UNIT 4 INTRODUCTION TO CYBERSPACE AND ITS ARCHITECTURE

Structure

4.1 INTRODUCTION

Cyberspace is such a term, which is not yet completely defined and also has no geographical limitation. It is a term associated with application of the Internet world-wide. It is also called as a virtual space as physical existence of cyberspace is not detectable at all. Cyberspace is "the total interconnectedness of human beings through computers and telecommunication without regard to physical geography. Cyberspace is a term coined by science fiction author William Gibson to describe the whole range of information resources available through computer networks. For our purposes, cyberspace is a realm in which communication and interaction between two individuals or between an individual and a computer is facilitated by digital data exchanged over computer networks. This interaction or communication can be used for a host of different purposes.

The Internet is currently the biggest network for linking computers, but cyberspace, as a concept, is independent of the Internet. Cyberspace communication began before the Internet and the World Wide Web, and cyberspace interaction and

communication will continue to take place after the Internet is no longer the network of choice.

Currently there is no generic system for identification in cyberspace. It is not possible to absolutely identify an entity or to accurately tell whether an object has a specific characteristic. Digital environments have inherent differences from real space which causes this discrepancy, and when implementing an identity system for cyberspace one needs to consider more than just the architectural nature of the system any system chosen will have the social repercussions which need to be also taken into account. Identity is a unique piece of information associated with an entity. Identity itself is simply a collection of characteristics which are either inherent or are assigned by another. The colour of a person's hair is good or bad and whether he is attractive or not is part of a person's identity which is usually reviewed by another person.

Interactions done in real space inherently carry the identity of the person originating the transaction. Generally, physical traits are carried along in a transaction - for example when one purchases a book from a book store, the book dealer may remember the buyer's face or build.

4.2 OBJECTIVES

After studying this unit, you should be able to:

- describe what is Cyberspace;
- explain the difference between Real Space and Cyberspace;
- explain the concept of Digital Identity;
- describe Computer and Cyber Crimes;
- describe the architecture of Cyberspace;
- state implications of choosing the link system; and
- list the barriers before cyberspace identity mechanism.

4.3 THE DIFFERENCE BETWEEN REAL SPACE AND CYBERSPACE

The difference between real space and cyberspace is that the essence of any digital transaction is unbundling. Ones and zeros do not inherently carry any separate information along with them; a real space transaction carries along inseparable secondary information. Digital transmissions can only transmit; there is no secondary information encoded in the transmission unless explicitly put there. Thus, for authentication purposes, additional information needs to be carried with cyberspace transactions for identity purposes.

Providing extra information in digital communication introduces the possibility for identity theft. Because nothing prevents the transmission of false identity information, or the duplication of another's identity information. To prevent these problems, the actual identity must not be transmitted along with the message; instead a verification scheme needs to be used to convince the recipient that the message was actually sent by the sender. This eliminates the need to send one's actual identity. The concept of verifying instead of revealing provides an extra layer of security to the sender.

The other point of insecurity is in the digital certificates which were issued to verify

these characteristics. These certificates are meant to be used only by their owner, but if another party obtains them, then that party can falsify his identity, representing him as the individual for whom he has digital certificates.

Architecturally, we must decide how to store and use these certificates. The certificates can be stored on a smart card for use on a computer terminal, or the certificates can be stored in an "identity server" locked via password or biometrics information and available for transmission over the Internet.

In real space, it is difficult to select, to verify or reveal portions of one's identity: most forms of identification contain more information than is needed for any transaction. The unbundling that is possible in cyberspace allows portions of identity to be disassociated and verified by a third party. This not only creates the ability to verify via the least revealing means, but it also creates the framework for anonymous transactions – it is possible to merely verify the proper information without ever distributing the same characteristic. Further, cyberspace users have control over the strength of the link between their real world and the cyber-identities.

4.4 OVERVIEW: WHAT IS DIGITAL IDENTITY?

A digital identity system must serve several functions. First: authentication-ensuring that when a message purports to be from Alice, Alice sent it, not someone pretending to be Alice. Second: message integrity-providing certainty that when a message arrives from Alice, it is the same message that Alice sent, not modified en route in any way. Third: non-repudiation-ensuring the inability of Alice later to deny that she sent the message, and the inability of the recipient of Alice's message to deny that the message was received. Fourth: establishing a digital identity architecture may have the beneficial side effect of facilitating confidentiality through encryption–the knowledge that no one besides Alice can read a message intended for her.

Before proceeding with cyber artitecture, however, it is important to examine the concept of identity itself. This section develops a working definition of identity, considers the ways in which people use their identities, and articulates the reasons why it is important to protect our identities, especially in the digital context.

4.4.1 Working Definition of Identity

It is difficult to craft a formal definition of identity. Basically, the essential and unique characteristics of an entity are what identity it. For example, how the system will identifies this person is called Joe Jindo where there are many Joe Jindo around the world. These characteristics might include, among other things, the unchanging physical traits of the person, his preferences, or other people's perceptions of the individual's personality. The skills that a person possesses can also become part of one's identity. For example, a person's identity could include the fact that he "has the ability to drive" or that he "has brown hair". Some characteristics, such as height, have one correct setting. Those traits of an individual that reflect someone else's perceptions do not have to have an absolute setting. Bob may set Alice's "is friendly" flag to true, whereas Charles may set the same flag to false. Even if Bob and Charles agree on what should be the flag's setting for Alice, Alice's own view may differ from theirs. Thus, in practice, there is a degree of fuzziness to the definition of an entity's identity, and most certainly to how others perceive it.

No two identities are the same. Each identity maps to a unique set of characteristics. Two people may share some of the same characteristics, such as being old enough to

drive or having the same hair colour, but that does not mean that they have the same identity. If Jow Jindo 2 can identified himself as Joe Jindo 1 then Joe Jindo 2 can access and manipulate all the private information of Joe Jindo 1 which is called identity theft.

4.4.2 Identity as a Commodity

In today's economy, information on identity often is viewed as a valuable commodity. This view of identity is worth a closer examination.

Businesses desire to advertise their products to the markets most interested in them, and may even retool their products to be more appealing to certain segments of a market. Knowing the preferences of individuals allows a corporation to target perfectly their products to those who would prefer and, thus, be most likely to purchase them. Making a detailed survey of an individual's preferences, though, is very difficult, if not impossible. Often an individual cannot specify the exact motivation for her purchase of a particular product. From the seller's perspective, determining which questions to ask purchasers can be a daunting task. Further, certain questions, despite their potential usefulness, are not likely to be answered by a purchaser. To work around this problem, businesses use identity information as a proxy for preferences. For example, rather than trying to discover the exact reason why an individual purchased a Ford Mustang, a car dealer might instead try to find out the purchaser's profession or income level. Suppose the car dealer discovers that a number of his customers who have purchased Ford Mustangs are lawyers. Although the car dealer may not understand why they purchased Ford Mustangs, he can assume with some level of confidence that there is something about lawyers that leads them to purchase Mustangs instead of Cougars.

Please answer the following Self Assessment Question.

Self Assessment Question 1 *Spend 3 Min.*

Why identity is viewed as a valuable commodity?

.....

.....

.....

.....

.....

.....

4.5 VERIFYING VERSUS REVEALING AN IDENTITY

Cyberspace creates opportunities for identity theft. One inherent property of digital media is that, it can be duplicated perfectly and easily. Exact copies of everything sent over a digital communications channel can be recorded. Consider the act of

sending a signed letter to someone. In the real space, I reveal to the recipient the exact form of my signature, but the difficulty of mastering the art of forgery protects me from the possibility that the recipient would begin signing letters with my signature. However, if I send a digital letter that contains the digital representation of my signature, the recipient could easily duplicate and use my signature to assume my identity when signing documents. The seriousness of this problem is highlighted when you consider that future technologies will allow extremely important identifiers, such as a retinal scan or a fingerprint, to be represented digitally. These biometrics characteristics are protected in real space because they are embedded in the physical body of the person. This is lost in cyberspace. Thus, cyberspace needs a system that allows individuals to verify their identities to others without revealing to them the digital representation of their identities. A verification system would let Bob, for example, know the identity of Alice or that she possesses a particular trait, but would not give him the ability to impersonate Alice or use the trait identifier as if it was his own. In our digital letter example, Bob would be able to verify that the letter contains Alice's signature but would not let him sign the documents as Alice. Similarly, a verification that someone is of the proper age to purchase alcohol would not give the person a change to verify this identifier anything that would allow him to represent himself as being of the proper age to purchase alcohol. Such a system helps both the parties obtain what they want out of exchanging identity information without the risk of identity theft.

4.6 CYBER AND COMPUTER CRIMES

Computer crimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery and mischief, all of which are subject everywhere to criminal sanctions. The term computer misuse and abuse are also used frequently but they have significantly different implications. Annoying behaviour must be distinguished from criminal behaviour in Law. As per IT Act, 2000, no description has been categorically made for computer crime and cyber crime. So till today, it is very difficult to differentiate between these two words. In relation to the issue of intent, the principle of claim of right also informs the determinations of criminal behaviour. For example, an employee who has received a password from an employer, without direction as to whether a particular database can be accessed, is unlikely to be considered guilty of a crime if he or she accesses those databases. So a distinction must be made between what is unethical and what is illegal, the legal response to the problems must be proportional to the activity that is alleged. Common types of computer crimes are:

- Forgery;
- Fraud by system manipulation intentionally;
- Any modification to data or programs or databases; and
- Accessing computers without authorization;

But cyber crimes are somehow different from computer crimes. Computer crime happens in physical space with or without the network. Cyber crime takes place in a virtual space through digital environment. Recent example of cyber crime was Bazzee.com case, which is a MMS scandal. Cyber crimes may happen globally as there is no geographical limit for cyberspace.

Please answer the following Self Assessment Question.

Self Assessment Question 2 *Spend 3 Min.*

Give two examples of Computer Crimes.

.....

.....

.....

.....

.....

.....

.....

4.7 ARCHITECTURE OF CYBERSPACE

Practically cyberspace architecture for global standard is not yet possible, though certain groups of networks are maintaining some rules and regulations to make a minimum architecture through TCP/IP and a virtual global server system. Here some theoretical architectural choice has been described.

4.7.1 Link and No-Link: An Architectural Choice

As identified earlier, any digital identification system must determine where to lie upon the continuum of anonymity and accountability; that is, a system must adopt an appropriate degree of Type II unbundling. However, within the context of law enforcement it becomes clear that not all points along this continuum are equal. One point is very different from all the others: the point at the far end of the spectrum where there is absolutely no traceability. For the sake of clarity in our further discussion, this point will be called "no-link". At the no-link point, there exists within the digital identification the architecture which has no mechanism for determining the link between data in cyberspace and the real world recipient or sender. The no-link point implies only that there is no mandatory link between cyberspace and the real world; this does not preclude an additional, non-mandatory method of determining an identity that could be layered on the top of the no-link architecture. All other points along the spectrum will be designated as "link" points. This indicates that there is some mandatory architectural mechanism for determining the real world identity of the sender and receiver of data in cyberspace.

Both link and no-link architecture have benefits and drawbacks associated with them. With a link architecture, access to the link information can be limited, presumably, only to an appropriately regulated law enforcement agency with specific regulatory processes in place for obtaining the information. However, the immediate point is that not everyone will have the access to the information contained in the architectural link; to those without access, link architecture is identical to no-link architecture. The benefit of identification is still present, but the ability to gain knowledge of the person's real world identity from the architecture of the system is limited to those specific bodies with access. Thus, once again, the interesting area of discussion is that pertaining to law enforcement: when can a link system effectively be used as a no-link system, and are there benefits able to determine a link which outweigh any corresponding drawbacks?

At all the points along the continuum, except for the extreme of one-to-one identity, there is a need to distinguish between "transient anonymity" and "persistent anonymity". With transient anonymity, no persistent link remains to the sender of the information; this is analogous to anonymous leafleting. Persistent anonymity is perhaps more useful: it allows continuity of cyber identity, generally without disclosing the real world identity, i.e both the sender and receiver mutually agreed and define their private communication channel in the network which is not accessible to any other at any circumstances unless the private information of any party is not tempered or compromised. It only permits disclosure of the real world identity within a link system. In a no-link system, continuity is preserved, but without facilitating the link. Both the types of anonymity are useful in some circumstances, but persistent anonymity is likely to be more generally useful.

No Link

The benefits of a no-link system are, as mentioned above, those pertaining mostly to issues of freedom of speech and freedom of action. In the commercial domain, the wheels of capitalism are greased by the no-link architecture. People who have no fear of ever being personally associated with what they buy are far less likely to be concerned about the social norms which might have previously restricted them from purchasing a product. Unbundling facilitates the necessary degree of identification that commerce will require without necessitating the revelation of the entire real world identity. Free speech is likewise assisted by the absence of traceability: where potential oppressors are unable to determine the sender's real world identity, there is no danger of oppression.

Link Architecture

No-link architecture provides protection from McCarthyism. But in so doing, it removes all accountability from speech. It is an architecture that completely eliminates the power of social norms, market regulation, and legal regulation to govern interaction on the Internet. Society should not overlook the more general consequences that may result from the ability to avoid accountability in all speech, especially the speech which would not be considered criminal: people may routinely and without concern spout inaccurate and misleading information, and the responsibility may disappear even further from the moral landscape. However, the aspects which can be most clearly identified and discussed are those which result in criminal behaviour.

Please answer the following Self Assessment Auestion.

Self Assessment Question 3 *Spend 3 Min.*

Discuss about the various types of Cyberspace Architecture.

.....

.....

.....

.....

.....

.....

.....

4.8 PREVENTING CRIMES

The issue then becomes one of the preventing crimes, while simultaneously attempting to mitigate this potential "chilling effect" on free speech. At the heart of this discussion, lies the distinction between transactional information and content information. Transactional information is the information regarding the sender, recipient, and other information associated with the transmission of the information, but not regarding the content of the information. Thus, so far the argument has centered on transactional information; however, the value of content to law enforcement must be considered: if it is absolutely necessary to have content as well as transactional information, then it will do no good to consider offering the latter without the former. If, on the other hand, transactional information without content is a tool that can be utilized, it may result an effective compromise between the needs of law enforcement and the desires of the society.

Encryption represents the single largest barrier to law enforcement obtaining content from a computer. This is an issue that is relatively unique to cyberspace, as handwritten and telephone encryption is relatively rare. One choice can be made with respect to encryption: allow it, without regulation, or disallow it. Disallowing encryption altogether is pragmatically different from allowing only key escrowed encryption, but for the purposes of this discussion, they are effectively the same. The overwhelming response of the government has been that, encryption controls are in fact necessary, and several initiatives have been proposed to this effect; however, both the public and legal reaction to these initiatives have been negative: many organizations are resisting the degree of control which law enforcement would be given, and the Communications Decency Act was recently ruled as too general to be constitutional. In this situation, law enforcement's claims of what it needs to be effective are strongly disputed by the public: the equilibrium between the two is harder to strike in cyberspace.

4.9 IMPLICATIONS OF CHOOSING THE LINK SYSTEM

The negative implications of choosing the link system are clear: it may place an unreasonable burden on free speech. Even if it is not unconstitutional in this manner, it may simply deter people from speaking out in situations where their voices would be most useful. In order to convince the society that its interests in avoiding unreasonable persecution are maintained, the architectural decision to include the link must be combined with legal regulations regarding who is given sanction to disclose the link, and under what circumstances such disclosure is acceptable. While the negative impacts of providing a link with all the transmitted data can never be fully accounted for, the goal of a system which provides an architectural link must be to mitigate the impact of the architecture as fully as possible.

No-link architecture has more tangible drawbacks. Crimes can be easily planned and carried out on a system with no accountability, and there is no reason to think that they would not be. However, practical concerns such as sovereignty and providing unrestricted speech to political dissidents regardless of their governments' policy on free speech may outweigh the potential societal costs. It may be also that suitable mechanisms for regulating their identity can be created in a legal or market based way; it is hard to see how these methods would be enforceable in a cost-effective manner, but the number of criminal deviants might be small enough that the identification by law enforcement could be reasonably achieved.

A Note on Architectural Choice

It is very important whether the architecture of a digital authentication mechanism

should be designed to permit traceability. Although the discussion focuses on how traceability on the Internet would meet the needs of the government in carrying out its law enforcement function, it should be noted that businesses also have an interest in the development of architecture with such a feature. Many corporations have established Intranets to facilitate communication between the various divisions of their companies. Traceability in the architecture would help the leadership of a business monitor the activities of its employees. Monitoring of this sort might be motivated by a desire to track the productivity of the individual workers or a need to ensure procedures designed to govern access to the company's sensitive information are followed. The development of architecture for the Internet that included traceability would provide a standard that could be adopted for the corporate internal networks, without the associated research and development costs.

Aside from the caveat presented above, business-domain interests in the use of identity do not require the developers of the architecture to make any fundamental architectural choices for the system. Instead, most of the concerns regarding the business arena are related to how businesses and consumers will behave in an environment using the digital authentication mechanism proposed.

Social Aspects

Community in cyberspace is based on the interaction between people.

Cyberspace has an important social aspect to it that must not be overlooked. Ever since the ARPA Net was created, its primary use has been to communicate with other people. With the advent of a faster backbone, different types of communication media became possible namely, interactive communications. Community in cyberspace is based on the interaction between people.

Although a community is a group of people who interact with each other, at the basic level it comprises a group of people who exist with each other in a common plane. Cyberspace can be treated as a conduit touching portion of real space at key points. Ideas are passed through the conduit, and business is transacted through this conduit. The cyberspace communities are members of the global community interacting on a different plane than in real space. These members rarely interact in the real space, but they communicate through multimedia means in cyberspace whether it be by text, image, sound, or a combination of the three. It is not possible to use the Internet without being part of this community of people; you cannot avoid being a part of the community, even if you are using the Internet as a conduit: by e-mailing people, reading web pages, reading newsgroups, or doing commerce online, one has joined the cyberspace community.

4.10 ROAD TO IMPLEMENTATION

The current state of cyberspace identification mechanisms is far from the flexible, broad potential of the identity architecture. There is still a long way to go from the 'here' of the Internet as it exists in 1998 to the 'there' of the ubiquitous, secure identity architecture. In order for the Internet to reach its full potential, a secure mechanism for managing and verifying the digital identity is necessary. There remain ranges of hurdles to overcome before a cyberspace identity mechanism will be deployed and ubiquitous. These hurdles can best be analysed in four categories: social norms, market, legal, and architectural barriers.

Social Norms Barriers

The main social obstacle to implementation of a cyberspace identification mechanism is that the general public does not recognise that there is a problem with the existing

identification architecture. The general public does not understand the need for an improved, secure cyberspace identification system. Even without any effective identification mechanism, the use of the Internet – for both casual and secure applications – has soared, with double-digit growth rates measured month-to-month rather than year-to-year. While more sophisticated Internet users may recognise the need for a digital identity mechanism, these advanced users represent a shrinking percentage of the overall Internet? Community? Many people using popular Internet applications seem to be satisfied with the existing levels of security and identification. E-mail, for instance, is often self-identifying through the content of the message. Forged e-mail, while easy to create in the current architecture, is not perceived to be a major problem. E-mail eavesdropping, also a relatively simple technical task, has not slowed the flood of e-mail communications. On-line commerce is booming even based on systems requiring credit card numbers and the overly revealing identification that credit card numbers enable.

Market Barriers

The market barriers to the implementation of a secure Internet identification system stem from the difficult business economics inherent in solving this type of problem. One of the key problems is that, there is significant business model risk for companies providing identity verification solutions. In other words, it is unclear exactly how these companies can make money. In addition, economic incentives do not encourage the development of an open-standard identity infrastructure. Ultimately, success of an open-standard identification architecture, such as our proposed system, may require government intervention in the marketplace.

Legal Barriers

The most critical legal obstacle to the development and adoption of any effective digital identity mechanism is the current confusion over legal liability rules. In other words, who is responsible if someone's digital identity is misused or stolen? Who bears the cost if a digital identification mechanism is compromised? The lack of a clear legal liability regime for these two issues discourages the cyberspace identity market from emerging in the first place and from operating efficiently once it does become widespread. Legislatures may need to enact liability laws that cover digital identity before the identity infrastructure can be effectively implemented.

The appropriate liability rules must reconcile two competing principles. First, because the market for the digital identity mechanisms is in its infancy, the selected liability rules must help create incentives that will drive towards the widespread adoption of a secure identity infrastructure. According to this goal, the liability for identity misuse should be placed on whichever party can best induce the introduction and implementation of the identity architecture. Second, in order to have an efficiently operating marketplace for identity mechanisms, it is desirable for the selected liability rules to place liability on the party who is the "least cost avoider" of harm. Adopting this goal, liability for identity misuse should be placed on whoever is best able to avoid misuse of the digital identity. If these two goals point towards the same party, both goals can be accomplished together. However, if these two goals suggest that different parties should bear liability, then one goal or another must be made paramount or the goals must be balanced.

Architectural Barriers

In broad terms, there are just three types of identification mechanisms. Authentication can be based on a person's shared knowledge (such as a password); a person's possession of unique information or device (such as a digital certificate); or a person's inherent unique characteristics (such as a fingerprint or other biometric).

Please answer the following Self Assessment Question.

Self Assessment Question 4 *Spend 3 Min.*

What are the barriers before cyberspace identity mechanism can be deployed?

.....

.....

.....

.....

.....

.....

.....

Let us now summarize the points covered in this unit.

4.11 SUMMARY

- There is no proper definition of Cyberspace yet. Only some concepts have been derived.
- Cyberspace is the total interconnection of human beings through networked computers and telecommunications without any regard to physical geography.
- The difference between real space and cyberspace is that the essence of any digital transaction is unbundling. Main problems are to identify the reality.
- Digital Identity is the mechanism to identify the man or product through digital environment.
- In the present scenario, digital identity is also often viewed as a commodity.
- Computer crime and cyber crime seem to be similar but both are different.
- Computer crime belongs to any individual computer without the Internet connection i.e. physically whereas cyber crime happens in cyberspace through the Internet only.

- Cyberspace architecture, which is not properly defined now, is a design in which virtual space transactions are being made through digital environment.
- Presently the cyberspace identification mechanism is not flexible; there are a number of barriers, for example: social norms, market, legal and architectural, before a cyberspace identity mechanism could be deployed.

4.12 TERMINAL QUESTIONS

1) What is Cyberspace and how it differs from the physical space?

2) Write about the concept of Digital Identity.

3) Differentiate between the computer crimes and the cyber crimes.

4.13 ANSWERS AND HINTS

Self Assessment Questions

1) As there is no chance of physical verification of personal identity in cyberspace, the identity, in cyberspace plays a crucial role for electronic identity. So, this electronic identity (called identity only) is viewed as valuable commodity for commercial purpose.

2) Forgery, Accessing the Computer without Authorization.

3) In practice, there is no specific architecture defined for cyberspace but some theoretical concept has been yet proposed for the same like link and no-link architecture for architecture frame work.

4) The cyberspace identification mechanism is not flexible; there are a number of barriers, for example: social norms, market, legal and architectural, before a cyberspace identity mechanism could be deployed.

Terminal Questions

1) Refer to section 4.2 and 4.3of the unit.

2) Refer to section 4.4 of the unit.

3) Refer to section 4.6 of the unit.

4.14 REFERENCES AND SUGGESTED READINGS

1. "Cybernotary Subcommittee Home Page". Section of Science and Technology Law. American Bar Association.6 jan.2007<www.abanet.org/scitech/ec/cn/home.html>.

2. "Digital & Electronic Signatures". WTV Home page. 5Dec.1997. Winchel "Todd" Vincent, III.8Jan.2007<members.aol.com/Winchel3/Links/Legal/Signatures/Signatures LegalLinks.htm>.

3. Uniform Electronic Transactions Act.23 Mar. 1998.