizations a comprehensive benchmarking program based on the SoGP.

North American Electric Reliability Corporation (NERC)

The North American Electric Reliability Corporation (NERC) has created many standards. The most widely recognized is NERC 1300 which is a modification/update of NERC 1200. The newest version of NERC 1300 is called CIP-002-1 through CIP-009-2 (CIP=Critical Infrastructure Protection). These standards are used to secure bulk electric systems although NERC has created standards within other areas. The bulk electric system standards also provide network security administration while still supporting best practice industry processes.

NIST

Special publication 800-12 provides a broad overview of computer security and control areas. It also emphasizes the importance of the security controls and ways to implement them. Initially this document was aimed at the federal government although most practices in this document can be applied to the private sector as well. Specifically it was written for those people in the federal government responsible for handling sensitive systems.

Special publication 800-14 describes common security principles that are used. It provides a high level description of what should be incorporated within a computer security policy. It describes what can be done to improve existing security as well as how to develop a new security practice. Eight principles and fourteen practices are described within this document.

Special publication 800-26 provides advice on how to manage IT security. This document emphasizes the importance of self assessments as well as risk assessments.

Special publication 800-37, updated in 2010 provides a new risk approach: "Guide for Applying the Risk Management Framework to Federal Information Systems"

Special publication 800-53 rev3, "Guide for Assessing the Security Controls in Federal Information Systems", updated in August 2009, specifically addresses the 194 security controls that are applied to a system to make it "more secure."

Common Criteria (ISO 15408)

This standard develops what is called the "Common Criteria". It allows many different software applications to be integrated and tested in a secure way.

RFC 2196

RFC 2196 is memorandum published by Internet Engineering Task Force for developing security policies and procedures for information systems connected on the Internet. The RFC 2196 provides a general and broad overview of information security including network security, incident response or security policies. The document is very practical and focusing on day-to-day operations.

ISA-99

ISA99 is the Industrial Automation and Control System Security Committee of the International Society for Automation (ISA). The committee is developing a multi-part series of standards and technical reports on the subject, several of which have been publicly released. Work products from the ISA99 committee are also submitted to IEC as standards and specifications in the IEC 63443 series.

ISA-99.01.01 (formerly referred to as "Part 1") (ANSI/ISA 99.00.01) is approved and published.

ISA-TR99.01.02 is a master glossary of terms used by the committee. This document is still a working draft but the content is available on the committee Wiki site (http://isa99.isa.org/ISA99%20Wiki/Master%20Glossary.aspx)

ISA-99.01.03 identifies a set of compliance metrics for IACS security. This document is currently under development.

ISA-99.02.01 (formerly referred to as "Part 2") (ANSI/ISA 99.02.01-2009) addresses how to establish an IACS security program. This standard is approved and published. It has also been approved and published by the IEC as IEC 62443-2-1

ISA-99.02.02 addresses how to operate an IACS security program. This standard is currently under development.

ISA-TR99.02.03 is a technical report on the subject of patch management. This report is currently under development.

ISA-TR99.03.01 is a technical report on the subject of suitable technologies for IACS security. This report is approved and published.

ISA-99.03.02 addresses how to define security assurance levels using the zones and conduits concept. This standard is currently under development.

ISA-99.03.03 defines detailed technical requirements for IACS security. This standard is currently under development.

ISA-99.03.04 addresses the requirements for the development of secure IACS products and solutions. This standard is currently under development.

Standards in the ISA-99.04.xx series address detailed technical requirements at the component level. These standards are currently under development.

ISA Security Compliance Institute

Related to the work of ISA 99 is the work of the ISA Security Compliance Institute. The ISA Security Compliance Institute (ISCI) has developed compliance test specifications for ISA99 and other control system security standards. They have also created an ANSI accredited certification program called ISA Secure for the certification of industrial automation devices such as programmable logic controllers (PLC), distributed control systems (DCS) and safety instrumented systems (SIS). These types of devices provided automated control of industrial processes such as those found in the oil & gas, chemical, electric utility, manufacturing, food & beverage and water/wastewater processing industries. There is growing concern from both governments as well as private industry regarding the risk that these systems could be intentionally compromised by "evildoers" such as hackers, disgruntled employees, organized criminals, terrorist organizations or even state-sponsored groups. The recent news about the industrial control system malware known as Stuxnet has heightened concerns about the vulnerability of these systems.

1.11 THE IT SECURITY POLICY SANDARD: ISO 27001

ISO27001 was developed by the International Organization for Standardization (ISO) and the International Electro technical Commission (IEC) as a certification standard for information security management systems. ISO27001 certification can be a powerful credential for an organization, showing that their IT security policy follows an international standard of due care.

ISO27001 is designed to be used in conjunction with the ISO 17799:2005

Best practice recommendations for information security management. To achieve ISO27001 certification, organizations much adopt a risk-based approach that uses the security controls specified within ISO 17799:2005.

Information Shield has the tools your organization needs to save money while developing an IT security policy that will enable ISO27001 certification.

Information Security Policies Made Easy provides over 1300 security policies built within the ISO 17799:2005 framework. The ISO 17799:2005 policy map outlines the security policies that will lead you to ISO27001 certification, providing coverage of each security domain and sub-clause.

Information Security Roles and Responsibilities Made Easy is a perfect companion product, helping your organization define and document the roles and responsibilities recommended by ISO 17799:2005. It includes job descriptions with security requirements, organizational charts, and departmental mission statements all designed to facilitate your organizations move to compliance and certification.

Information Security Policies Made Easy does more than just enable development of your IT security policy. It shows you how to maintain and monitor those policies as required by the certification process.

Why re-invent the wheel? We can provide you with detailed IT security policy solutions, saving you hundreds of man-hours and thousands of dollars. Please contact Information Shield today for more information how we can help your ISO27001 certification.

Check Your Progress 3

Note: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

1) What are Cyber Security Standards?

.....

.....

.....

2) Explain NERC and NIST.

.....

.....

.....

.....

3) Describe ISA-99.

.....

.....

.....

.....

1.12 LET US SUM UP

Policy is both the starting point and the touchstone for information security in any company. Policy provides evidence of the company's stance on security and provides a living tool for every employee to help build and maintain that level of security. It is therefore essential that security policy is accurate, comprehensive, and useable. It can be a daunting task to produce policy that lives up to this standard. Assessing policy audiences, topics and methods using the processes.

This unit helps to ensure that your policy documents are as efficient and useable as possible. In turn, this will help ensure that your efforts to raise the standard of security in your company are worthwhile.

1.13 CHECK YOUR PROGRESS: THE KEY

Check Your Progress 1

1) Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

2) The two policy types supported by procedural documents:

- Governing Policy
- Technical Policy
- Job Aids / Guidelines

Check Your Progress 2

1) Refer to Section 1.6

2) **Top-Down versus Bottom-Up**

There are many starting points for developing policy. New or forthcoming legislation can often be a powerful impetus to develop policy, as can recent security incidents or enthusiastic administrators recently returned from the latest training course. All these provide great inputs to policy but the key is to be balanced. Relying solely on the 'top-down' approach of using only legislation, regulations and best practice to write your policy will leave you with unrealistic, artificial policy that won't be workable in the real world. Similarly, relying only on a 'bottom-up' method based only on system administrator knowledge can result in policy that is too specific to a given environment (perhaps just one part of a large company), possibly based too much on local current practice or on the latest training suggestions, making it too unrealistic. The best policy will come from a combination of these approaches, both top-down and bottom-up. In order to achieve this it is something that must be considered from the outset and must be reflected in the diversity of areas involved in policy development and the types of review policy undergoes. This balanced approach is likely to result in a more mature policy development process. It can work for both small companies (where there is little space between top and bottom) and big companies where the breadth of knowledge is needed to ensure a realistic and workable resulting policy.

3) Refer to Section 1.8

Check Your Progress 3

1) Refer to Section 1.10

2) **North American Electric Reliability Corporation (NERC)**

The North American Electric Reliability Corporation (NERC) has created many standards. The most widely recognized is NERC 1300 which is a modification/update of NERC 1200. The newest version of NERC 1300 is called CIP-002-1 through CIP-009-2 (CIP=Critical Infrastructure Protection). These standards are used to secure bulk electric systems although NERC has created standards within other areas. The bulk electric system standards also provide network security administration while still supporting best practice industry processes.

NIST

Special publication 800-12 provides a broad overview of computer security and control areas. It also emphasizes the importance of the security controls

and ways to implement them. Initially this document was aimed at the federal government although most practices in this document can be applied to the private sector as well. Specifically it was written for those people in the federal government responsible for handling sensitive systems.

Special publication 800-14 describes common security principles that are used. It provides a high level description of what should be incorporated within a computer security policy. It describes what can be done to improve existing security as well as how to develop a new security practice. Eight principles and fourteen practices are described within this document.

Special publication 800-26 provides advice on how to manage IT security. This document emphasizes the importance of self assessments as well as risk assessments.

Special publication 800-37, updated in 2010 provides a new risk approach: "Guide for Applying the Risk Management Framework to Federal Information Systems"

Special publication 800-53 rev3, "Guide for Assessing the Security Controls in Federal Information Systems", updated in August 2009, specifically addresses the 194 security controls that are applied to a system to make it "more secure."

3) Refer to Section 1.10

Basic Question and Answer

1) **Why has ISO 17799 been renamed to ISO 27002?**

Ans: The rename was initiated by ISO, who wanted to align the information security standards under a common naming structure (the 'ISO 27000 series').

2) **Which ISO27002 controls are most important?**

Ans: That largely depends upon the individual organization. However, ISO27002 does give some guidance, in the form of 'legislative essentials' and 'common best practice' under the IS "starting point" section. These are:

- intellectual property rights
- safeguarding of organizational records
- data protection and privacy of personal information
- information security policy document
- allocation of information security responsibilities
- information security education and training

- reporting security incidents
- business continuity management

3) **What is a Certification body?**

Ans: An accredited certification body is a third party organization that assesses/certifies the IS management system against the standard (BS7799-2 / ISO 27001).

4) **Who are the Accredited Certification bodies for the standard?**

Ans: There are a growing number of organizations accredited to grant certification against ISO27001. The following are amongst them: BSI, Certification Europe, DNV, JACO IS, KEMA, KPMG, SFS-Sertifiointi Oy, SGS, STQC, SAI Global Limited, UIMCert GmbH

5) **How do I become a certified auditor?**

Ans: The International Register for Certified Auditors operates a certification scheme for ISMS auditors.

6) **How does this standard fit with ISO 9000**?

Ans: ISO27001 is actually being "harmonized" with other management standards, including ISO 9000 and ISO 14000. Watch this space!

7) **Who originally wrote the security standard?**

Ans: Originally a BSI/DISC committee, which included representatives from a wide section of industry/commerce. It was reviewed subsequently by an ISO (International Standards Organization) committee and ultimately emerged through the ISO publication process.

8) **What is the ISO 27000 Toolkit?**

Ans: This is the main support resource for the standard, including the standard itself, ISO 27002 policy, etc. See top right panel for a more complete description.

9) **What is ISO/IEC Guide 62?**

Ans: This is largely for those bodies operating certification schemes and contains general requirements applicable to them.

10) **What is ISO 27001?**

Ans: BS7799-2, the original specification for an information security management system, was 'fast tracked' by ISO to become ISO 27001 in 2005.

1.14 SUGGESTED READINGS

- "Best Practices – Security Plans and Policies." URL: www.itsc.state.md.us/info/InternetSecurity/BestPractices/SecPolicy.htm (24 Sept 2003)
- Barman, Scott. Writing Information Security Policies. New York: Que, 2001.
- Danchev, Dancho. "Building and Implementing a Successful information Security Policy." 2003. URL: http://www.windowsecurity.com/pages/security-policy.pdf (10 July 2006)
- Desilets, Gary. "Shelfware: How to Avoid Writing Security Policy and Documentation That Doesn't Work." 20 Apr. 2001. URL: http://www.giac.org/practical/gsec/Gary_Desilets_GSEC.pdf (10 July 2006)
- Guel, Michele D. "A Short Primer for Developing Security Policies." 2001. URL: http://www.sans.org/resources/policies/Policy_Primer.pdf (12 July 2006)
- Harris, Shon, CISSP All in One Certification Exam Guide. New York: The McGraw-Hill Companies, 2002.
- Jarmon, David. "A Preparation Guide to Information Security Policies." 12 Mar. 2002. URL: http://www.sans.org/rr/paper.php?id=503 (10 July 2006)
- JISC, "Developing an Information Security Policy", 1 May 2001. URL: http://www.jisc.ac.uk/index.cfm?name=pub_smbp_infosec (10 July 2006)
- Kok Kee, Chaiw. "Security Policy Roadmap – Process for Creating Security Policies." 2 Oct. 2001. URL: http://www.sans.org/rr/paper.php?id=494 (10 July 2006)
- Lambe, Jennifer L. Intercom, "Techniques for successful SME interviews." Mar. 2000, pp.30-32
- Lindley, Patrick J. "Technical Writing for IT Security Policies in Five Easy Steps." 20 Sept. 2001. URL: http://www.sans.org/rr/paper.php?id=492 (10 July 2006)
- Long, Gerald P. "Security Policies in a Global Organization." 25 Feb. 2002. URL: http://www.sans.org/rr/paper.php?id=501 (10 July 2006)
- Peltier, Thomas, R. "Information Security Fundamentals." 2002. URL: http://www.gocsi.com/ip.htm (29 Sept. 2003)
- Russell, Chelsa. "Security Awareness – Implementing an Effective Strategy." 25 Oct. 2002. URL: http://www.sans.org/rr/paper.php?id=418 (10 July 2006)

UNIT 2 SECURITY FRAMEWORK STANDARDS

Structure

2.0 INTRODUCTION

ISO (International Organization for Standardization) is a global network that identifies what International Standards are required by business, government and society, develops them in partnership with the sectors that will put them to use, adopts them by transparent procedures based on national input and delivers them to be implemented worldwide. ISO standards distil an international consensus from the broadest possible base of stakeholder groups. Expert input comes from those closest to the needs for the standards and also to the results of implementing them. In this way, although voluntary, ISO standards are widely respected and accepted by public and private sectors internationally.

ISO – a non-governmental organization – is a federation of the national standards bodies of 157 countries, one per country, from all regions of the world, including developed, developing and transitional economies.

Each ISO member is the principal standards organization in its country. The members propose the new standards, participate in their development and provide support in collaboration with ISO Central Secretariat for the 3 000 technical groups that actually develop the standards.

ISO standards make a positive contribution to the world. They ensure vital features such as quality, ecology, safety, economy, reliability, compatibility, interoperability, efficiency and effectiveness. They facilitate trade, spread knowledge, and share technological advances and good management practices. ISO members appoint national delegations to standards committees.

In all, there are some 50 000 experts contributing annually to the work of the Organization. When their work is published as an ISO International Standard, it may be adopted as a national standard by the ISO members and translated.

Fig. 1: International organization for standardization

ISO's Partners

ISO collaborates with its partners in international standardization, the IEC (International Electro technical Commission) and the ITU-T (International

Telecommunication Union), particularly in the field of information and communication technology. They have established the World Standards Cooperation (WSC) as the focus for their combined strategic activity. ISO has a strategic partnership with the World Trade Organization (WTO) aiming to promote a free and fair global trading system. Signatories to the WTO Agreement on Technical Barriers to Trade (TBT) commit themselves to promoting and using international standards of the type developed by ISO.

ISO cooperates closely with most of the specialized agencies and bodies of the United Nations that are involved in technical harmonization and assistance to developing countries. ISO also maintains close working relations with regional

standards organizations, many of whose members also belong to ISO. In addition, several hundred specialized organizations representing trade or regulatory sectors participate in developing ISO standards.

New Growth Areas for ISO Standards in the Coming Years

- **The environment** – with standards for meeting new requirements such as greenhouse gas verification (climate change mitigation) and for other aspects of sustainable development ;
- **The service sectors** – with standards already being developed for personal financial services, market opinion, social research and tourism;
- **Security** – among aspects already addressed are maritime port security, freight transport and countering illegal trafficking of radioactive materials;
- **Good managerial and organizational practice** – such as the guidelines ISO is developing on societal responsibility.

In addition, ISO is well placed to provide voluntary standards for formerly regulated areas such as energy, water supply or transportation.

2.1 OBJECTIVES

After studying this unit, you should be able to learn the objective of ISO which include:

- set the standards;
- ensure products and services are quality assured;
- achieve consistency of the output;
- provide products that is customer focused or oriented;
- produce products that meets customers' requirements;

- enhance customer satisfaction for the products and their trust in it;
- enhance quality management;
- enhance effective and efficient products design and development.

2.2 IMPORTANCE OF ISO STANDARDS

ISO (International Organization for Standardization) is the world's largest and foremost developer and publisher of international standards. Because the organization is present globally, and the name "International Organization for Standardization" would be abbreviated differently in different countries, the founders chose the name "ISO," derived from the Greek term "isos," which means "equal." ISO is a non-governmental organization headquartered in Geneva, Switzerland, and networks the regional standards institutes and regulatory bodies of 163 countries.

- **Bridging the Public and Private Sectors**

The ISO structure, with one member institute per country, bridges the gap between the public and private sectors and facilitates exchange of information between regulators and businesses. In many countries, the member institute is a governmental entity, whereas in other countries, the member institute is a private entity. This part public-part private structure in different parts of the world enables ISO to develop standards and solutions that benefit both the business sector and society as a whole, making sure that one entity's interests are not prioritized over another.

- **Role of Standards**

The ISO official site contends that "Standards make an enormous and positive contribution to most aspects of our lives." The importance of standards may be better appreciated when considering what would happen in its absence; when a product is made according to predefined standards and meets customer expectations, it is often taken for granted. However, in an environment without standards, people would very likely voice concerns about poor quality and unsafe products. Whether a business manufactures goods or provides services, when it meets standards relevant to its industry, it ensures that positive characteristics such as quality, durability, efficiency, safety and environmental friendliness are reinforced.

- **Benefits for Business**

ISO standards benefit businesses because they can focus their resources on producing goods and services that are internationally standardized. With an industry-wide set of standards in place, businesses are better equipped to develop and offer products and services to foreign markets that recognize the same set of standards. ISO standards improve production by making each activity within the overall process, such as developing, manufacturing and supplying, more efficient. Standards also play a vital role in the development of high-tech goods. When a business innovates a new technology, international standards facilitate the development of terminology and compatibility, making the innovation marketable.

- **Benefits for Governments**

For governments, standards provide tools to assess and evaluate conformity, and provide a legitimate base for health and safety legislation. Having standards in place also facilitates fairer trade between regions by ensuring that both the importer side and exporter side of foreign trade transactions know about the relevant set of standards. For governments in developing countries, ISO standards give information about expected attributes of products and services for export markets. This information gives a basis for governments to allocate resources accordingly, and produce goods and services that will be accepted in different regions.

- **Importance in Society**

ISO standards benefit end consumers by safeguarding their interests and by ensuring that the products and services they purchase are safe and reliable. The standards also help to reduce environmental impact of business operations by publishing accepted levels of gas and radiation emission, and controlling the quality of water, air and soil. In addition, ISO standards drive the move toward sustainable productions processes; ISO synchronizes and aligns businesses to cleaner and safer production methods by laying down operational guidelines for different industries.

2.3 IS027K (ISO/IEC 27000-SERIES) STANDARDS

The **ISO27k (ISO/IEC 27000-series) standards** concern the protection of valuable information assets through information security, particularly the use of Information Security Management Systems (ISMSs) and the ISO/IEC 27000-series numbering ("ISO27k") has been reserved for a family of information security management standards derived from British Standard BS 7799.

The following standards are either published or under development. The content of as-yet unpublished standards mentioned below may well change prior to their publication:

- **ISO/IEC 27000:2009** - provides an overview/introduction to the ISO27k standards as a whole plus the specialist vocabulary used in ISO27k.
- **ISO/IEC 27001:2005** is the Information Security Management System (ISMS) requirements standard, a specification for an ISMS against which thousands of organizations have been certified compliant.
- **ISO/IEC 27002:2005** is the code of practice for information security management describing a comprehensive set of information security control objectives and a set of generally accepted good practice security controls.
- **ISO/IEC 27003:2010** provides guidance on implementing ISO/IEC 27001.
- **ISO/IEC 27004:2009** is an information security management measurement standard.
- **ISO/IEC 27005:2011** is an information security risk management standard.
- **ISO/IEC 27006:2007** is a guide to the certification or registration process for accredited ISMS certification or registration bodies.
- **ISO/IEC 27007** will be a guideline for auditing Information Security Management Systems.
- **ISO/IEC TR 27008** will guide the auditing of information security controls.
- **ISO/IEC 27010** will provide guidance on information security management for intersector and inter-organizational communications.
- **ISO/IEC 27011:2008** is the information security management guideline for telecommunications organizations (also known as ITU X.1051).
- **ISO/IEC 27013** will provide guidance on the integrated/joint implementation of both ISO/IEC 20000-1 (derived from ITIL) and ISO/IEC 27001 (ISMS).
- **ISO/IEC 27014** will cover governance of information security.
- **ISO/IEC 27015** will provide information security management guidance for organizations in the financial services industry.
- **ISO/IEC TR 27016** will cover the economics of information security management.

- **ISO/IEC 27031** is an ICT-focused standard on business continuity.
- **ISO/IEC 27032** will provide guidelines for cyber security.
- **ISO/IEC 27033** is replacing the multi-part ISO/IEC 18028 standard on IT network security (part 1 released, rest in preparation).
- **ISO/IEC 27034** will provide guidelines for application security.
- **ISO/IEC 27035** on information security incident management.
- **ISO/IEC 27036** guideline for security for supplier relationships.
- **ISO/IEC 27037** guideline for digital evidence.
- **ISO/IEC 27038** specification for digital redaction.
- **ISO/IEC 27039** concerns intrusion detection and prevention systems.
- **ISO/IEC 27040** guideline on storage security.
- **ISO 27799:2008** provides health sector specific ISMS implementation guidance based on ISO/IEC 27002.

Check Your Progress 1

Note: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

1) "The titles of the ISO27k standards mention 'Information Technology -- Security Techniques'. Does this mean they only apply to IT?"

.....

.....

.....

.....

2) "What does 'ISO' mean? And what about 'ISO/IEC'?"

.....

.....

.....

.....

2.3.1 ISO/IEC 27000:2009

The scope of ISO/IEC 27000 is "to specify the fundamental principles, concepts and vocabulary for the ISO/IEC 27000 (information security management system) series of documents."

ISO/IEC 27000 contains the overview and vocabulary, in other words:

- An **overview** of the ISO27k standards showing how they are used collectively to plan, implement, certify and operate an ISMS, with a basic introduction to information security, risk management and management systems
- Carefully-worded **definitions** for the information security-related terms as they are used throughout the ISO27k standards.

Information security, like most technical subjects, is evolving a complex web of terminology. Several core terms in information security (such as "risk") have different meanings according to the context and the reader's preconceptions. Few authors take the trouble to define precisely what they mean but this is unacceptable in the standards arena as it leads to confusion and devalues formal assessment and certification.

ISO/IEC 27000 is similar to other vocabulary and definitions standards and will hopefully become a generally-accepted reference for information security terms amongst the information security profession.

A revised version of ISO/IEC 27000 is currently in the works. It will be based on the existing/current versions of ISO/IEC 27001 and 27002.

2.3.2 ISO/IEC 27001:2005

ISO/IEC 27001 is the formal set of specifications against which organizations may seek independent certification of their Information Security Management System (ISMS).

ISO/IEC 27001 specifies requirements for the establishment, implementation, monitoring and review, maintenance and improvement of a management system - an overall management and control framework - for managing an organization's information security risks. It does not mandate specific information security controls but stops at the level of the management system.

The standard covers all types of organizations (e.g. commercial enterprises, government agencies and non-profit organizations) and all sizes from micro-businesses to huge multinationals.

Bringing information security under management control is a prerequisite for sustainable, directed and continuous improvement. An ISO/IEC 27001 ISMS therefore incorporates several Plan-Do-Check-Act (PDCA) cycles: for

example, information security controls are not merely specified and implemented as a one-off activity but are continually reviewed and adjusted to take account of changes in the security threats, vulnerabilities and impacts of information security failures, using review and improvement activities specified within the management system.

ISO/IEC 27001 "is intended to be suitable for several different types of use, including:

- Use within organizations to formulate security requirements and objectives;
- Use within organizations as a way to ensure that security risks are cost-effectively managed;
- Use within organizations to ensure compliance with laws and regulations;
- Use within an organization as a process framework for the implementation and management of controls to ensure that the specific security objectives of an organization are met;
- The definition of new information security management processes;
- Identification and clarification of existing information security management processes;
- Use by the management of organizations to determine the status of information security management activities;
- Use by the internal and external auditors of organizations to demonstrate the information security policies, directives and standards adopted by an organization and determine the degree of compliance with those policies, directives and standards;
- Use by organizations to provide relevant information about information security policies, directives, standards and procedures to trading partners and other organizations that they interact with for operational or commercial reasons;
- Implementation of a business enabling information security; and
- Use by organizations to provide relevant information about information security to customers."

2.3.3 ISO/IEC 27002:2005

ISO/IEC 27002:2005, the latest version of "Information technology - Security techniques - Code of practice for information security management", to give it its full title, is an internationally-accepted standard of good practice for

- Scoping and defining the boundaries in terms of ICT and physical locations;
- Assessing information security risks and planning appropriate risk treatments, where necessary defining information security control requirements;
- Designing the ISMS;
- Planning the implementation project.

This standard references and is builds upon other ISO27k standards, particularly the normative standards ISO/IEC 27000 and ISO/IEC 27001.

2.3.5 ISO/IEC 27004:2009

ISO/IEC 27004 covers information security management measurements, generally known as security metrics.

The standard was published in December 2009.The standard is intended to help organizations measure, report on and hence systematically improve the effectiveness of their Information Security Management Systems.

It "provides guidance on the development and use of measures and measurement in order to assess the effectiveness of an implemented information security management system (ISMS) and controls or groups of controls, as specified in ISO/IEC 27001. This would include policy, information security risk management, control objectives, controls, processes and procedures, and support the process of its revision, helping to determine whether any of the ISMS processes or controls needs to be changed or improved."

2.3.6 ISO/IEC 27005:2011

"ISO/IEC 27005 provides guidelines for information security risk management. It supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach. Knowledge of the concepts, models, processes and terminologies described in ISO/IEC 27001 and ISO/IEC 27002 is important for a complete understanding of ISO/IEC 27005:2008. ISO/IEC 27005:2008 is applicable to all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations) which intend to manage risks that could compromise the organization's information security."

ISO/IEC 27005 revises and supersedes the Management of Information and Communications Technology Security (MICTS) standards ISO/IEC TR 13335-3:1998 plus ISO/IEC TR 13335-4:2000.

The standard doesn't specify, recommend or even name any specific method although it does specify a structured, systematic and rigorous method of analyzing risks through to creating the risk treatment plan.

2.3.7 ISO/IEC 27006:2007

ISO/IEC 27006 is the published ISO/IEC accreditation standard that guides certification bodies on the formal processes for certifying or registering other organizations' information security management systems (ISMSs).

The scope of ISO/IEC 27006 is "to specify general requirements a third-party body operating ISMS certification/registration has to meet, if it is to be recognized as competent and reliable in the operation of ISMS certification / registration."

ISO/IEC 27006 specifies requirements and provides guidance for ISMS certification, in addition to the requirements contained within ISO/IEC 17021-1 from which it was derived and ISO/IEC 27001 which specifies requirements for the ISMS. It is focused on auditing the management system and has limited interest in the information security controls managed by the management system.

2.3.8 ISO/IEC 27007

This standard will provide guidance for accredited certification bodies, internal auditors, external/third party auditors and others auditing ISMSs against ISO/IEC 27001 (i.e. auditing the management system for compliance with the standard). It will also offer guidance on the competence and evaluation of ISMS auditors.

ISO/IEC 27007 will directly reflect ISO 19011, the ISO standard for auditing quality and environmental management systems - "management systems" of course being the common factor linking it to the ISO27k standards. It will provide additional ISMS-specific guidance.

2.3.9 ISO/IEC TR 27008

This standard will provide guidance for all auditors regarding "information security management systems controls" selected through a risk-based approach (e.g. as presented in a statement of applicability) for information security management. It will support the information security risk management process and internal, external and third-party audits of ISMS by explaining the relationship between the ISMS and its supporting controls. It will provide guidance on how to verify the extent to which required "ISMS controls" are implemented. Furthermore, it will support any organization using ISO/IEC 27001 and ISO/IEC 27002 to satisfy assurance requirements, and as a strategic platform for Information Security Governance.

Purpose of this standard:

- Be applicable to all organizations, including public and private companies, government entities and not-for-profit organizations and organizations of all sizes regardless of the extent of their reliance on information;
- Support planning and execution of ISMS audits and the information security risk management process;
- Further add value and enhance the quality and benefit of the ISO27k standards by closing the gap between reviewing the ISMS in theory and, when needed, verifying evidence of implemented ISMS controls (e.g. in the ISO27k user organizations, assessing security elements of business processes, IT systems and IT operating environments);
- Provide guidance for auditing information security controls based on the controls guidance in ISO/IEC 27002;
- Improve ISMS audits by optimizing the relationships between the ISMS processes and required controls (e.g. mechanisms to limit the harm caused by failures in the protection of information - erroneous financial statements, incorrect documents issued by an organization and intangibles such as reputation and image of the organization and privacy, skills and experience of people);
- Support an ISMS-based assurance and information security governance approach and audit thereof [?? This appears to stray into the area of management systems auditing rather than information security auditing];
- Ensure effective and efficient use of audit resources.

2.3.10 ISO/IEC 27010

This standard will providing guidance in relation to sharing information on information security risks, controls, issues and/or incidents that span the boundaries between industry sectors and/or nations, particularly those affecting "critical infrastructure".

Sometimes it is necessary to share confidential information regarding information security threats, vulnerabilities and/or incidents between or within a community of organizations, for example when private companies, governments, law enforcement and CERT-type bodies are collaborating on the investigation, assessment and resolution of serious pan-organizational and often international or pan-jurisdictional cyber attacks. Such information is often highly sensitive and it may need, for example, to be restricted to certain individuals within the recipient organizations. Information sources may need to be protected by remaining anonymous. Such information exchanges typically happen in a highly charged and stressful atmosphere under intense time pressures - hardly the most conducive environment for establishing trusted

working relationships and agreeing on suitable information security controls. The standard should help by laying out common ground-rules for security.

The standard will provide guidance on methods, models, processes, policies, controls, protocols and other mechanisms for the sharing of information securely with trusted counterparties on the understanding that important information security principles will be respected.

2.3.11 ISO/IEC 27011:2008

"For telecommunications organizations, information and the supporting processes, telecommunications facilities, networks and lines are important business assets. In order for telecommunications organizations to appropriately manage these business assets and to correctly and successfully continue their business activities, information security management is extremely necessary. This recommendation provides the requirements on information security management for telecommunications organizations.

This standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented information security management system (ISMS) within the context of the telecommunication's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual telecommunications or parts thereof."

2.3.12 ISO/IEC 27013

This standard will provide guidance on implementing an integrated information security and IT service management system, based on both ISO/IEC 27001:2005 (ISMS) and ISO/IEC 20000-1:2011 (IT service management specification, derived from ITIL) standards respectively, since those management systems are felt to complement and support each other.

The standard will provide a framework for organizing and prioritizing activities, with advice on:

- Aligning the information security and service management and improvement objectives;
- Coordinating multidisciplinary activities, leading to a more integrated and aligned approach (e.g. both donor standards specify incident management activities, with differing scopes for the incidents but otherwise quite similar);
- A collective system of processes and supporting documents (policies, procedures etc.);
- A common vocabulary and shared vision;

- Combined business benefits to customers and service providers plus additional benefits arising from the integration of both management systems; and
- Combined auditing of both management systems at the same time, with the consequent reduction in audit costs.

2.3.13 ISO/IEC 27014

The standard will hopefully cover aspects such as:

- The organization's business strategies, policies and objectives [in relation to information security, risks and controls];
- Compliance with applicable governance regulations, laws, contractual and other legal obligations to third parties, and vice versa [in respect of information security obligations], including the associated assurance activities such as certification audits, internal audits, management reviews etc. on the ISMS;
- Risk management - specifically management of information security risks;
- Distinguishing management controls - specifically the ISMS being a management system managing a coherent framework/suite of information security controls - from governance;
- The relationship between governance of information security [information security governance], IT [IT governance], possibly information [information governance], and the entire corporation [corporate governance];
- Both accountability and responsibility for information security, issues arising from the nominal 'ownership' of information assets by specific individuals or functions within many organizations.

2.3.14 ISO/IEC 27015

"This standard aims to support sectors in fulfilling sector specific information security related legal and regulatory requirements through an internationally agreed and well-accepted framework. It aims to provide guidelines on how to meet baseline information security management requirements and implement appropriate controls and processes to meet confidentiality, integrity, availability and any other relevant security requirements. This standard should serve the financial and insurance sector as well as their business partners and customers. This standards follows the ISMS risk based approach and therefore this standard incorporates flexibility to address the following topics related to the protection of the organizations information assets:

- The organization's business strategy and focused market segments;
- Characteristics of different geographical and domestic regions;
- The organization's specific services and products;
- Applicable legal and regulatory constraints.

This standard does not intend to specify mandatory requirements but should rather serve as guidance how to provide visible evidence can be provided to business partners, customers and regulatory bodies that an organization follows commonly agreed best practice levels for information security management."

2.3.15 ISO/IEC TR 27016

"Information security professionals, whether working as specialist consultants or working as employees of organizations, commonly report difficulty justifying the expenditure of money on information security controls to managers with a primary focus on financial matters concerning the core business of that organization. In many cases, this problem arises because there is no agreed way to relate matters concerning economics and information security. This standard will reduce such problems.

The objective of the standard is to present guidelines based on commonly accepted good practice that can be used and understood by both information security professionals and general managers to discuss information security program initiatives and alternatives in terms of the financial outcomes that are expected."

Purpose of this standard:

- Help management appreciate and understand the financial impacts of information security in the context of an ISO27k ISMS, along with political, social, compliance and other potential impacts on the organization that collectively influence how much it needs to invest in protecting its information assets;
- Support the CISO or ISM in proposing corporate investment in an ISMS to senior management, and justifying the budget;
- Cover the valuation of information assets plus the corresponding information security risks and information security controls, and hence will help management determine the appropriate level of resources needed to implement and operate an ISMS. The idea being, basically, to invest just the right amount in the ISMS, neither too little nor too much;
- Extend to the level of determining appropriate investment in various parts or elements of an ISMS, for example how much to invest in information security risk assessment activities versus information security controls;

- Supplement other ISO27k standards by providing the financial perspective, providing guidance on the fundamentals of economics in this field and showing how to apply useful economic or financial models to information security through descriptions and examples, perhaps including a cost-benefit statement or business case and suggesting financial metrics;
- Be generic: each user organization will have to develop its own customized business case for the ISMS investment, reflecting its particular circumstances and needs. Each organization is unique. However, the standard may provide a general framework or structure as a starting point, along with some 'donor text' that might be quoted or adapted by users where applicable, for example laying out the fundamentals and suggesting common ways to value and justify an ISMS.

2.3.16 ISO/IEC 27031:2011

ISO/IEC 27031 provides guidance on the concepts and principles behind the role of information and communications technology in ensuring business continuity.

The standard will:

- Suggest a structure or framework (methods and processes) for any organization – private, governmental, and non-governmental
- Identify and specify all relevant aspects including performance criteria, design, and implementation details, for improving ICT readiness as part of the organization's ISMS, helping to ensure business continuity.
- Enable an organization to measure its continuity, security and hence readiness to survive a disaster in a consistent and recognized manner.

The scope of this standard encompasses all events and incidents (not just information security related) that could have an impact on ICT infrastructure and systems. It therefore extends the practices of information security incident handling and management.

2.3.17 ISO/IEC 27032

ISO/IEC 27032 will address "Cyber security" or "Cyberspace security", which is defined as the "preservation of confidentiality, integrity and availability of information in the Cyberspace". In turn "the Cyberspace" is defined as "the complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form".

2.3.18 ISO/IEC 27033

ISO/IEC 27033 will be a multi-part standard derived from the existing five-part network security standard ISO/IEC 18028. The existing standard is being substantially revised, not just renamed.

"The purpose of ISO/IEC 27033 is to provide detailed guidance on the security aspects of the management, operation and use of information system networks, and their inter-connections. Those individuals within an organization that are responsible for information security in general, and network security in particular, should be able to adapt the material in this standard to meet their specific requirements."

ISOI/IEC 27033 provides detailed guidance on implementing the network security controls that are introduced in ISO/IEC 27002. It applies to the security of networked devices and the management of their security, network applications/services and users of the network, in addition to security of information being transferred through communications links. It is aimed at network security architects, designers, managers and officers.

2.3.19 ISO/IEC 27034

This multi-part standard will provide guidance on specifying, designing/selecting and implementing information security controls through a set of processes integrated throughout an organization's Systems Development Life Cycle/s. It will cover software applications developed internally, by external acquisition, outsourcing/off shoring or through hybrid approaches. It will address all aspects from determining information security requirements, to protecting information accessed by an application as well as preventing unauthorized use and/or actions of an application.

The standard will be 'SDLC method agnostic', in other words it will not mandate particular development methods, approaches or stages but will be written in a general manner to be applicable to all. In this way, it will complement other systems development standards without conflicting with them.

2.3.20 ISO/IEC 27035

Information security controls are imperfect in various ways: controls can fail, work partially, or be completely missing (*e.g.* not implemented or not operational). Consequently, incidents are bound to happen since preventive controls are not totally reliable and effective.

Managing incidents effectively involves detective and corrective controls designed to minimize adverse impacts, gather forensic evidence (where applicable) and 'learn the lessons' in terms of prompting improvements to the ISMS, especially the implementation of more effective preventive controls.

Information security incidents commonly involve the exploitation of previously unrecognized and/or uncontrolled vulnerabilities; hence vulnerability management (*e.g.* applying relevant security patches to IT systems and addressing control weaknesses in procedures) is part preventive and part corrective action.

ISO/IEC 27035 lays out a structured and planned approach to:

- Detect report and assess information security incidents;
- Respond to and manage information security incidents;
- Detect, assess and manage information security vulnerabilities; and
- Continuously improve information security and incident management as a result of managing information security incidents and vulnerabilities.

The standard includes vulnerability management as well as incident management.

2.3.21 ISO/IEC 27036

ISO/IEC 27036 will be a multi-part standard offering guidance on the evaluation and mitigation of security risks involved in the procurement and use of information or IT-related services supplied by other organizations. It is planned to cover the following broad areas:

- Strategic goals, objectives and business needs in relation to information security;
- Information security risks and mitigation techniques;
- Provision of assurance (and presumably compliance with contractual obligations etc.).

This standard may include the information security aspects of cloud computing.

2.3.22 ISO/IEC 27037

The standard will provide detailed guidance on the identification, collection and/or acquisition, marking, storage, transport and preservation of electronic evidence, particularly to maintain its integrity. It will define and describe the process of recognition and identification of the evidence, documentation of the crime scene, collection and preservation of the evidence, and the packaging and transportation of evidence.

The scope has been refined slightly to cover 'traditional' IT systems and media rather than vehicle systems, cloud computing etc., at this time anyway. New technologies inevitably present new challenges and the field are continually evolving, but the project team wants to complete and release the initial

guidance as soon as practicable, which means concentrating on current, stable technologies. The guidance is aimed primarily at first responders.

Benefits of the standard include:

- Maintaining an assured minimum level of integrity of digital forensic evidence required for cross-border legal actions; and
- Assisting law enforcement and private sector organizations that gather and/or preserve and communicate digital forensic evidence for criminal investigations, to achieve and protect the quality of evidence required.

2.3.23 ISO/IEC 27038

Digital data sometimes have to be revealed to third parties, occasionally even published to the general public, for reasons such as disclosure of official documents under 'freedom of information' law or as evidence in commercial disputes or legal cases. However, where it is deemed inappropriate to disclose certain sensitive data within the files (such as the names or locations of people who must remain anonymous and various other personal or proprietary information that must remain strictly confidential), those must be securely removed from the files prior to their release. 'Redaction' is the name of the process to deny file recipients access to certain sensitive data within the original files.

Given that redaction is usually only relevant to the protection of highly confidential information, failures in the process that lead to inappropriate data disclosure are almost bound to be serious and in the worst cases can be grave. Redaction failures have led to incidents such as identity theft, disclosure of confidential security matters, and compromising the identities of undercover agents and informants, while disclosure of trade secrets could prove extremely costly in a commercial context. At the very least, redaction failures are embarrassing to those responsible for the process.

"This international standard specifies characteristics of techniques for performing digital redaction on electronic documents as well as approaches for the validation of digital redaction functions within document preparation software or standalone digital redaction tools."

2.3.24 ISO/IEC 27039

IDS (Intrusion Detection Systems) are largely automated systems for identifying attacks on and intrusions into a network or system by hackers and raising the alarm. IPS (Intrusion Prevention Systems) take the automation a step further by automatically responding to certain types of identified attack, for example by closing off specific network ports through a firewall to block hacker traffic. This standard refers to either type.

2.3.25 ISO/IEC 27040

The standard will help the purchasers and users of computer storage technologies determine and treat the associated information security risks.

The objectives for this standard are to:

- Draw attention to common information security risks associated with protecting the confidentiality, integrity and availability of information on storage technologies;
- Encourage organizations to improve their protection of stored information using suitable information security controls; and
- Improve assurance, for example facilitate reviews or audits of the information security controls protecting data storage.

The information security issues associated with backup/disaster recovery locations and cloud storage will probably be covered, as well as those associated with primary/local storage on a variety of technologies, media and storage subsystems. Media sanitization may also be covered.

2.3.26 ISO 27799:2008

"This International Standard provides guidance to healthcare organizations and other custodians of personal health information on how best to protect the confidentiality, integrity and availability of such information by implementing ISO/IEC 27002. Specifically, this International Standard addresses the special information security management needs of the health sector and its unique operating environments. While the protection and security of personal information is important to all individuals, corporations, institutions and governments, there are special requirements in the health sector that need to be met to ensure the confidentiality, integrity, audit ability and availability of personal health information. This type of information is regarded by many as being among the most confidential of all types of personal information. Protecting this confidentiality is essential if the privacy of subjects of care is to be maintained. The integrity of health information must be protected to ensure patient safety, and an important component of that protection is ensuring that the information's entire life cycle be fully auditable. The availability of health information is also critical to effective healthcare delivery. Health informatics systems must meet unique demands to remain operational in the face of natural disasters, system failures and denial-of-service attacks. Protecting the confidentiality, integrity and availability of health information therefore requires health-sector-specific expertise ... It is not intended to supplant ISO/IEC 27002 or ISO/IEC 27001. Rather, it is a complement to these more generic standards.

2.3.27 OTHER ISO27K STANDARDS

In addition to the ISO27k standards that have already been allocated numbers, SC27 is considering further ISO27k standards as well.

Check Your Progress 2

Note: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

1) What should we cover in information security policy?

.....

.....

.....

.....

2) Which information security risk analysis method/s could you use if you are just starting an ISO 27k program?

.....

.....

.....

.....

2.4 LET US SUM UP

ISO27k" (the ISO/IEC 27000-series) is the most influential and popular suite of information security standard in the world. The ISO27k standards provide generally-accepted good practice guidance on Information Security Management Systems to protect the confidentiality, integrity and availability of the information assets on which we all depend.

This unit is an attempt to explain how you should support the information security awareness activities that are essential for compliance with ISO27k and particularly for certification against ISO/IEC 27001.

2.5 CHECK YOUR PROGRESS: THE KEY

Check Your Progress 1

1) No, most certainly not! The formal titles simply reflect the name of the joint · ISO + IEC committee that oversees their production, namely SC27

"Information Technology -- Security Techniques", itself a subcommittee of JTC1 "Information Technology".

The scope of the ISO27k standards naturally includes many aspects of IT but does not stop there. The introduction to ISO/IEC 27002 states explicitly: "Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post of using electronic means, shown on films, or spoken in conversation. Whatever form information takes, or means by which it is shared or stored, it should always be appropriately protected."

Not all an organization's information assets belong to or are managed within the IT function. IT typically owns and manages the shared IT infrastructure (the main corporate IT and network systems) but acts as a *custodian* for most corporate information content which belongs to other business units, and for other content belonging to customers and business partners. There are important implications in that information owners are accountable for ensuring that their information assets are adequately protected, just like other corporate assets. While information asset owners generally delegate key responsibilities for information security to an information security management function and/or IT function, they remain accountable and must ensure that information security is adequately funded and supported to achieve the necessary level of protection.

2) ISO is the short or common name of the global standards body known in English as the International Organization for Standardization. "ISO" is not strictly an abbreviation since the long name varies in different languages - it is in fact derived from the Greek word *isos* meaning equal.

IEC is the International Electro technical Commission, another international standards body that cooperates closely with ISO on electrical, electronic and related technical standards. Standards developed jointly with ISO are prefixed "ISO/IEC" although in practice most users [incorrectly] shorten it to "ISO".

ISO/IEC also collaborates on some standards with other international organizations (both governmental and private sector) such as the ITU, the International Telecommunication Union. The ITU is primarily a trade body coordinating telecoms organizations and practices to enable worldwide communications. It allocates radio frequencies, for example, to minimize co-channel interference and encourage the manufacture of radio equipment that can be sold and used internationally.

Check Your Progress 2

1) Two styles of information security policies are common:

- Individual policies covering specific security issues such as "E-mail security policy" and "Network access control policy". Typically these are quite formally worded and define security responsibilities of key groups, functions, teams or people. They may include introductions and explanations to aide reader comprehension, and should reference relevant documents at higher and lower levels of the policy hierarchy. They should be technology-neutral and succinct - ideally no more than a few pages.

- A comprehensive policy manual containing succinct policy statements reflecting the whole of ISO/IEC 27002, with numerous embedded cross-references between related policy statements and references to the related axioms, standards, procedures and guidelines. The manual functions as a master index for the entire policy suite, which helps avoid overlaps, gaps and (worst of all) conflicts.

Many organizations use both styles of policy. This is not an either-or situation.

2) It is difficult to recommend particular methods or tools without knowing more about any organization in terms of its experience with risk analysis and information security management, size/complexity, industry, ISMS maturity and so on. While ISO/IEC 27005 offers general advice on choosing and using information security risk analysis or assessment methods, the ISO27k standards do not specify any specific method, giving you the flexibility to select a method, or more likely several methods and/or tools, that suit your organization's requirements.

   Many different information security risk analysis methods and tools exist, in two main groups sharing broadly similar characteristics: the quantitative (mathematical) and qualitative (experiential) methods. None of them, not one, is explicitly required or recommended by the ISO27k standards which give some guidance but leave the choice of method/s down to users, depending on their requirements and factors such as their familiarity with certain methods.

   By the way, it is perfectly acceptable, advised even, for an organization to use multiple information security risk analysis methods. Some are more suited to particular situations than others - for example, it might make sense to use a simple high-level overview method to identify areas/aspects of concern, and then to change to other more detailed in-depth method/s to examine those particular areas/aspects more fully. Furthermore, some risk analysis methods are favored by audit, risk management, health and safety, penetration testing, application design and testing, contingency planning, and many other groups: there is no real benefit in stopping them using their favorite methods and tools just to conform to ISO27k. In fact, the differing

perspectives, experience and insight these methods/tools bring could prove very useful.

One thing to take care over, though, is how to resolve the inevitable discrepancies in the results from different methods. A crude policy such as "Pick whichever recommends the least costly controls and minimize only the obvious risks" is no better than "Pick the most comprehensive and minimize all the risks". The analyses are merely decision support tools to guide management, who still need to make the vital decisions about how much security investment is appropriate, how much risk can be tolerated, how much certainty is really needed in the decision process, and when to make any needed information security improvements.

2.6 SUGGESTED READINGS

- Edward Humphreys, *ISO/IEC 27001 for Small Businesses: Practical Advice*, Publisher: ISO/IEC, 2010.
- Krag Brotby, *Information Security Management Metrics,A Definitive Guide to Effective Security Monitoring and Measurement.*ISBN: 978-1-4200-5285-5 Publisher: Auerbach (CRC Press) in 2009.
- *Information Security Incident Management- A Methodology* by Neil Hare Brown, British Standards Institution, 2007

UNIT 3 SECURITY MECHANISM STANDARDS

Structure

3.0 INTRODUCTION

Security is a matter of great concern. To protect data and information different techniques are used by the organizations. Especially when the data in used on the internet and it moves in the cyber world from one compute to another computer crossing different geographical boundaries. There are chances of data theft on the way by some malicious users. To protect data against such threats the data protection is a must. There are some techniques like encryption and digital signature are used as security measures to cope up with security concerns. Here in this unit some techniques like encryption are used to provide the overview of how we can safeguard our data against such threats.

3.1 OBJECTIVES

After studying this unit, you should be able to understand:

- Encryption;
- Cryptography;
- Algorithm; and
- Digital Signature.

3.2 ENCRYPTION

Encryption is a process of changing information (plaintext) using an algorithm (cipher) to convert it into a form that is not readable to anyone except those

possessing special knowledge , referred to as key. By following the above mentioned process we obtain encrypted information (in cryptography referred to as ciphertext). In many contexts, the word encryption also implicitly refers to the reverse process, decryption (e.g. "software for encryption" can also perform decryption) to convert the encrypted piece of information into understandable format.

Encryption is not new, it has been in use since long, it was used by military and government to facilitate secret communication. Encryption is now commonly used in protecting information within many kinds of civilian systems. For example, the Computer Security Institute reported that in 2007, 71% of companies surveyed utilized encryption for some of their data in transit, and 53% utilized encryption for some of their data in storage. Encryption can be used to prevent data from loss, data which is "at rest" files such as files on computers and storage devices (e.g usb flash drive). In few recent years we have come across cases which involve theft of customer's personal data through the theft of laptops or backup drops. Encryption of such helps them to be protected. Digital rights management systems which prevent unauthorized use or reproduction of copyrighted material and protect software against reverse engineering (see also copy protection) are another somewhat different example of using encryption on data at rest.

The process of encryption also helps also has advantage in protecting data in transit , for example data being transferred via networks (e.g. the Internet , e-commerce), mobile phones , wireless microphones , wireless intercom systems , Bluetooth devices , and bank automatic teller machines .There have been numerous reports of data in transit being intercepted in recent years . Encryption helps to protect data.

Encryption can maintain the privacy of the message but still other techniques are required to protect the integrity and authenticity of the message. For example, verification of a message authentication code (MAC) or a digital signature. Many cryptographic software and hardware and standards are available but security is still a challenging problem .A single slip in system design can allow attacks to be successful. Sometimes an adversary can obtain unencrypted information without directly undoing the encryption

One of the earliest public key encryption applications was called Pretty Good Privacy (PGP). It was written in 1991 by Phil Zimmermann and was purchased by Symantec in 2010.

In order to avoid tampering we should make sure that the digital signature and encryption should be applied at the message creation time. Or else any node between the sender and the encryption agent could potentially tamper it. It has been seen that due to the manufacturer's ignorance, most mobile devices come without user – controlled encryption or digital signature capabilities.

3.3 CRYPTOGRAPHY

Cryptography can be defined as the practice and study of hiding information. Modern cryptography passes through the disciplines of mathematics, computer science, and electrical engineering .some of the applications of cryptography are ATM cards, computer passwords and electronic commerce.

The synonym of encryption, before the modern age was cryptology, the conversion of message from understandable form to non- understandable form.

The sender maintain the ability to decrypt the information therefore avoid unwanted person from reading it. Since the computer came into existence the methods for cryptography are becoming increasingly complex.

Modern cryptography is based on scientific approach, designs cryptographic algorithms around computational hardness assumptions, all this makes such algorithms hard to be broken by an adversary. Such systems are not unbreakable in theory but it is infeasible to do so by any practical means. Such schemes are secure. There exist information-theoretically secure schemes that provably cannot be broken—an example is the one-time pad--but these schemes are more difficult to implement than the theoretically breakable but computationally secure mechanisms. Cryptography has given rise to issues which are legal and some of them are still to be solved.

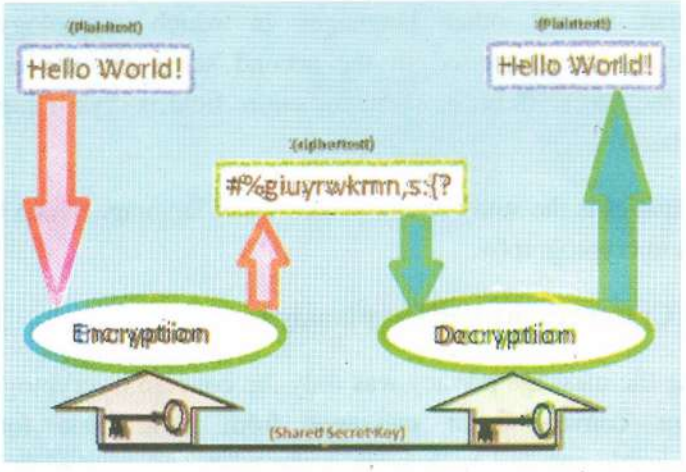


Fig. 1

Terminology

Cryptography was referred to encryption until modern times, which is the process of converting ordinary information (called plaintext) into unintelligible gibberish (called ciphertext). The opposite of encryption is decryption, in other words, converting from the unreadable ciphertext back to plaintext. A pair of algorithms that create the encryption and the reversing decryption is called as cipher. Algorithm and instance by a key both control the operation of cipher.

This is a secret parameter (ideally known only to the communicants) for a specific message exchange context. A "cryptosystem" is the ordered list of elements of finite possible plaintexts, finite possible cyphertexts, finite possible keys, and the encryption and decryption algorithms which correspond to each key. Keys form an important part, as ciphers without variable keys can be trivially broken with only the knowledge of the cipher used and are therefore useless (or even counter-productive) for most purposes. Historically, ciphers were often used directly for encryption or decryption without additional procedures such as authentication or integrity checks.

For conversational use, the term "code" is used to represent encryption or hiding the meaning. However if we talk of cryptography it has a more specific meaning. It means converting of a unit of plaintext with a code word. Codes are no longer used in serious cryptography—except incidentally for such things as unit designations if we properly choose the ciphers both serve to be more practical and secure than even best codes and better adapted computers.

Cryptanalysis is defined as study of methods for understanding the meaning of encrypted information without the access to key normally needed to do so.

Sometimes the terms cryptology and cryptography interchangeably used. While at many places the term cryptography is used to refer specifically to use and practice of techniques involving cryptography, and the combination of cryptography and cryptanalysis is termed as cryptology. English is more flexible than several other languages in which cryptology (done by cryptologists) is always used in the second sense above. In the English Wikipedia the general term used for the entire field is cryptography (done by cryptographers).

Cryptolinguistics is the study of characteristics of language which have some application in cryptography.

History of Cryptography and Cryptanalysis

Maintaining the message privacy was only the concern of cryptography before modern era—conversion of messages from a readable form into an incomprehensible one and back again at the other end, rendering it unreadable by interceptors or eavesdroppers without secret knowledge (namely the key needed for decryption of that message). The aim of encryption was to (attempt to) retain the secrecy in communications, such as those of spies, military leaders, and diplomats. But in the recent times the message integrity is also taken care of, sender/receiver identity authentication, digital signatures, interactive proofs and secure computation, among others.

clearly by Leon Battista Alberti around the year 1467, though there is some indication that it was already known to Al-Kindi. Alberti's innovation was to use different ciphers (i.e., substitution alphabets) for various parts of a message (perhaps for each successive plaintext letter at the limit). He also invented what was probably the first automatic cipher device, a wheel which implemented a partial realization of his invention. In the polyalphabetic Vigenère cipher, encryption uses a key word, which controls letter substitution depending on which letter of the key word is used. In the mid-19th century Charles Babbage showed that the Vigenère cipher was vulnerable to Kasiski examination, but this was first published about ten years later by Friedrich Kasiski.

Though frequency analysis is a powerful and general technique against many ciphers, encryption has still been often effective in practice; many a would-be cryptanalyst were not aware of the technique. Breaking a message without using frequency analysis essentially required knowledge of the cipher used and perhaps of the key involved, thus making espionage, bribery, burglary, defection, etc., more attractive approaches to the cryptanalytically uninformed. It was finally explicitly recognized in the 19th century that secrecy of a cipher's algorithm is not a sensible nor practical safeguard of message security; in fact, it was further realized that any adequate cryptographic scheme (including ciphers) should remain secure even if the adversary fully understands the cipher algorithm itself. Security of the key used should alone be sufficient for a good cipher to maintain confidentiality under an attack. This fundamental principle was first explicitly stated in 1883 by Auguste Kerckhoffs and is generally called Kerckhoffs's Principle; alternatively and more bluntly, it was restated by Claude Shannon, the inventor of information theory and the fundamentals of theoretical cryptography, as Shannon's Maxim—'the enemy knows the system'.

Many different types of physical devices and aids have been used to help with ciphers. One of the earliest may have been the scytale of ancient Greece, a rod supposedly used by the Spartans as an aid for a transposition cipher (see image above). In medieval times, other aids were invented such as the cipher grille, which was also used for a kind of steganography. With the invention of polyalphabetic ciphers came more sophisticated aids such as Alberti's own cipher disk, Johannes Trithemius' tabula recta scheme, and Thomas Jefferson's multi-cylinder (not publicly known, and reinvented independently by Bazeries around 1900). Early in the 20th century, many mechanical encryption/decryption devices were invented and several patented, among them rotor machines—famously including the Enigma machine used by the German government and military from the late '20s and during World War II. The ciphers implemented by better quality examples of these machine designs brought about a substantial increase in cryptanalytic difficulty after WWI.

The Computer Era

After the advent of digital computers and electronics after WWII made ciphers more complex. Furthermore, computers allowed for the encryption of any kind of data representable in any binary format, unlike classical ciphers which only encrypted written language texts; this was new and significant. The use of Computer has replaced language cryptography, both for cipher design and cryptanalysis. We can classify ciphers by their operation on binary bit sequences, unlike classical and mechanical schemes, which generally manipulate traditional characters (i.e., letters and digits) directly. However, computers have also assisted cryptanalysis, which has compensated to some extent for increased cipher complexity. Nonetheless, good modern ciphers have stayed ahead of cryptanalysis; it is typically the case that use of a quality cipher is very efficient, breaking cipher requires an effort that is many orders of magnitude larger, and vastly larger than that required for any classical cipher, making cryptanalysis inefficient and impractical as to be effectively impossible.

Credit card with smart-card capabilities- The 3-by-5-mm chip embedded in the card is enlarged. Smart cards combine low cost and portability with the power to compute cryptographic algorithms

Extensive open academic research on cryptography is relatively recent; it began only in the mid-1970s. In recent times, the algorithm designed by IBM personnel became the Federal (i.e. US) Data Encryption Standard; Whitfield Diffie and Martin Hellman published their key agreement algorithm, and the RSA algorithm was published in Martin Gardner's Scientific American column. Since then, cryptography is increasingly used in communications, computer networks, and computer security generally. Some modern cryptographic techniques can only keep their keys secret if certain mathematical problems are intractable, such as the integer factorization or the discrete logarithm problems, so there are deep connections with abstract mathematics. Still there are no sure proofs that a cryptographic technique is secure (but see one-time pad); at best, there are proofs that some techniques are secure if some computational problem is difficult to solve, or this or that assumption about implementation or practical use is met.

Inspite of being aware of cryptographic history, cryptographic algorithm and system designers must take into considerations of probable future developments while working on their designs. For instance, with the increased improvements in computer processing power, there is scope of brute-force attacks, so the length of key required also increases. The potential effects of quantum computing are already being considered by some cryptographic system designers; the announced imminence of small implementations of these machines may be making the need for this preemptive caution rather more than merely speculative.

Before 20th century, cryptography was chiefly concerned with language and editing patterns. Since then the emphasis has shifted, and cryptography now makes use of mathematics, including aspects of information theory, computational complexity, statistics, combinatorics, abstract algebra, number theory, and finite mathematics generally. Cryptography is a branch of engineering, but an unusual one as it deals with active, intelligent, and malevolent opposition (see cryptographic engineering and security engineering); other kinds of engineering (e.g., civil or chemical engineering) need deal only with neutral natural forces. There is also active research examining the relationship between cryptographic problems and quantum physics (see quantum cryptography and quantum computing).

Symmetric-Key Cryptography

In this type of cryptography the sender and the receiver both share the same key, such cryptography is known as symmetric – key cryptography. This was the only kind of encryption publicly known until June 1976.

The modern study of symmetric-key ciphers relates mainly to the study of block ciphers and stream ciphers and to their applications. A block cipher is, in a sense, a modern abstraction of Alberti's polyalphabetic cipher: block ciphers take as input a block of plaintext and a key, and output a block of ciphertext of the same size. Since the length of messages is longer than a single block, some method of combining together successive blocks is required. Several have been developed, some with better security in one aspect or another than others. They are the modes of operation and must be carefully considered when using a block cipher in a cryptosystem.

The Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) are block cipher designs which have been designated cryptography standards by the US government. Although its deprecation as an official standard, DES remains quite popular; it is used in a variety of applications, from ATM encryption to e-mail privacy and secure remote access. There are many other block ciphers designed and released, with some difference in quality. Many have been thoroughly broken, such as FEAL.

On the contrary stream ciphers, are the 'block' type, which create an arbitrarily long stream of key material, which is combined with the plaintext bit-by-bit or character-by-character, somewhat like the one-time pad. In a stream cipher, the cipher operates and changes the hidden internal state as output is generated. That internal state is initially set up using the secret key material. RC4 is a widely used stream cipher; see Category: Stream ciphers. Block ciphers can be used as stream ciphers; see Block cipher modes of operation

The third type of cryptographic algorithm consists of cryptographic hash functions. They take a message of any length as input, and output a short, fixed length hash which can be used in (for example) a digital signature. If the hash

function is good, an attacker cannot find two messages that produce the same hash. MD4 is a long-used hash function which is now broken; MD5, a strengthened variant of MD4, is also widely used but broken in practice. The U.S. National Security Agency developed the Secure Hash Algorithm series of MD5-like hash functions: SHA-0 was a flawed algorithm that the agency withdrew; SHA-1 is widely deployed and more secure than MD5, but cryptanalysts have identified attacks against it; the SHA-2 family improves on SHA-1, but it isn't yet widely deployed, and the U.S. standards authority thought it "prudent" from a security perspective to develop a new standard to "significantly improve the robustness of NIST's overall hash algorithm toolkit." Thus, a hash function design competition is underway and meant to select a new U.S. national standard, to be called SHA-3, by 2012.

Message authentication codes (MACs) are much like cryptographic hash functions, except that a secret key can be used to authenticate the hash value upon receipt.

Public-Key Cryptography

Symmetric-key cryptosystems use the same key for encryption and decryption of a message, though a message or group of messages may have a different key than others. But there is disadvantage of using symmetric ciphers, key management is necessary to use them securely. Each distinct pair of communicating parties must, ideally, share a different key, and perhaps each ciphertext exchanged as well. The number of keys required increases as the square of the number of network members, which very quickly requires complex key management schemes to keep them all straight and secret. The difficulty of securely establishing a secret key between two communicating parties, when a secure channel does not already exist between them, also presents a chicken-and-egg problem which is a considerable practical obstacle for cryptography users in the real world.

Whitfield Diffie and Martin Hellman, authors of the first published paper on public-key cryptography

In a groundbreaking 1976 paper, Whitfield Diffie and Martin Hellman proposed the notion of public-key (also, more generally, called asymmetric key) cryptography in which two different but mathematically related keys are used—a public key and a private key. A public key system is so constructed that calculation of one key (the 'private key') is computationally infeasible from the other (the 'public key'), even though they are necessarily related. Instead, both keys are generated secretly, as an interrelated pair. The historian David Kahn described public-key cryptography as "the most revolutionary new concept in the field since polyalphabetic substitution emerged in the Renaissance".

In public-key cryptosystems, the public key may be freely distributed, while its paired private key must remain secret. The public key is typically used for encryption, while the private or secret key is used for decryption. Diffie and Hellman showed that public-key cryptography was possible by presenting the Diffie–Hellman key exchange protocol.

In 1978, Ronald Rivest, Adi Shamir, and Len Adleman invented RSA, another public-key system. In 1997, it finally became publicly known that asymmetric key cryptography had been invented by James H. Ellis at GCHQ, a British intelligence organization, and that, in the early 1970s, both the Diffie–Hellman and RSA algorithms had been previously developed (by Malcolm J. Williamson and Clifford Cocks, respectively).

The Diffie–Hellman and RSA algorithms, in addition to being the first publicly known examples of high quality public-key algorithms, have been among the most widely used. Others include the Cramer–Shoup cryptosystem, ElGamal encryption, and various elliptic curve techniques. See Category: Asymmetric-key cryptosystems.

Padlock icon from the Firefox Web browser, was invented too indicate a page has been sent in SSL or TLS-encrypted protected form. Though, such an icon is not a guarantee of security; any subverted browser might mislead a user by displaying such an icon when a transmission is not actually being protected by SSL or TLS.

Digital signature schemes can be implemented using, public-key cryptography. A digital signature is reminiscent of an ordinary signature; they both have the characteristic that they are easy for a user to produce, but difficult for anyone else to imitate. Digital signatures can also be permanently attached to a content of the message being signed; they cannot then be 'moved' from one document to another, for any attempt will be traceable. In digital signature schemes, there are two algorithms: one for signing, in which a secret key is used to process the message and one for verification, in which the matching public key is used with the message to check the validity of the signature. RSA and DSA are two of the most popular digital signature schemes. Digital signatures are central to the operation of public key infrastructures and many network security schemes (e.g. SSL/TLS, many VPNs etc.).

Public-key algorithms are derived from the computational complexity of "hard" problems, often from number theory. For example, the hardness of RSA is related to the integer factorization problem, while Diffie–Hellman and DSA are related to the discrete logarithm problem. More recently, elliptic curve cryptography has developed in which security is based on number theoretic problems involving elliptic curves. Because of the difficulty of the underlying problems, most public-key algorithms involve operations such as modular multiplication and exponentiation, which are much more computationally

expensive than the techniques used in most block ciphers, especially with typical key sizes. As a result, public-key cryptosystems are commonly hybrid cryptosystems, in which a fast high-quality symmetric-key encryption algorithm is used for the message itself, while the relevant symmetric key is sent with the message, but encrypted using a public-key algorithm. Similarly, hybrid signature schemes are often used, in which a cryptographic hash function is computed, and only the resulting hash is digitally signed.

Cryptanalysis

Variants of the Enigma machine, used by Germany's military and civil authorities from the late 1920s through World War II, implemented a complex electro-mechanical polyalphabetic cipher. Breaking and reading of the Enigma cipher at Poland's Cipher Bureau, for 7 years before the war, and subsequent decryption at Bletchley Park, was important to Allied victory.

The aim of cryptanalysis is to find some shortcomings or insecurity in a cryptographic scheme, thus permitting its subversion or evasion.

It is very wrong to believe that every encryption method can be broken. In connection with his WWII work at Bell Labs, Claude Shannon proved that the one-time pad cipher is unbreakable, provided the key material is truly random, never reused, kept secret from all possible attackers, and of equal or greater length than the message. Most ciphers, apart from the one-time pad, can be broken with enough computational effort by brute force attack, but the amount of effort needed may be exponentially dependent on the key size, as compared to the effort needed to make use of the cipher. In such cases, security can be proved if the effort required (i.e., "work factor", in Shannon's terms) which is beyond the ability of any adversary. This means it must be shown that no efficient method (as opposed to the time-consuming brute force method) can be found to break the cipher. Since no such proof has been found till date, the one-time-pad remains the only theoretically unbreakable cipher.

Wide variety of cryptanalytic attacks are present, and they can be classified in any of several ways. A common distinction can be made by what an attacker knows and what capabilities are available. In a ciphertext-only attack, the cryptanalyst has access only to the ciphertext. In a known-plaintext attack, the cryptanalyst has access to a ciphertext and it s corresponding plaintext (or to many such pairs). In a chosen-plaintext attack, the cryptanalyst may choose a plaintext and learn its corresponding ciphertext (perhaps many times); an example is gardening, used by the British during WWII. Finally, in a chosen-ciphertext attack, the cryptanalyst may be able to choose ciphertexts and learn their corresponding plaintexts.

Poznań monument (center) to Polish cryptologists whose breaking of Germany's Enigma machine ciphers, beginning in 1932, altered the course of World War II.

Cryptanalysis of symmetric-key ciphers typically involves looking for attacks against the block ciphers or stream ciphers that are more efficient than any attack that could be against a perfect cipher. For example, a simple brute force attack against DES requires one known plaintext and 255 decryptions, trying approximately half of the possible keys, to reach a point at which chances are better than even the key sought will have been found. But this may not be enough assurance; a linear cryptanalysis attack against DES requires 243 known plaintexts and approximately 243 DES operations. This is a considerable improvement on brute force attacks.

Public-key algorithms are derived from the computational difficulty of various problems. The most famous of these is integer factorization (e.g., the RSA algorithm is based on a problem related to integer factoring), but the discrete logarithm problem is also important. Much public-key cryptanalysis concerns numerical algorithms for solving these computational problems, or some of them, efficiently (i.e., in a practical time). For instance, the best known algorithms for solving the elliptic curve-based version of discrete logarithm are much more time-consuming than the best known algorithms for factoring, at least for problems of more or less equivalent size. Thus, other things being equal, if we want an equivalent strength of attack resistance, factoring-based encryption techniques must use larger keys than elliptic curve techniques. For this reason, public-key cryptosystems based on elliptic curves have become popular since their invention in the mid-1990s.

While pure cryptanalysis uses weaknesses in the algorithms themselves, other attacks on cryptosystems are based on actual use of the algorithms in real devices, and are called side-channel attacks. If a cryptanalyst has access to, for example, the amount of time the device took to encrypt a number of plaintexts or report an error in a password or PIN character, he may be able to use a timing attack to break a cipher that is otherwise resistant to analysis. An attacker might also study the pattern and length of messages to derive valuable information; this is known as traffic analysis, and can be quite useful to an alert adversary. Poor administration of a cryptosystem, such as permitting too short keys, will make any system vulnerable, regardless of other virtues. And, of course, social engineering, and other attacks against the personnel who work with cryptosystems or the messages they handle (e.g., bribery, extortion, blackmail, espionage, torture ...) may be the most productive attacks of all.

Cryptographic Primitives

Much of the theoretical work in cryptography concerns cryptographic primitives—algorithms with basic cryptographic properties—and their relationship to other cryptographic problems. We can develop more complex cryptographic tools from the basic primitives. These primitives provide fundamental properties, which are used to develop more complex tools called cryptosystems or cryptographic protocols, which guarantee one or more high-

level security properties. Note however, that the distinction between cryptographic primitives and cryptosystems, is quite arbitrary; for example, the RSA algorithm is sometimes considered a cryptosystem, and sometimes a primitive. Typical examples of cryptographic primitives include pseudorandom functions, one-way functions, etc.

Cryptosystems

One or more cryptographic primitives are often used to develop a more complex algorithm, called a cryptographic system, or cryptosystem. Cryptosystems (e.g. El-Gamal encryption) are designed to provide particular functionality (e.g. public key encryption) while guaranteeing certain security properties (e.g. chosen-plaintext attack (CPA) security in the random oracle model). Cryptosystems use the properties of the underlying cryptographic primitives to support the system's security properties. Of course, as the distinction between primitives and cryptosystems is somewhat arbitrary, a sophisticated cryptosystem can be derived from a combination of several more primitive cryptosystems. In many cases, the cryptosystem's structure involves back and forth communication among two or more parties in space (e.g., between the sender of a secure message and its receiver) or across time (e.g., cryptographically protected backup data). Such cryptosystems are sometimes called cryptographic protocols.

Some widely known cryptosystems include RSA encryption, Schnorr signature, El-Gamal encryption, PGP, etc. More complex cryptosystems include electronic cash systems, signcryption systems, etc. Some more 'theoretical' cryptosystems include interactive proof systems, (like zero-knowledge proofs,), systems for secret sharing etc.

Until recently, most security properties of most cryptosystems were demonstrated using empirical techniques, or using ad hoc reasoning. Recently, there has been considerable effort to develop formal techniques for establishing the security of cryptosystems; this has been generally called provable security. The general idea of provable security is to give arguments about the computational difficulty needed to compromise some security aspect of the cryptosystem (i.e., to any adversary).

The study of how best to implement and integrate cryptography in software applications is itself a distinct field; see: Cryptographic engineering and Security engineering.

Legal Issues

Prohibitions

Intelligence gathering and law enforcement agencies find interest in cryptography. Secret communications may be criminal or even treasonous.

Because of its facilitation of privacy, and the diminution of privacy attendant on its prohibition, cryptography is also of considerable interest to civil rights supporters. But, there has been a lot of controversial legal issues surrounding cryptography, especially since the advent of inexpensive computers have made widespread access to high quality cryptography possible.

In some countries, even the domestic use of cryptography is, or has been, restricted. Until 1999, France significantly restricted the use of cryptography domestically, though it has relaxed many of these. In China, a license is still required to use cryptography. Many countries have tight restrictions on the use of cryptography. Among the more restrictive are laws in Belarus, Kazakhstan, Mongolia, Pakistan, Singapore, Tunisia, and Vietnam.

In the United States, cryptography is legal for domestic use, but there has been much conflict over legal issues related to cryptography. One particularly important issue has been the export of cryptography and cryptographic software and hardware. Probably because of the importance of cryptanalysis in World War II and an expectation that cryptography would continue to be important for national security, many Western governments have, at some point, strictly regulated export of cryptography. After World War II, it was illegal in the US to sell or distribute encryption technology overseas; in fact, encryption was designated as auxiliary military equipment and put on the United States Munitions List. Until the development of the personal computer, asymmetric key algorithms (i.e., public key techniques), and the Internet, this was not especially problematic. However, as the Internet grew and computers became more widely available, high quality encryption techniques became well-known around the globe. As a result, export controls came to be seen to be an impediment to commerce and to research.

Export Controls

In the 1990s, there were several challenges to US export regulations of cryptography. One involved Philip Zimmermann's Pretty Good Privacy (PGP) encryption program; it was released in the US, together with its source code, and found its way onto the Internet in June 1991. After a complaint by RSA Security (then called RSA Data Security, Inc., or RSADSI), Zimmermann was criminally investigated by the Customs Service and the FBI for several years. No charges were ever filed, however. Also, Daniel Bernstein, then a graduate student at UC Berkeley, brought a lawsuit against the US government challenging some aspects of the restrictions based on free speech grounds. The 1995 case Bernstein v. United States ultimately resulted in a 1999 decision that printed source code for cryptographic algorithms and systems was protected as free speech by the United States Constitution.

In 1996, thirty-nine countries signed the Wassenaar Arrangement, an arms control treaty that deals with the export of arms and "dual-use" technologies

such as cryptography. The treaty stipulated that the use of cryptography with short key-lengths (56-bit for symmetric encryption, 512-bit for RSA) would no longer be export-controlled. Cryptography exports from the US are now much less strictly regulated than in the past as a consequence of a major relaxation in 2000; there are no longer very many restrictions on key sizes in US-exported mass-market software. In practice today, since the relaxation in US export restrictions, and because almost every personal computer connected to the Internet, everywhere in the world, includes US-sourced web browsers such as Firefox or Internet Explorer, almost every Internet user worldwide has access to quality cryptography (i.e., when using sufficiently long keys with properly operating and unsubverted software, etc.) in their browsers; examples are Transport Layer Security or SSL stack. The Mozilla Thunderbird and Microsoft Outlook E-mail client programs similarly can connect to IMAP or POP servers via TLS, and can send and receive email encrypted with S/MIME. Many Internet users don't realize that their basic application software contains such extensive cryptosystems. These browsers and email programs are so ubiquitous that even governments whose intent is to regulate civilian use of cryptography generally don't find it practical to do much to control distribution or use of cryptography of this quality, so even when such laws are in force, actual enforcement is often effectively impossible.

NSA Involvement

Another contentious issue connected to cryptography in the United States is the influence of the National Security Agency on cipher development and policy. NSA was involved with the design of DES during its development at IBM and its consideration by the National Bureau of Standards as a possible Federal Standard for cryptography. DES was designed to be resistant to differential cryptanalysis, a powerful and general cryptanalytic technique known to NSA and IBM that became publicly known only when it was rediscovered in the late 1980s. According to Steven Levy, IBM rediscovered differential cryptanalysis, but kept the technique secret at NSA's request. The technique became publicly known only when Biham and Shamir re-rediscovered and announced it some years later. The entire affair illustrates the difficulty of determining what resources and knowledge an attacker might actually have.

Another instance of NSA's involvement was the 1993 Clipper chip affair, an encryption microchip intended to be part of the Capstone cryptography-control initiative. Clipper was widely criticized by cryptographers for two reasons. The cipher algorithm was then classified (the cipher, called Skipjack, though it was declassified in 1998 long after the Clipper initiative lapsed). The secret cipher caused concerns that NSA had deliberately made the cipher weak in order to assist its intelligence efforts. The whole initiative was also criticized based on its violation of Kerckhoffs's Principle, as the scheme included a special escrow

key held by the government for use by law enforcement, for example in wiretaps.

Digital Rights Management

Cryptography is central to digital rights management (DRM), a group of techniques for technologically controlling use of copyrighted material, being widely implemented and deployed at the behest of some copyright holders. In 1998, American President Bill Clinton signed the Digital Millennium Copyright Act (DMCA), which criminalized all production, dissemination, and use of certain cryptanalytic techniques and technology (now known or later discovered); specifically, those that could be used to circumvent DRM technological schemes. This had a noticeable impact on the cryptography research community since an argument can be made that any cryptanalytic research violated, or might violate, the DMCA. Similar statutes have since been enacted in several countries and regions, including the implementation in the EU Copyright Directive. Similar restrictions are called for by treaties signed by World Intellectual Property Organization member-states.

The United States Department of Justice and FBI have not enforced the DMCA as rigorously as had been feared by some, but the law, nonetheless, remains a controversial one. Niels Ferguson, a well-respected cryptography researcher, has publicly stated that he will not release some of his research into an Intel security design for fear of prosecution under the DMCA. Both Alan Cox (longtime number 2 in Linux kernel development) and Professor Edward Felten (and some of his students at Princeton) have encountered problems related to the Act. Dmitry Sklyarov was arrested during a visit to the US from Russia, and jailed for five months pending trial for alleged violations of the DMCA arising from work he had done in Russia, where the work was legal. In 2007, the cryptographic keys responsible for Blu-ray and HD DVD content scrambling were discovered and released onto the Internet. In both cases, the MPAA sent out numerous DMCA takedown notices, and there was a massive internet backlash triggered by the perceived impact of such notices on fair use and free speech.

3.4 THE NEED OF ALGORITHM

For a detailed presentation of the various points of view around the definition of "algorithm" see Algorithm characterizations. For examples of simple addition algorithms specified in the detailed manner described in Algorithm characterizations, see Algorithm examples.

An algorithm can be stated in simple words as "a set of rules that precisely defines a sequence of operations." For some people, a program is only an

algorithm if it stops eventually; for others, a program is only an algorithm if it stops before a given number of calculation steps.

A prototypical example of an algorithm is Euclid's algorithm to determine the maximum common divisor of two integers; an example (there are others) is described by the flow chart above and as an example in a later section.

Boolos & Jeffrey (1974, 1999) offer an informal meaning of the word in the following quotation:

No human being can write fast enough, or long enough, or small enough to list all members of an enumerably infinite set by writing out their names, one after another, in some notation. But humans can do something equally useful, in the case of certain enumerably infinite sets: They can give explicit instructions for determining the nth member of the set, for arbitrary finite n. Such instructions are to be given quite explicitly, in a form in which they could be followed by a computing machine, or by a human who is capable of carrying out only very elementary operations on symbols.

The term "enumerably infinite" means "countable using integers perhaps extending to infinity." Thus Boolos and Jeffrey are saying that an algorithm implies instructions for a process that "creates" output integers from an arbitrary "input" integer or integers that, in theory, can be chosen from 0 to infinity. Thus an algorithm can be an algebraic equation such as y = m + n—two arbitrary "input variables" m and n that produce an output y. But various authors' attempts to define the notion indicate that the word implies much more than this, something on the order of (for the addition example): Precise instructions for a fast, efficient, "good" process that specifies the "moves" of "the computer" (machine or human, equipped with the necessary internally contained information and capabilities) to find, decode, and then process arbitrary input integers/symbols m and n, symbols + and = ... and "effectively" produce, in a "reasonable" time, output-integer y at a specified place and in a specified format.

The concept of algorithm can be used to solve a problem and bring it to a decidable form. That notion is central for explaining how formal systems come into being starting from a small set of axioms and rules. In logic, the time an algorithm takes to complete cannot be measured, as it is not apparently related with our customary physical dimension. From such uncertainties, that characterize ongoing work, stems the unavailability of a definition of algorithm that suits both concrete (in some sense) and abstract usage of the term.

Legal Issues

Algorithms, by themselves, are not usually patentable. In the United States, a claim consisting solely of simple manipulations of abstract concepts, numbers, or signals does not constitute "processes" (USPTO 2006), and hence algorithms

are not patentable (as in Gottschalk v. Benson). However, practical applications of algorithms are sometimes patentable. For example, in Diamond v. Diehr, the application of a simple feedback algorithm to aid in the curing of synthetic rubber was deemed patentable. The patenting of software is highly controversial, and there are highly criticized patents involving algorithms, especially data compression algorithms, such as Unisys' LZW patent

Check Your Progress 1

Note: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

1) Write a note on cryptographic primitives.

.....

.....

.....

.....

2) Write a note on encryption.

.....

.....

.....

.....

3) Write a note on Symmetric key cryptography.

.....

.....

.....

.....

4) Write a note on legal issues of algorithm.

.....

.....

.....

.....

3.5 DIGITAL SIGNATURES

A digital signature scheme is a mathematical scheme for illustrating the genuineness of a digital message. A valid digital signature is one which gives recipient a reason to believe that the message was created by sender and it was not changed during the transmission. Some applications of digital signatures

are software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.

Digital signatures are often used to carry out electronic signatures, a broader term that refers to any electronic data that carries the significance of a signature, but not all electronic signatures use digital signatures. In some countries, including the United States, India, and members of the European Union, electronic signatures have legal significance. However, laws concerning electronic signatures do not always make clear whether they are digital cryptographic signatures in the sense used here, leaving the legal definition, and so their importance, somewhat confused.

Digital signatures make use of asymmetric cryptography. For instance if the messages are sent through a channel that is not secure, a properly carried digital signature gives the receiver a kind of surety to believe that the message was sent by the claimed sender. Digital signatures and handwritten signatures are somewhat are equivalent; properly implemented digital signatures are more difficult to forge than the handwritten type. Digital signature techniques which are used here are based on cryptography, and must be implemented properly to be effective. Digital signatures can also provide a way where in the signer cannot successfully claim they did not sign a message, and there private key remains secret; further, some non-repudiation schemes offer a time stamp for the digital signature, so that even if the private key is exposed, the signature is valid nonetheless. Digitally signed messages might be in the form of bitstring: some examples are electronic mail, contracts, or a message sent via some other cryptographic protocol.

A Digital signature scheme typically consists of three algorithms

- In a key generation algorithm a private key is uniformly selected at random from a set of possible private keys. The algorithm as a result produces the private key and a corresponding public key as output.
- In a signing algorithm, the given a message and a private key, produces a signature.
- In a signature verifying algorithm, a given message, where public key and a signature, either accepts or rejects the message's claim to authenticity.

There are two main properties which are required. Firstly, a signature generated from fixed message and fixed private key should verify the authenticity of that message by using the corresponding public key. Secondly, it should be impossible for a third party to generate valid signature who does not have a private key.

Uses of Digital Signatures

As we know that organizations are moving away from paper documents with ink signatures or authenticity stamps, digital signatures can assure the evidence of the origin, identity, and status of an electronic document as well as acknowledging informed consent and approval by a signatory. The United States Government Printing Office (GPO) publishes electronic versions of the budget, public and private laws, and congressional bills with digital signatures. Universities including Penn State, University of Chicago, and Stanford are publishing electronic student transcripts with digital signatures.

Following are some reasons for applying digital signatures to communications:

Authentication

Though the messages might contain the information regarding the entity sending a message, that information may not be consistent. Digital signatures can be used to validity of the sources of messages. The ownership of a digital signature secret key is with a specific user, the authenticity of the signature shows that the message was sent by that user. The importance of high confidence in sender authenticity is especially obvious in a financial context. For example, suppose a bank's branch office sends instructions to the central office requesting a change in the balance of an account. If the central office is not convinced that such a message is truly sent from an authorized source, acting on such a request could be a grave mistake.

Integrity

In many cases, it is required that the sender and receiver of a message may have a need for confidence that the message has not been modified during transit. As we know that encryption abstracts the contents of a message, still it may be possible to alter an encrypted message without understanding it. However, if once the message is digitally signed, any modification in the message after signature will not be valid. Furthermore, it is computationally impossible to modify a message and its signature to produce a new message with a valid signature.

Non-repudiation

Non-repudiation, or more specifically non-repudiation of origin, is an important aspect of digital signatures. By this property we mean that if an entity has signed some information, so it cannot deny it at a later time that it had signed it. Similarly, access to the public key only does not enable a cheater party to imitate a valid signature.

Using digital signatures only with trusted applications

One of the main distinction between a digital signature and a written signature is that the user does not "see" what he signs. The user application presents a hash code to be encrypted by the digital signing algorithm using the private key. An attacker who gains control over the user's PC can possibly substitute the user application with a foreign substitute, in effect replacing the user's own communications with those of the attacker. This could allow a malicious application to trick a user into signing any document by displaying the user's original on-screen, but presenting the attacker's own documents to the signing application.

As a protection against such cases, a validation system can be set up between the user's application and the signing application. The aim behind this idea is to provide some method by which both the user app and signing app must verify each other's integrity. For example, the signing application may require all requests to come from digitally-signed binaries.

WYSIWYS

On a Technical point of view, a digital signature applies to a string of bits, whereas humans and applications "believe" that they sign the semantic interpretation of those bits. In order to be semantically interpreted the bit string must be modified to a form that is meaningful for humans and applications, and this is achieved through a combination of hardware and software based processes on a computer system. The problem is that the semantic interpretation of bits can change as a function of the processes used to transform the bits into semantic content. It is however comparatively easy to modify the interpretation of a digital document by implementing changes on the computer system where the document is being processed. From a semantic perspective this creates uncertainty about what exactly has been signed. WYSIWYS (What You See Is What You Sign) means that the semantic interpretation of a signed message cannot be changed. In particular this also means that a message cannot contain hidden info that the signer is unaware of, and that can be revealed after the signature has been applied. WYSIWYS is a desirable property of digital signatures that is difficult to guarantee because of the increasing complexity of modern computer systems.

Digital Signatures vs. Ink on Paper Signatures

As we know that an ink signature can be easily duplicated from one document to another by imitating the image manually or digitally. While Digital signatures use cryptography to bind an electronic identity to an electronic document and the digital signature cannot be copied to another document. Paper contracts consist of ink signature block on the last page, and the previous pages may be replaced after a signature is applied. Digital signatures are

applied to entire document, such that the digital signature on the last page will indicate tampering if any data on any of the pages have been altered.

Need of Digital Signature

Companies all over the globe spend millions of dollars every year in automating their operations and business processes. As a result, electronic documentation permeates every aspect of the business workflow in industries ranging from engineering and healthcare to government and life sciences. Despite this, a hard copy is also printed when a signature authorization is required on a document, requiring physical routing for signatures. And This reintroduction of paper into the workflow increases organizational costs, increases time, and resists an organization from realizing the true benefits of a fully electronic workflow.

Digital signature generates a legally enforceable electronic record, by finishing the gap in going fully paperless by completely eliminating the need to print documents for signing. Digital signatures provide benefits by enabling the replacement of slow and expensive paper-based approval processes with fast, low-cost, and fully digital ones.

Check Your Progress 2

Note: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

1) Write a note on Digital signature.

.....

.....

.....

.....

2) What do you understand by non repudiation?

.....

.....

.....

.....

3) Write a note on WYSIWYS.

.....

.....

.....

.....

4) Write a note on need of digital signature.

.....

.....

.....

.....

3.6 SOME DIGITAL SIGNATURE ALGORITHMS

- RSA-based signature schemes, such as RSA-PSS
- DSA and its elliptic curve variant ECDSA
- ElGamal signature scheme as the predecessor to DSA, and variants Schnorr signature and Pointcheval–Stern signature algorithm
- Rabin signature algorithm
- Pairing-based schemes such as BLS
- Undeniable signatures
- Aggregate signature - a signature scheme that supports aggregation: Given n signatures on n messages from n users, it is possible to aggregate all these signatures into a single signature whose size is constant in the number of users. This single signature will convince the verifier that the n users did indeed sign the n original messages.

DSA

The Digital Signature Algorithm (DSA) is a United States Federal Government standard or FIPS for digital signatures. It was proposed by the National Institute of Standards and Technology (NIST) in August 1991 for use in their Digital Signature Standard (DSS), specified in FIPS 186, adopted in 1993. A minor revision was issued in 1996 as FIPS 186-1. The standard was expanded further in 2000 as FIPS 186-2 and again in 2009 as FIPS 186-3.

DSA is covered by U.S. Patent 5,231,668, filed July 26, 1991, and attributed to David W. Kravitz, a former NSA employee. This patent was given to "The United States of America as represented by the Secretary of Commerce, Washington, D.C." and the NIST has made this patent available worldwide royalty-free. Dr. Claus P. Schnorr claims that his U.S. Patent 4,995,082 (expired) covered DSA; this claim is disputed. DSA is a variant of the ElGamal Signature Scheme.

ElGamal Signature Scheme

The ElGamal signature scheme is a digital signature scheme which is based on the difficulty of computing discrete logarithms. It was described by Taher ElGamal in 1984.

The ElGamal signature algorithm described in this article is rarely used in practice. A variant developed at NSA and known as the Digital Signature Algorithm is much more widely used. There are several other variants. The ElGamal signature scheme must not be confused with ElGamal encryption which was also invented by Taher ElGamal.

The ElGamal signature scheme allows that a verifier can confirm the authenticity of a message m sent by the signer sent to him over an insecure channel.

Rabin Signature Scheme

In cryptography the Rabin Signature Scheme is a method of Digital signature which was originally proposed by Michael O. Rabin in 1979. The Rabin Signature Scheme was one of the first digital signature schemes proposed, and it was the first to relate the hardness of forgery directly to the problem of integer factorization. Because of its simplicity and prominent role in early public key cryptography, the Rabin Signature Scheme is covered in most introductory courses on cryptography. The Rabin Signature Scheme is existentially unforgeable in the random oracle model assuming the integer factorization problem is intractable. The Rabin Signature Scheme is also closely related to the Rabin cryptosystem.

Boneh–Lynn–Shacham

In cryptography, the Boneh–Lynn–Shacham signature scheme allows a user to validate that a signer is authentic. The scheme uses a pairing function for validation and signatures are group elements in some elliptic curve. Working in an elliptic curve provides defense against index calculus attacks against allowing shorter signatures than FDH signatures. Signatures are often referred to as short signatures, BLS short signatures, or simply BLS signatures. The signature scheme is provably secure (that is, the scheme is existentially unforgeable under adaptive chosen-message attacks) assuming both the existence of random oracles and the intractability of the computational Diffie–Hellman problem.

Undeniable Signatures

Undeniable signatures are a form of digital signature invented by David Chaum and Hans van Antwerpen in 1989. They have two different features,

The validating process is interactive, so the signatory can put a limit on who can verify the signature. A disavowal protocol is a cryptographic protocol which allows them to determine whether a given signature is a forgery.

The first means that a signatory can permit only others who are authorized to access the document to verify their signature. If the document were to be leaked to a third party, the third party would be unable to verify that the signature is genuine. This is a designated verifier signature.

However, because of this property it means that the signatory may deny a signature which was valid. To prevent this, there is the second property, a method to prove that a given signature is a forgery.

Cryptographic Hash Function

A cryptographic hash function is preimage resistant and 2nd preimage resistant function which consists of a constant output which is used to generate the hashcode of a document to be signed. For a secure electronicsignatures a hash function must b collision – resistant, meaning that it is impossible to find two different documents having the same hashcode.

If there are advances in the computing technology or cryptography, these conditions will not be met and the hash function will be considered insecure which must be removed from list of approved hash functions.

Padding Methods

Few signature algorithms need a hashcode to be padded up to a certain block length used with a specific algorithm setting. However this document does not specify that it is necessary to have padding methods, but requires a padding method, if required by an algorithm, to meet certain requirements defined in the given normative references.

It is intended that further padding schemes will be added as and when they have been fully standardised. These include several methods based on ISO/IEC 9796-2, currently under review. The emsa-pss method is included as, despite not being finalised, it has been stable for a long time and is a good improvement to the emsa-pkcs1-v1_5 scheme.

Signature Algorithms

A signature algorithm is applied to the hashcode of the document to be signed to generate a signature with the SCD.

The algorithm to be applied for verification with the SVD must be given. Before a signature algorithm is applicable a complete set of approved parameters must be defined. It must be practically impossible to compute

the SCD from the SVD.

Check Your Progress 3

Note: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

1) Write a note on DSA.

.....

.....

.....

.....

2) Discuss Rabin signature scheme.

.....

.....

.....

.....

3) Discuss cryptographic hash function.

.....

.....

.....

.....

4) What is padding method?

.....

.....

.....

.....

3.7 LET US SUM UP

This unit is all about the security measures. After studying this unit learners will be able to understand security concerns. The techniques like encryption, cryptography and their role to provide security to the data and information are also covered. The role of algorithm is very important in security concern. That is also discussed and explained in this unit. The digital signature are very important in the security measurements in business world, thus are covered very well.

3.8 CHECK YOUR PROGRESS: THE KEY

Check Your Progress 1

1) **Cryptographic Primitives**

Much of the theoretical work in cryptography concerns cryptographic primitives—algorithms with basic cryptographic properties—and their relationship to other cryptographic problems. We can develop more complex cryptographic tools from the basic primitives. These primitives provide fundamental properties, which are used to develop more complex tools called cryptosystems or cryptographic protocols, which guarantee one or more high-level security properties. Note however, that the distinction between cryptographic primitives and cryptosystems, is quite arbitrary; for example, the RSA algorithm is sometimes considered a cryptosystem, and sometimes a primitive. Typical examples of cryptographic primitives include pseudorandom functions, one-way functions, etc.

2) **Encryption**

Encryption is a process of changing information (plaintext) using an algorithm (cipher) to convert it into a form that is not readable to anyone except those possessing special knowledge , referred to as key. By following the above mentioned process we obtain encrypted information (in cryptography referred to as ciphertext). In many contexts, the word encryption also implicitly refers to the reverse process, decryption (e.g. "software for encryption" can also perform decryption) to convert the encrypted piece of information into understandable format.

Encryption is not new, it has been in use since long, and it was used by military and government to facilitate secret communication. Encryption is now commonly used in protecting information within many kinds of civilian systems. For example, the Computer Security Institute reported that in 2007, 71% of companies surveyed utilized encryption for some of their data in transit, and 53% utilized encryption for some of their data in storage. Encryption can be used to prevent data from loss, data which is "at rest" files such as files on computers and storage devices (e.g usb flash drive). In few recent years we have come across cases which involve theft of customer's personal data through the theft of laptops or backup drops. Encryption of such helps them to be protected. Digital rights management systems which prevent unauthorized use or reproduction of copyrighted material and protect software against reverse engineering (see also copy protection) are another somewhat different example of using encryption on data at rest.

The process of encryption also helps also has advantage in protecting data in transit , for example data being transferred via networks (e.g. the Internet , e-commerce), mobile phones , wireless microphones , wireless intercom systems , Bluetooth devices , and bank automatic teller machines .There have been numerous reports of data in transit being intercepted in recent years . Encryption helps to protect data.

Encryption can maintain the privacy of the message but still other techniques are required to protect the integrity and authenticity of the message. For example, verification of a message authentication code (MAC) or a digital signature. Many cryptographic software and hardware and standards are available but security is still a challenging problem .A single slip in system design can allow attacks to be successful. Sometimes an adversary can obtain unencrypted information without directly undoing the encryption

One of the earliest public key encryption applications was called Pretty Good Privacy (PGP). It was written in 1991 by Phil Zimmermann and was purchased by Symantec in 2010.

In order to avoid tampering we should make sure that the digital signature and encryption should be applied at the message creation time. Or else any node between the sender and the encryption agent could potentially tamper it. It has been seen that due to the manufacturer's ignorance, most mobile devices come without user – controlled encryption or digital signature capabilities.

3) **Symmetric key cryptography**

In this type of cryptography the sender and the receiver both share the same key, such cryptography is known as symmetric – key cryptography. This was the only kind of encryption publicly known until June 1976.

The modern study of symmetric-key ciphers relates mainly to the study of block ciphers and stream ciphers and to their applications. A block cipher is, in a sense, a modern abstraction of Alberti's polyalphabetic cipher: block ciphers take as input a block of plaintext and a key, and output a block of ciphertext of the same size. Since the length of messages is longer than a single block, some method of combining together successive blocks is required. Several have been developed, some with better security in one aspect or another than others. They are the modes of operation and must be carefully considered when using a block cipher in a cryptosystem.

The Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) are block cipher designs which have been designated cryptography standards by the US government. Although its deprecation as an official standard, DES remains quite popular; it is used in a variety of

applications, from ATM encryption to e-mail privacy and secure remote access. There are many other block ciphers designed and released, with some difference in quality. Many have been thoroughly broken, such as FEAL.

On the contrary stream ciphers, are the 'block' type, which create an arbitrarily long stream of key material, which is combined with the plaintext bit-by-bit or character-by-character, somewhat like the one-time pad. In a stream cipher, the cipher operates and changes the hidden internal state as output is generated. That internal state is initially set up using the secret key material. RC4 is a widely used stream cipher; see Category: Stream ciphers. Block ciphers can be used as stream ciphers; see Block cipher modes of operation

The third type of cryptographic algorithm consists of cryptographic hash functions. They take a message of any length as input, and output a short, fixed length hash which can be used in (for example) a digital signature. If the hash function is good, an attacker cannot find two messages that produce the same hash. MD4 is a long-used hash function which is now broken; MD5, a strengthened variant of MD4, is also widely used but broken in practice. The U.S. National Security Agency developed the Secure Hash Algorithm series of MD5-like hash functions: SHA-0 was a flawed algorithm that the agency withdrew; SHA-1 is widely deployed and more secure than MD5, but cryptanalysts have identified attacks against it; the SHA-2 family improves on SHA-1, but it isn't yet widely deployed, and the U.S. standards authority thought it "prudent" from a security perspective to develop a new standard to "significantly improve the robustness of NIST's overall hash algorithm toolkit." Thus, a hash function design competition is underway and meant to select a new U.S. national standard, to be called SHA-3, by 2012.

Message authentication codes (MACs) are much like cryptographic hash functions, except that a secret key can be used to authenticate the hash value upon receipt.

4) **Legal issues of algorithm**

Algorithms, by themselves, are not usually patentable. In the United States, a claim consisting solely of simple manipulations of abstract concepts, numbers, or signals does not constitute "processes" (USPTO 2006), and hence algorithms are not patentable (as in Gottschalk v. Benson). However, practical applications of algorithms are sometimes patentable. For example, in Diamond v. Diehr, the application of a simple feedback algorithm to aid in the curing of synthetic rubber was deemed patentable. The patenting of software is highly controversial, and there are highly criticized patents

involving algorithms, especially data compression algorithms, such as Unisys' LZW patent

Check Your Progress 2

1) **Digital Signature**

A digital signature scheme is a mathematical scheme for illustrating the genuineness of a digital message. A valid digital signature is one which gives recipient a reason to believe that the message was created by sender and it was not changed during the transmission. Some applications of digital signatures are software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.

Digital signatures are often used to carry out electronic signatures, a broader term that refers to any electronic data that carries the significance of a signature, but not all electronic signatures use digital signatures. In some countries, including the United States, India, and members of the European Union, electronic signatures have legal significance. However, laws concerning electronic signatures do not always make clear whether they are digital cryptographic signatures in the sense used here, leaving the legal definition, and so their importance, somewhat confused.

2) Non-repudiation, or more specifically non-repudiation of origin, is an important aspect of digital signatures. By this property we mean that if an entity has signed some information, so it cannot deny it at a later time that it had signed it. Similarly, access to the public key only does not enable a cheater party to imitate a valid signature.

3) **WYSIWYS**

On a Technical point of view, a digital signature applies to a string of bits, whereas humans and applications "believe" that they sign the semantic interpretation of those bits. In order to be semantically interpreted the bit string must be modified to a form that is meaningful for humans and applications, and this is achieved through a combination of hardware and software based processes on a computer system. The problem is that the semantic interpretation of bits can change as a function of the processes used to transform the bits into semantic content. It is however comparatively easy to modify the interpretation of a digital document by implementing changes on the computer system where the document is being processed. From a semantic perspective this creates uncertainty about what exactly has been signed. WYSIWYS (What You See Is What You Sign) means that the semantic interpretation of a signed message cannot be changed. In particular this also means that a message cannot contain hidden info that the signer is unaware of, and that can be revealed after the signature has been applied. WYSIWYS is a desirable property of digital

signatures that is difficult to guarantee because of the increasing complexity of modern computer systems.

4) Companies all over the globe spend millions of dollars every year in automating their operations and business processes. As a result, electronic documentation permeates every aspect of the business workflow in industries ranging from engineering and healthcare to government and life sciences. Despite this, a hard copy is also printed when a signature authorization is required on a document, requiring physical routing for signatures. And this reintroduction of paper into the workflow increases organizational costs, increases time, and resists an organization from realizing the true benefits of a fully electronic workflow. Digital signature generates a legally enforceable electronic record, by finishing the gap in going fully paperless by completely eliminating the need to print documents for signing. Digital signatures provide benefits by enabling the replacement of slow and expensive paper-based approval processes with fast, low-cost, and fully digital ones.

Check Your Progress 3

1) DSA

The Digital Signature Algorithm (DSA) is a United States Federal Government standard or FIPS for digital signatures. It was proposed by the National Institute of Standards and Technology (NIST) in August 1991 for use in their Digital Signature Standard (DSS), specified in FIPS 186, adopted in 1993. A minor revision was issued in 1996 as FIPS 186-1. The standard was expanded further in 2000 as FIPS 186-2 and again in 2009 as FIPS 186-3.

DSA is covered by U.S. Patent 5,231,668, filed July 26, 1991, and attributed to David W. Kravitz, a former NSA employee. This patent was given to "The United States of America as represented by the Secretary of Commerce, Washington, D.C." and the NIST has made this patent available worldwide royalty-free. Dr. Claus P. Schnorr claims that his U.S. Patent 4,995,082 (expired) covered DSA; this claim is disputed. DSA is a variant of the ElGamal Signature Scheme.

2) In cryptography the Rabin Signature Scheme is a method of Digital signature which was originally proposed by Michael O. Rabin in 1979. The Rabin Signature Scheme was one of the first digital signature schemes proposed, and it was the first to relate the hardness of forgery directly to the problem of integer factorization. Because of its simplicity and prominent role in early public key cryptography, the Rabin Signature Scheme is covered in most introductory courses on cryptography. The Rabin Signature Scheme is existentially unforgeable in the random oracle

model assuming the integer factorization problem is intractable. The Rabin Signature Scheme is also closely related to the Rabin cryptosystem.

3) A cryptographic hash function is preimage resistant and 2nd preimage resistant function which consists of a constant output which is used to generate the hashcode of a document to be signed. For a secure electronicsignatures a hash function must b collision – resistant, meaning that it is impossible to find two different documents having the same hashcode. If there are advances in the computing technology or cryptography, these conditions will not be met and the hash function will be considered insecure which must be removed from list of approved hash functions

   Few signature algorithms need a hashcode to be padded up to a certain block length used with a specific algorithm setting. However this document does not specify that it is necessary to have padding methods, but requires a padding method, if required by an algorithm, to meet certain requirements defined in the given normative references.

4) **Padding method**

   It is intended that further padding schemes will be added as and when they have been fully standardised. These include several methods based on ISO/IEC 9796-2, currently under review. The emsa-pss method is included as, despite not being finalised, it has been stable for a long time and is a good improvement to the emsa-pkcs1-v1_5 scheme

3.9 SUGGESTED READINGS

- https://incometaxindiaefiling.gov.in
- http://prismintl.org
- http://en.wikipedia.org
- http://www.bangor.ac.uk1
- http://www.sans.org
- www.arx.com
- www.youdzone.com

UNIT 4 SECURITY PROTOCOL STANDARDS

Structure

4.0 INTRODUCTION

During the early ages computer networks were used by researcher and limited number of people. So at that time no extra efforts were made towards the network securities. But now a days bulk of data is exchanged over the internet. So securities issues are very sensitive. Day by day network security is becoming very important as the amount of data exchanged on the internet is increasing. Although network security is a broad topic but in the simplest form it is concerned with making sure that unauthorized people cannot read, modified messages intended for other recipients. It is concerned with people trying to access remote serves that they are not authorized to use. Generally security is breeched by malicious people trying to gain some benefit to harm other bodies. While surfing on the internet people expect that their data should be secured. Data confidentiality and data integrity is expected by them. They

want to be able to identify the sender of the message. At the same time they want that they can prove that certain message is sent by a particular sender even if sender denies. On the basis of these points we can say that network security problems can be divided roughly into four areas.

1) Authentication
2) Integrity
3) Non repudiation
4) Privacy

Authentication

Authentication means that the receiver of the message is sure of the sender identity and no other person sends the information except the real sender. People can be authenticated by recognizing their faces, features, voices and handwriting, although messages may often include information about the entity sending a message, that information may not be accurate. Digital signatures can be used to authenticate the source of messages. When ownership of a digital signature secret key is bound to a specific user, a valid signature shows that the message was sent by that user. The importance of high confidence in sender authenticity is especially obvious in a financial context. For example, suppose a bank's branch office sends instructions to the central office requesting a change in the balance of an account. If the central office is not convinced that such a message is truly sent from an authorized source, acting on such a request could be a grave mistake.

Integrity

Data Integrity means that the data must arrive in the correct form to the receiver. No changes were made during the transmission either accidentally or maliciously. Data integrity becomes very crucial when very sensitive data is transmitted over the internet. So in a secure network data integrity must be preserved.In many scenarios, the sender and receiver of a message may have a need for confidence that the message has not been altered during transmission. Although encryption hides the contents of a message, it may be possible to change an encrypted message without understanding it. (Some encryption algorithms, known as nonmalleable ones, prevent this, but others do not.) However, if a message is digitally signed, any change in the message after signature will invalidate the signature. Furthermore, there is no efficient way to modify a message and its signature to produce a new message with a valid signature, because this is still considered to be computationally infeasible by most cryptographic hash functions.

Non repudiation

Non repudiation means that a receiver can prove that the received message came from a specific sender. In no case the sender can deny sending a message that is actually send by him. Non-repudiation, more specifically non-repudiation of origin, is an important aspect of digital signatures. By this property an entity that has signed some information cannot at a later time deny having signed it. Similarly, access to the public key only does not enable a fraudulent party to fake a valid signature.

Privacy

Privacy is also called confidentiality it means that the sender and the receiver believe in secrecy and unauthorized user can access the information transmitted over the net. The transmitted information should be available to the intended receiver only and to the others, information should be unclear. To maintain the privacy of the information, the message should be encrypted that is message should be ambiguous to the unauthorized user.

4.1 OBJECTIVES

After studying this unit, you should be able to:

- understand entity authentication protocols;
- explain key establishment; and
- explain time stamping.

4.2 ENTITY AUTHENTICATION PROTOCOLS

Security Issues and Authentication

Security is one place where the world of computation interacts with the physical world. Nothing proves this better than the fact that most security breaches in connection with computers are based on "social engineering" rather than flaws in encryption, access control or authentication algorithms. Hence, our first step in understanding authentication must be to understand the context in which authentication takes place. We will then examine the different mechanisms by which authentication is achieved and finally we will see how authentication can be translated into access and authorization.

4.2.1 The Context

In order to authenticate we must first grant anonymous access to a certain resource which has an immutable attribute. Authentication is the process of identifying the entity that has obtained access to this resource.

To justify this let us begin in the "distant" past when the only way in which multi-tasking multi-user systems were used was via terminals that were permanently attached to the computer. These terminals were placed in individual offices of the users. At this point authentication was not required since one could assume that only person with access to a specific office was a specific user. The user was identified by the resource she made use of. In this case the resource and its immutable attribute is the terminal which is an input/output device for the computer. The entity is identified by the physical access that the user has to the resource.

So what happens when user B walks into this user A's office and wants to use the computer from there? The solution is to introduce the username: prompt. Each terminal has a reset button. When this button is pressed the computer prompts the user to supply a name and then authenticates the user by the name supplied.

In this case the identification was based on the trust of the individual whose office is used by the second user; the system did not even ask for a password. However, when multi-user systems had terminals in public access areas passwords were required; at this point access to the terminal had truly become anonymous and thus some form of computer-based authentication was required.

Note that even in this case the computer had no control over the data that was flowing in via this terminal even before authentication had been performed. Thus the program login that monitored the logins had to handle this incoming data carefully otherwise there could be buffer overflow attacks, denial of service attacks and so on. Handling "tainted" data from an unauthenticated source is an important facet of all programs that deal with anonymous entities; e. g. authentication programs.

With network connectivity come, the possibility of the terminal not being attached to the computer directly but over an external wire. The immutable attribute that was algorithmically authenticated was now limited to a serial port. As usual, one must assume that the physical equipment—in this case the wire—was inviolable.

However, in practice it could be tapped or spliced. This became more serious when packet-switched networks were used in place of the external wire. The terminal oriented connection protocol or TCP was designed to provide an immutable attribute called a TCP socket. In this case establishing a TCP connection involved the creation of a software "socket" which is represented as a pair of pairs, where the pair consists of a hostid and a port. The authentication process then authenticates the socket.

However, this creation of a socket out of a packet-switched network protocol (IP) is quite problem-ridden and requires its own host-authentication methods.

In the past, simple host-authentication methods using IP addresses were considered sufficient. Nowadays there is a move towards securing the networks using SSL, IPSec or more general authentication techniques present in IPv6. In this case, there is low-level authentication via session-keys and other mechanisms that permeates the entire transaction in a manner that is mostly invisible to the user. Such techniques make use of immutable attributes that are mostly software; but one may ask "Can one really make something immutable out of software?" That we can is the legend of cryptographic authentication.

4.2.2 Mechanisms

As explained above the first authentication mechanism used is the just a "username" or IP address. Since the external entity provides this information at the time that it acquires anonymous access, it may or may not be reliable for identification depending on the physical context. So it is common to require additional proof. One of the standard mechanisms used is a password.

In the older contexts where the possibility of wire tapping or wire splicing was remote, such a password would be transmitted "in the clear" over the network. Nowadays, that is not considered particularly secure unless the channel is secured in some way. However, securing the channel requires some other authentication in order to prevent monkey-in-the-middle attacks. In either case we need to consider some form of authentication that does not involve the clear transmission of the password.

In spite of this, a number of systems around the world still use password-based authentication or something similar—like requiring the user to present a credit-card number or date of birth. Other than wire-tapping and replay attacks, this has other vulnerabilities. For example, user's often have the same password on all systems; if the "password" is biometric then this may not even be the user's choice! The information is "given away" by the user to the authenticating system—but not all systems that wish to authenticate you are reliable; e. g. we have seen a spate of "phishing" attacks. So what are the replacements for password based systems?

One way is to use a different password each time. In a "one-time-password" system a password can only be used once. The obvious difficulty with this system is how the user and the system decide on the sequence or list of passwords to be used. Another difficulty is that if the user does not verify the system that requests the password so this is still susceptible to "phishing" and monkey-in-the-middle even though the damage may be limited to one session. One significant advantage of this system is that the user is not required to do any computations unlike the systems being discussed below.

One way to generate the list of one-time-passwords is to use a secret generating secret. This second secret must be shared between the user and the service provider so we have "shared secret" systems. In this case the authenticating

system and the user have a shared secret. This secret can also be used to create some kind of time-stamped token which is exchanged as proof of possession of the shared secret; the actual secret is never exchanged across the wire. For example, we could take a cryptographic hash function and apply it to the concatenation of the current time, the local address and the shared secret; each party sends its own version of this across the wire. In such a system both the user and the system are sure of the identity of the other party (assuming the invulnerability of the cryptosystem used). One vulnerability is at the point where the shared secret is created and stored by the user and the system. Another vulnerability is due to the fact that today's user must interact with a number of different systems and so must keep a shared secret with each of these systems; the larger the amount of secret material to be stored the greater its vulnerability.

An alternative is the public-key system. Each user and each system that participate in the protocol publish the public-key component of a private-public pair. The cryptographic invulnerability of the cryptosystem will mean that only the entity which generated the public key can have the private key—unless that entity is compromised. Each party uses the private key to attach a "digital signature" to a concatenation of the current time and the local socket address; the other party can then verify the signature and thus authenticate the other party. A major vulnerability of this system is the difficulty of verifying that the public-key actually belongs to the entity whom one wants to authorize. Usually public-keys are exchanged at a "key-signing party" or via a tree or web of trust in order to circumvent this problem. Another vulnerability of this system is the requirement of significant computational resources for the creation and verification of digital signatures; this can be used to initiate a denial of service attack.

One way around this computational requirement is the "trusted third party" authentication system. In this case, there is a separate entity that everyone trusts and has significant computational resources dedicated to providing others with authentication information. An elaborate protocol called "Kerberos" has been developed that explains how a session may be securely initiated between parties who are individually known to this Authenticator. Each party expends some computational resources in obtaining recognition from the Authenticator but does not need to spend significant computational resources thereafter.

4.2.3 Applications

Once an input resource like a socket is authenticated then all data that comes in from that socket can be marked as coming from that particular authenticated source. The login application that we started with makes essentially only this use of the authentication. However, off late numerous other applications also make use of authentication; e. g. web servers. In all such cases it is important to distinguish between authentication and authorization.

The process that carries out the authentication transaction does not need to have access to too many system resources; in the case of password-based system it needs to have access only to the appropriate form of the password database. Thus the authenticator need not be a privileged process and can run with low privileges. In particular, compromise of the authenticator does not automatically grant access at all levels; all such a compromise can achieve is fake authentication.

On the other hand a process can only grant access to resources that it too has access to. Thus the authorizing process must have very wide access to the system. For example, the login process must run with "root" privileges after it has authenticated the user and is creating a shell process for a particular user. In a typical scenario, an application runs a number of sub-processes at lower privilege; one of these is the authentication process and the rest are authenticated processes. The latter processes run with the privilege level of the user who has been authorized by the authentication process. It is ideal if the top-level of the application limits its "job" to the creation of these processes as that simplifies its security analysis. Since this top-level is the authorizing process, its compromise would lead to a wide-ranging compromise of the system.

In practice one sees that monolithic programming is the norm and the kind of privilege separation that is recommended above is only slowly making its way into application programming. One can hope that this situation will improve as the different roles of authentication and authorization become clearer to programmers.

Security (cryptographic protocol or encryption protocol) is an abstract or concrete protocol that performs a security-related function and applies cryptographic methods. A protocol describes how algorithms should be used. A sufficiently detailed protocol includes details about data structures and representations, at which point it can be used to implement multiple, interoperable versions of programs. Cryptographic protocols are widely used for secure application-level data transport. **A cryptographic protocol** usually incorporates at least some of these aspects:

- Key agreement or establishment
- Entity Authentication
- Non-repudiation method

Entity authentication protocols verify the credibility of incoming messages from one network to another network. Techniques like cryptography and encryption are used to develop these protocols. The main aim behind the protocol development is to avoid hacking issues in many business industries such as finance and ecommerce.

4.2.4 LCMQ Entity Authentication Protocol

LCMQ Entity Authentication Protocol is a lightweight authentication protocol that filters the network packages and inspects the address in the back end. In large networks, the volume of messages is quite high to authenticate them. LCMQ is an advanced protocol that works on Object Oriented Concept. The algorithm of the protocol is based on a strong encryption method. It operates in multiple threads to inspect millions of messages in a single instance. It was developed on HB entity protocol standard. The protocol is a better solution in terms of storage expenses, cost of communication and overhead of tag computation.

4.2.5 ECC Entity Authentication Protocol

ECC Entity Authentication Protocol is a customized protocol to detect the error codes of authentication and propose solution accordingly. The protocol has a strong encryption algorithm and contributes significantly in authenticating the RFID packets and releasing the correct information across other networks. The protocol plays a significant role in boosting server security and reducing costs and network load with its lightweight structure. ECC analyzes the error codes and verifies the codes from its database to operate accordingly. The protocol can resend, reject, terminate and accept packets from other source.

4.2.6 3PAKE Entity Authentication Protocol

3PAKE Entity Authentication Protocol or three-party Password Exchange Protocol authenticates the two clients and assists in setting up a dedicated connection. The messages and all communications are held through a public-encrypted key based on latest security cryptographic standards. Through a password encrypted and authenticated by the protocol, the clients can more easily communicate between the two parties.

Check Your Progress 1

Note: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

1) What is non repudiation?

.....

.....

.....

.....

.....

2) Define the term Authentication.

.....

.....

.....

.....

.....

3) What is LCMQ Entity Authentication Protocol?

.....

.....

.....

.....

.....

4.3 KEY ESTABLISHMENT

Key establishment is a technique or a protocol using which a secret can be available to two or more parties, for subsequent cryptographic use. Key establishment may be broadly subdivided into two parts:-

- key transport
- key agreement

A **key transport protocol** or mechanisms is a key establishment technique where one party generates or obtains a secret value by some means, and securely transfers it to the other(s).

A **key agreement protocol** or mechanism is a key establishment technique in which a shared secret is derived by two (or more) parties as a function of information contributed by, or associated with, each of these, (ideally) such that no party can predetermine the resulting value. Key establishment protocols involving authentication typically require a set-up phase whereby authentic and possibly secret initial keying material is distributed. Most protocols have as an objective the creation of distinct keys on each protocol execution. In some cases, the initial keying material pre-defines a fixed key which will result every time the protocol is executed by a given pair or group of users. Systems involving such static keys are insecure under known-key attacks.

Besides this some Key pre-distribution schemes are key establishment protocols whereby the resulting established keys are completely determined a

priori by initial keying material. In contrast, dynamic key establishment schemes are those whereby the key established by a fixed pair (or group) of users varies on subsequent executions.

Dynamic key establishment is also referred to as session key establishment. In this case the session keys are dynamic, and it is usually intended that the protocols are immune to known-key attacks.

Many key establishment protocols involve a centralized or trusted party, for either or both initial system setup and on-line actions (i.e., involving real-time participation). This party is referred to by a variety of names depending on the role played, including: trusted third party, trusted server, authentication server, key distribution center (KDC), key translation center (KTC), and certification authority (CA).

4.3.1 Entity Authentication, Key Authentication

It is generally desired that each party in a key establishment protocol be able to determine the true identity of the other(s) which could possibly gain access to the resulting key, implying preclusion of any unauthorized additional parties from deducing the same key. In this case, the technique is said (informally) to provide secure key establishment. This requires both secrecy of the key, and identification of those parties with access to it. Furthermore, the identification requirement differs subtly, but in a very important manner, from that of entity authentication – here the requirement is knowledge of the identity of parties which may gain access to the key, rather than corroboration that actual communication has been established with such parties.

Key authentication is the property whereby one party is assured that no other party aside from a specifically identified second party (and possibly additional identified trusted parties) may gain access to a particular secret key. Key authentication is independent of the actual possession of such key by the second party, or knowledge of such actual possession by the first party; in fact, it need not involve any action whatsoever by the second party. For this reason, it is sometimes referred to more precisely as (implicit) key authentication. Key confirmation is the property whereby one party is assured that a second (possibly unidentified) party actually has possession of a particular secret key. Explicit key authentication is the property obtained when both (implicit) key authentication and key confirmation hold.

In the case of explicit key authentication, an identified party is known to actually possess a specified key, a conclusion which cannot otherwise be drawn. Encryption applications utilizing key establishment protocols which offer only implicit key authentication often begin encryption with an initial known data unit serving as an integrity check-word, thus moving the burden of key confirmation from the establishment mechanism to the application. The focus in key authentication is the identity of the second party rather than the

value of the key, whereas in key confirmation the opposite is true. Key confirmation typically involves one party receiving a message from second containing evidence demonstrating the latter's possession of the key. In practice, possession of a key may be demonstrated by various means, including producing a one-way hash of the key itself, use of the key in a (keyed) hash function, and encryption of a known quantity using the key. These techniques may reveal some information (albeit possibly of no practical consequence) about the value of the key itself; in contrast, methods using zero-knowledge techniques allow demonstration of possession of a key while providing no additional information (beyond that previously known) regarding its value.

Entity authentication is not a requirement in all protocols. Some key establishment protocols provide none of entity authentication, key authentication, and key confirmation. Unilateral key confirmation may always be added e.g., by including a one-way hash of the derived key in a final message.

In a key establishment protocol which involves entity authentication, it is critical that the protocol be constructed to guarantee that the party whose identity is thereby corroborated is the same party with which the key is established. When this is not so, an adversary may enlist the aid of an unsuspecting authorized party to carry out the authentication aspect, and then impersonate that party in key establishment

4.3.2 Assumptions and Adversaries in Key Establishment Protocols

To clarify the threats protocols may be subject to, and to motivate the need for specific protocol characteristics, one requires (as a minimum) an informal model for key establishment protocols, including an understanding of underlying assumptions. Attention here is restricted to two-party protocols, although the definitions and models may be generalized.

4.3.3 Adversaries in Key Establishment Protocols

Communicating parties or entities in key establishment protocols are formally called principals, and assumed to have unique names. In addition to legitimate parties, the presence of an unauthorized "third" party is hypothesized, which is given many names under various Circumstances, including: adversary, intruder, opponent, enemy, attacker, eavesdropper, and impersonator. When examining the security of protocols, it is assumed that the underlying cryptographic mechanisms used, such as encryption algorithms and digital signatures schemes, are secure. If otherwise, then there is no hope of a secure protocol. An adversary is hypothesized to be not a cryptanalyst attacking the underlying mechanisms directly, but rather one attempting to subvert the protocol objectives by defeating the manner in which such mechanisms are combined, i.e., attacking the protocol itself.

4.3.4 Secret Sharing

Secret sharing schemes are multi-party protocols related to key establishment. The original motivation for secret sharing was the following. To safeguard cryptographic keys from loss, it is desirable to create backup copies. The greater the number of copies made, the greater the risk of security exposure; the smaller the number, the greater the risk that all are lost. Secret sharing schemes address this issue by allowing enhanced reliability without increased risk. They also facilitate distributed trust or shared control for critical activities (e.g., signing corporate cheques; opening bank vaults), by gating the critical action on cooperation by t of n users. The idea of secret sharing is to start with a secret, and divide it into pieces called shares which are distributed amongst users such that the pooled shares of specific subsets of users allow reconstruction of the original secret. This may be viewed as a key pre-distribution technique, facilitating one-time key establishment, wherein the recovered key is pre-determined (static), and, in the basic case, the same for all groups. A secret sharing scheme may serve as a shared control scheme if inputs (shares) from two or more users are required to enable a critical action

4.3.5 Conference Keying

A **conference keying protocol** is a generalization of two-party key establishment to provide three or more parties with a shared secret key. Despite superficial resemblance, conference keying protocols differ from dynamic secret sharing schemes in fundamental aspects. General requirements for conference keying include that distinct groups recover distinct keys (session keys); that session keys are dynamic (excepting key pre-distribution schemes); that the information exchanged between parties is non-secret and transferred over open channels; and that each party individually computes the session key (vs. pooling shares in a black box). A typical application is telephone conference calls. The group able to compute a session key is called the privileged subset. When a central point enables members of a (typically large) privileged subset to share a key by broadcasting one or more messages, the process resembles pre-positioned secret sharing somewhat and is called broadcast encryption. An obvious method to establish a conference key K for a set of t _ 3 parties is to arrange that each party share a unique symmetric key with a common trusted party. Thereafter the trusted party may choose a new random key and distribute it by symmetric key transport individually to each member of the conference group. Disadvantages of this approach include the requirement of an on-line trusted third party, and the communication and computational burden on this party. A related approach not requiring a trusted party involves a designated group member (the chair) choosing a key K, computing pairwise Diffie-Hellman keys with each other group member, and using such keys to securely send K individually to each. A drawback of this

approach is the communication and computational burden on the chair, and the lack of protocol symmetry.

4.4 TIME STAMP

A **timestamp** is a sequence of characters, denoting the date and/or time at which a certain event occurred. It represents the time at which an event is recorded by a computer, not the time of the event itself. **Time stamping** is the process of safely keeping track of the creation and modification time of a document. Basically time stamping is needed to properly validate the signature. Time stamping should be used if the signature is supposed to be used in long term, i.e. longer than one or several days. But Time stamping is not necessary when we, for example, send a short signed note to the colleague and this note is expected to be read and disposed of the same day as it has been written. Of course, timestamping can not be used when it's not supported by the signing technologies or when timestamping authority is not available.

4.4.1 How Time Stamping Works?

Time stamping involves two components. The code to be time stamped is treated as time stamping client and a time stamping server called Time Stamping Authority (TSA).Firstly the code signs some data and then the hash of the data signature is calculated. This hash is sent to TSA for signing. TSA signs the received hash using TSA certificate and includes current time on the server to this signature. The signature made by TSA is sent back to the code and the code adds this signature to the original signature made over the initial data. TSA services are offered by the companies which issue digital certificates Besides this there exist local (national, governmental or private) time stamping authorities, but their usability is limited as they are usually offered as part of some closed infrastructure. For example, if the governmental agency or bank accepts digitally signed documents, it can offer the TSA for use with such documents, but this TSA will be only accepted and validated by this governmental agency or bank.

Fig. 1

It must be notice that as like any other signature, time stamping signature can become invalid if the time stamping certificate expired.

4.4.2 Importance of Time Stamp

The timestamp tells the entity, which validates the signature, when exactly the signature was made. As we know that the certificate is not everlasting. It has certain validity period, i.e. the certificate may only be used for it's purpose during some period of time. If we use the certificate, that has expired, to sign the data, such signature will not be accepted as valid. If the signature validator finds a timestamp, it will know when the signature was made, and will check if the certificate was valid at that moment of time. If there's no timestamp, then nobody knows, when the signature was made, and it's assumed that it could be made at any moment of time, possibly after the certificate has expired. There are two possible results from this situation: either the signature is claimed as not valid, or the signature is assumed to be made at the moment of validation. In the second case, if the signing certificate itself has expired by the moment of signature validation, the signature will not be accepted as valid too. And if the signature is expected to be validated somewhere in future, then it's likely that such problem will happen sooner or later. So if the signature is not time stamped properly, there are chances that it will not be accepted as valid.

4.4.3 Classification of Time Stamping

The idea of time stamping information was very old and it can be classified into a number of categories depending upon the objectives of security purpose.

- PKI-based - Timestamp
- Linking-based schemes
- Transient key scheme
- MAC - simple secret key based scheme

PKI Based Time Stamp

Here time stamp token is protected using a PKI digital signature. Firstly a hash is calculated from the given data. A hash is a sort of digital fingerprint of the original data: a string of bits that is different for each set of data. If the original data is changed then this will result in a completely different hash. This hash is sent to the Time stamping Authority (TSA). The TSA concatenates a timestamp to the hash and calculates the hash of this concatenation. This hash is in turn digitally signed with the private key of the TSA. This signed hash + the timestamp is sent back to the requester of the timestamp who stores these with the original data Since the original data can not be calculated from the hash, the TSA never gets to see the original data, which allows the use of this method for confidential data

Linking-Based Schemes

Linking-based time-stamping is a type of time stamping where issued time-stamps are related to each other.

This time-stamping creates time-stamp tokens which are dependent on each other, mixed into some authenticated data structure. Later modification of issued time-stamps would invalidate this structure. Temporal order of issued time-stamps is also protected by this data structure, making backdating of the issued time-stamps is impossible, even by the issuing server itself. Top of the authenticated data structure is generally published in some hard-to-modify and widely witnessed media like printed newspaper

Suitable candidates for authenticated data structure are:

- Linear hash chain,
- Hash tree
- Skip list.

The linking-based time-stamping authority (TSA) usually performs the following distinct functions:

Aggregation

For increased scalability TSA might group time-stamping requests arriving within a short timeframe. These requests will be aggregated together without retaining their temporal order and then assigned the same time value. Aggregation creates cryptographic connection between all involved requests; authenticating aggregate value will be used as input for the linking operation.

Linking

Linking creates verifiable and ordered cryptographic link between current and already issued time-stamp tokens.

Publishing

TSA publishes periodically some links, so that all previously issued time-stamp tokens depend on the published link and that it is practically impossible to forge the published values. By publishing widely witnessed links the TSA creates unforgeable verification points for validating all previously issued time-stamps.

Security Aspects

Linking-based time-stamping is more secure than the usual, public-key signature based time-stamping. All consequential time-stamps "seal" previously issued ones - hash chain, could be built only in one way; modifying

issued time-stamps is nearly as hard as finding a preimage for the used cryptographic hash function.

Linking-based time-stamping scales well - hashing is much faster than public key cryptography. There is no need for specific cryptographic hardware with its limitations.

Transient Key Scheme

In a transient-key system, private keys are used for a short period and then destroyed, that is why it is sometimes called "**disposable crypto**." Data encrypted with a private key associated with a specific time interval can be linked to that interval, making transient-key cryptography particularly useful for digital time stamping. In a transient-key system, the source of time must be a consistent standard understood by all senders and receivers. Since a local system clock may be changed by a user, it is never used as a source of time. Instead, data is digitally signed with a time value derived from Universal Coordinated Time (UTC) accurate to within a millisecond. Whenever a time interval in a transient-key system expires, a new public/private key pair is generated, and the private key from the previous interval is used to digitally certify the new public key. The old private key is then destroyed.

MAC - Simple Secret Key Based Scheme

A **message authentication code** (**MAC**) is a short piece of information used to authenticate a message. A MAC algorithm, sometimes called a **keyed** hash **function**, accepts as input a secret key and an arbitrary-length message to be authenticated, and outputs a MAC (sometimes known as a tag). The MAC value protects both a message's data integrity as well as its authenticity, by allowing verifiers to detect any changes to the message content.

Security Aspects

Although MAC functions are similar to cryptographic hash functions, but still they possess different security requirements. To be considered secure, a MAC function must resist existential forgery. This means that even if an attacker has an access to a document which possesses the secret key and generates MACs for messages, but the attacker cannot guess the MAC for other messages without performing infeasible amounts of computation.

MACs differ from digital signatures as MAC values are both generated and verified using the same secret key. This implies that the sender and receiver of a message must agree on the same key before initiating communications, as is the case with symmetric encryption. For the same reason, MACs do not provide the property of non-repudiation offered by signatures specifically in the case of a network-wide shared secret key: any user who can verify a MAC is also capable of generating MACs for other messages. In contrast, a digital

signature is generated using the private key of a key pair, which is asymmetric encryption. Since this private key is only accessible to its holder, a digital signature proves that a document was signed by none other than that holder. Thus, digital signatures do offer non-repudiation.

Check Your Progress 2

Note: a) Space is given below for writing your answer.

b) Compare your answer with the one given at the end of the Unit.

1) Define Key Establishment.

.....

.....

.....

.....

2) Define ECC Entity Authentication Protocol.

.....

.....

.....

.....

3) What do you mean by key agreement protocol?

.....

.....

.....

.....

4) What do you mean by Time Stamp?

.....

.....

.....

.....

5) Discuss the working of a Time Stamping.

.....

.....

.....

.....

6) What is PKI based Time Stamp?

.....

.....

.....

.....

7) Discuss linking based Time Stamping.

.....

.....

.....

.....

8) Discuss various security aspects of MAC.

.....

.....

.....

.....

4.5 LET US SUM UP

The most important issues to be considered in security are privacy, authentication, integrity and non repudiation. Privacy can be obtained by encryption of the plain text into cipher text. Authentication, integrity and non repudiation are achieved by using the digital signature. It covers entity authentication protocol, key establishment and time stamping technique. The study of security standard protocols is necessary for the security of sensitive information so that the authorized user can not access the sensitive data. In addition to this the entity authentication protocols are responsible for identifying the correct entity to whom and by whom the information is sent or received. At the same time with the help of these protocols a sender could not deny later, that the information was not send by him which was actually send by him. Using the concept of time stamping an eye can be kept at the time of development of a document. So in order to maintain the security issues, different techniques can be used so that the document should be authorized received without any tempering.

4.6 CHECK YOUR PROGRESS: THE KEY

Check Your Progress 1

1) Non-repudiation means that a receiver can prove that the received message came from a specific sender. In no case a sender can deny sending a message that is actually send by him. More specifically non-repudiation of origin is an important aspect of digital signatures. By this property an entity that has signed some information cannot at a later time deny having signed it. Similarly, access to the public key only does not enable a fraudulent party to fake a valid signature.

2) **Authentication** means that the receiver of the message is sure of the sender identity and no other person sends the information except the real sender. People can be authenticated by recognizing their faces, features, voices and handwriting, Aalthough messages may often include information about the entity sending a message, that information may not be accurate. Digital signatures can be used to authenticate the source of messages. When ownership of a digital signature secret key is bound to a specific user, a valid signature shows that the message was sent by that user. The importance of high confidence in sender authenticity is especially obvious in a financial context. For example, suppose a bank's branch office sends instructions to the central office requesting a change in the balance of an account. If the central office is not convinced that such a message is truly sent from an authorized source, acting on such a request could be a grave mistake.

3) **LCMQ Entity Authentication Protocol** is a lightweight authentication protocol that filters the network packages and inspects the address in the back end. In large networks, the volume of messages is quite high to authenticate them. LCMQ is an advanced protocol that works on Object Oriented Concept. The algorithm of the protocol is based on a strong encryption method. It operates in multiple threads to inspect millions of messages in a single instance. It was developed on HB entity protocol standard. The protocol is a better solution in terms of storage expenses, cost of communication and overhead of tag computation.

Check Your Progress 2

1) Key establishment is a technique or a protocol using which a secret can be available to two or more parties, for subsequent cryptographic use. Key establishment may be broadly subdivided into two parts

   - key transport
   - key agreement,

A **key transport protocol** or mechanisms is a key establishment technique where one party generates or obtains a secret value by some means, and securely transfers it to the other(s).

A **key agreement protocol** or mechanism is a key establishment technique in which a shared secret is derived by two (or more) parties as a function of information contributed by, or associated with, each of these, (ideally) such that no party can predetermine the resulting value.

2) **ECC Entity Authentication Protocol** is a customized protocol to detect the error codes of authentication and propose solution accordingly. The protocol has a strong encryption algorithm and contributes significantly in authenticating the RFID packets and releasing the correct information across other networks. The protocol plays a significant role in boosting server security and reducing costs and network load with its lightweight structure. ECC analyzes the error codes and verifies the codes from its database to operate accordingly. The protocol can resend, reject, terminate and accept packets from other source.

3) A **key agreement protocol** or mechanism is a key establishment technique in which a shared secret is derived by two (or more) parties as a function of information contributed by, or associated with, each of these, (ideally) such that no party can predetermine the resulting value. Key establishment protocols involving authentication typically require a set-up phase whereby authentic and possibly secret initial keying material is distributed. Most protocols have as an objective the creation of distinct keys on each protocol execution. In some cases, the initial keying material pre-defines a fixed key which will result every time the protocol is executed by a given pair or group of users. Systems involving such static keys are insecure under known-key attacks.

4) A **Time Stamp** is a sequence of characters, denoting the date and/or time at which a certain event occurred. It represents the time at which an event is recorded by a computer, not the time of the event itself. **Time stamping** is the process of safely keeping track of the creation and modification time of a document. Basically time stamping is needed to properly validate the signature. Time stamping should be used if the signature is supposed to be used in long term, i.e. longer than one or several days. But Time stamping is not necessary when we, for example, send a short signed note to the colleague and this note is expected to be read and disposed of the same day as it has been written. Of course, time stamping can not be used when it's not supported by the signing technologies or when time stamping authority is not available.

5) Time stamping involves two components. The code to be time stamped is treated as time stamping client and a time stamping server called Time

Stamping Authority (TSA).Firstly the code signs some data and then the hash of the data signature is calculated. This hash is sent to TSA for signing. TSA signs the received hash using TSA certificate and includes current time on the server to this signature. The signature made by TSA is sent back to the code and the code adds this signature to the original signature made over the initial data. TSA services are offered by the companies which issue digital certificates Besides this there exist local (national, governmental or private) time stamping authorities, but their usability is limited as they are usually offered as part of some closed infrastructure. For example, if the governmental agency or bank accepts digitally signed documents, it can offer the TSA for use with such documents, but this TSA will be only accepted and validated by this governmental agency or bank.

It must be notice that as like any other signature, time stamping signature can become invalid if the time stamping certificate expired.

6) Here time stamp token is protected using a PKI digital signature. Firstly a hash is calculated from the given data. A hash is a sort of digital fingerprint of the original data: a string of bits that is different for each set of data. If the original data is changed then this will result in a completely different hash. This hash is sent to the Time stamping Authority (TSA). The TSA concatenates a timestamp to the hash and calculates the hash of this concatenation. This hash is in turn digitally signed with the private key of the TSA. This signed hash + the timestamp is sent back to the requester of the timestamp who stores these with the original data Since the original data can not be calculated from the hash, the TSA never gets to see the original data, which allows the use of this method for confidential data.

7) **Linking-based time-stamping** is a type of time stamping where issued time-stamps are related to each other.

   This time-stamping creates time-stamp tokens which are dependent on each other, mixed into some authenticated data structure. Later modification of issued time-stamps would invalidate this structure. Temporal order of issued time-stamps is also protected by this data structure, making backdating of the issued time-stamps is impossible, even by the issuing server itself. Top of the authenticated data structure is generally published in some hard-to-modify and widely witnessed media like printed newspaper.

8) Although MAC functions are similar to cryptographic hash functions, but still they possess different security requirements. To be considered secure, a MAC function must resist existential forgery. This means that even if an attacker has an access to a document which possesses the secret key and generates MACs for messages, but the attacker cannot guess the MAC for

other messages without performing infeasible amounts of computation. MACs differ from digital signatures as MAC values are both generated and verified using the same secret key. This implies that the sender and receiver of a message must agree on the same key before initiating communications, as is the case with symmetric encryption. For the same reason, MACs do not provide the property of non-repudiation offered by signatures specifically in the case of a network-wide shared secret key: any user who can verify a MAC is also capable of generating MACs for other messages. In contrast, a digital signature is generated using the private key of a key pair, which is asymmetric encryption. Since this private key is only accessible to its holder, a digital signature proves that a document was signed by none other than that holder. Thus, digital signatures do offer non repudiation.

4.7 SUGGESTED READINGS

- Data Communication and Networking by Behrouz A. Forouzan
- J. Katz and Y. Lindell, "Introduction to Modern Cryptography" (Chapman and Hall/CRC Press, 2007)
- *Secrets and Lies: Digital Security in a Networked World*

MPDD/IGNOU/P.O.1T/Oct.2011

ISBN : 978-81-266-7522-3