Course Name: Cyber Security and Privacy
Professor Name: Prof Saji K Mathew
Department Name: Department of Management Studies
Institute Name: Indian Institute Of Technology Madras, Chennai
Week: 9
Lecture: 25

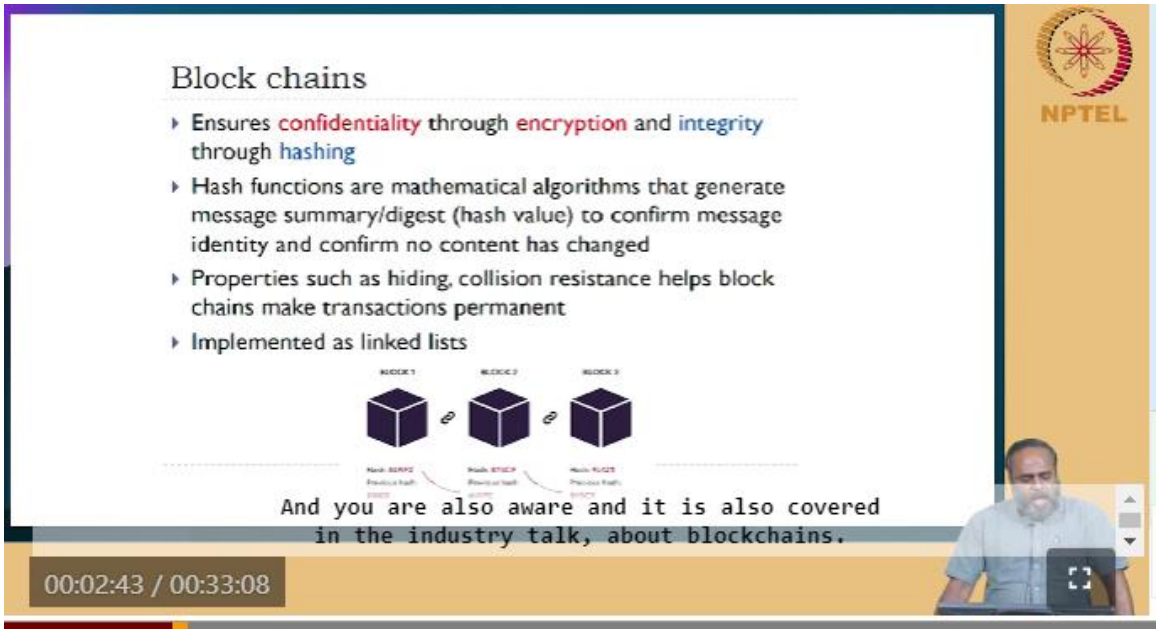
Welcome back to Cybersecurity and Privacy course. So we discussed technologies in the last session and the session before that, of course, you had a industry perspective or a practising manager's perspective on cybersecurity technologies and I noticed that a lot of technologies were covered which from multiple perspectives and you also had an overview of what is current and what is currently, current focus of cybersecurity technologies and intelligence. So and I, some of the topics I discussed was again reaffirming or again, re-informing what you already covered in the session before that. I would conclude the session on cybersecurity technologies. So you have already seen there are technologies for controlling access, access control. You can access an information stored in a, stored or transmitted in a computer network and that of course, we have seen current technologies for identification, authentication, authorization.

So all these are based on technologies. Then you also found that access, even when it is controlled in the best way, still unauthorized access can happen and then the next step is when data is being transmitted from point A to point B or node A to node B, then you encrypt the message that even if someone gains unauthorized access, that intruder does not understand what is being transmitted. So encryption technologies is something that we looked at and encryption is a technology that is very important and very critical for cybersecurity systems to function and I would say it is at the heart of the matter, it is the heart of the matter when it comes to technology. If there is no encryption, there is no e-commerce, just think about it.

You cannot actually send your credit card information on a public network, when there is no security. It just would not be trustworthy. So the trust in computerized financial transactions is thanks to cybersecurity using encryption technologies. And you are also aware and it is also covered in the industry talk, about blockchains. Blockchains as a current and evolving technology and blockchain technically as a linked list.

One block is linked to the other in a system and we can also articulate that in terms of security, it ensures confidentiality through encryption, unauthorized access, unauthorized reading of information is prevented through encryption and encryption also ensures non-

repudiation. I think we discussed that concept. Once somebody makes a transaction, you know there is a private key that is used to transmit that information and one cannot deny that, that you made a transaction and that is transmitted with a private key of that individual and therefore it cannot be repudiated, it cannot be denied. So that is another feature of the blockchains, non-repudiation, confidentiality and also integrity. Or in blockchain terminology, it is called mutability.



Once a transaction is made, it cannot change. So there is a hash function, which I see that you have already discussed. A hash function once it is generated for a block, you cannot change that hash value which is generated. And therefore if you try to make a change in the original block which cannot be done, then the hash, you know with the hash value changes or the hash is permanent and therefore any change is not possible because a hash function generates a hash value for the block forever, it is immutable. And I saw a very nice slide illustrating that as to how hash functions actually ensures immutability of blockchains.

So the industry standards that exists for encryption, you could note that an initiative to have a open standard, data encryption standard DES ,was developed by IBM. It was a 64 block size with a 56-bit key and here is Rivest, Shamir and Aldeman who actually employed people and cracked that code. And therefore DES was no more secure and that they became very popular and RSA key or the RSA was developed by these three gentlemen, I think one of them from Israel. And so the standards have to change and become more unbreakable. So you have triple DES standard today.

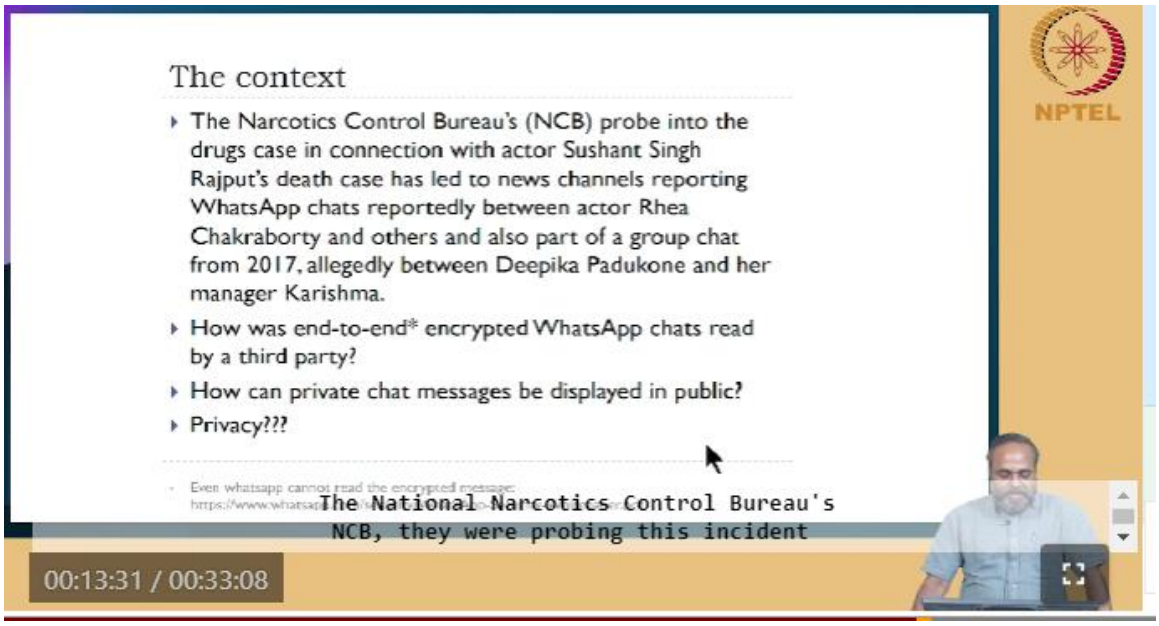
And the other one, most widely used is the Advanced Encryption Standard, AES which pertains both to NIST and ISO; and RSA standard, another competing standard developed by Rivest, Shamir and Aldeman. These are the encryption standards that exist in the industry and key length could be either 128, 192 or 256. And depending on the number of bits in the key, the key becomes more complex, in terms of the ability to break the key. So well, I have just taken this from your textbook, there is some research on the difficulty in breaking a key in encryption. You can see how many years it may take to break a 128-bit encrypted message.

So you can count the number of years, if you can. So essentially what it says is once an encryption is done, say using a 128-bit encryption or 64-bit encryption etc., it is virtually impossible to break the key and read the message. And to the best of my knowledge, I have not read about an incident where an encrypted message was decrypted by a hacker and read. That is something which I have not come across.

If you know, you can share with me. So once a message is encrypted using a standard encryption, encryption standard, it is virtually impossible. So that is the assurance or guarantee that encryption technologies provide. So but there are other ways of actually hacking, but it is extremely difficult, extremely, extremely difficult to break the key. So we will close with that note.

So technologies for cyber security is something that we try to cover. And today let me actually take you to another scenario which is related. The second topic in your course, which is Privacy. What is Privacy and what is its linkage with security, cyber security? And why this linkage is important etc, is going to be covered in the subsequent session. So we also look at what is currently happening in the domain of Privacy and in particular, Information Privacy.

So our focus would be more on Information Privacy. And we will come to that as we go. So we will try to find the difference between Privacy and Information Privacy and the connection between Cyber Security and Information Privacy. So today is an introductory class and we will also have a case discussion towards the end to understand the implications of privacy for individuals and organizations. Well, this is something you must have, if you are actually watching popular media like TV, this is something I am sure a few years ago you watched.



WhatsApp claims that messages are encrypted end to end. So I was watching this news and I saw a WhatsApp message between two individuals, Two celebrities of course, you know them by face. That was shown in the TV screen. That was appearing in the TV screen. If I do not know if you recall what was the conversation that was shown in the TV screen, it was about substance abuse or weeds.

So you know, popular media actually had a lot of interest in actually watching and commenting and digesting and talking about it for quite some, after some months. But the important thing is, well, here is an encrypted text which is available in public domain, number one. And number two, even if somebody got access by cracking the encryption, you know, which I just said is impossible, then how can a TV channel publicly transmit a private conversation? So it is a conversation between two individuals. I may talk to you something which is very private to me or I may talk to my wife or someone, some private message or I may send a text which is very private. How can a TV channel, first of all gain access, that is question one and second, make it public? Do you have comments? Question one, how was it cracked? Was encryption, is encryption vulnerable? I am not sure of this case but I think the one possibility of, because WhatsApp has a feature of backing up the chats to Google Ray which was initially unencrypted.

So the law enforcement could have access to their Google or the leakage of credentials of Google accounts. So from further that, they could have gained access to WhatsApp chats in plain text. So you are saying it is not the encrypted message that was accessed but it is the backup. So it looks like you have tracked the story. Actually how, you know the government agency which actually had a crackdown on this was the Narcotics Bureau

of India, Narcotics Board of India, Narcotics Control Board, NCB.

So, so here is the government. So government if they want, can access information for governance. And that is one aspect of it but it is not the government, this message is not in the custody of government, it has gone public. So you are saying, so both of you are saying it is not the problem with encryption. If a message, a WhatsApp message is backed up in some drive, then that is not encrypted.

WhatsApp does not guarantee that the backup, backed up message would be encrypted or it is not readable. So there is no encryption or guarantee for message that is stored or backed up, which is true. That is what happened in this case. How, that is how they got access. The they meaning the government agency for investigation purpose.

But this is public. What justifies that? So that there is another dimension to it. That is a dimension of privacy. Can a private conversation be made public by a TV channel? No? Then, I think TV channel is still operating, right? They have shown everything that was going on between two individuals. I think I expanded it wrongly. The National Narcotics Control Bureau's NCB, they were probing this incident because it became public.

And but it, but during the investigation, whatever information or text messages they gathered also became public. And of course, we do not doubt the encryption. So I want to reaffirm that, WhatsApp gives us end to end encryption. And its encryption standard is open and public. I have given a reference to WhatsApp security.

There is a white paper which is given in public and where they have described the complex process of encryption they follow. For example, there is a distinct key for every message that is transmitted. So it is very secure and it is not the encrypted message that was cracked. But it was the backed up message. So that is, that actually answers the first question I have asked.

And the second question is not answered. How can private chat messages be displayed in public? Channels defend themselves. These individuals can of course, file a defamation case. You know, this is actually my private information. Some years ago, you know, of course, maybe 6 or 7 years ago, there was a similar case when Ratan Tata's conversation with Niira Radia was leaked.

It was available in YouTube for you to listen to. And Ratan Tata filed a case in the Supreme Court against that leakage to the public. So it is an intrusion into the private space of an individual. But what would the government or what would the TV channel would say? This is just showing what is WhatsApp message about backup. Media and

messages you backup are not protected by WhatsApp end to end encryption while in cloud.

So they have a disclaimer there. So this is actually a very complex topic. I am touching on a topic which is legal, political and it is not easy to resolve. There is something called public interest. The media say, well, this is in the public interest. The public interest or national security, which is government's argument, which is provided for even by the court, that government for the purpose of national security can access private information.

That is a caveat. When we make tall claims about privacy as a fundamental right and so on in the country, it is not an absolute right. This is something we would see in detail as we go and touch on regulation. But we know that there is no 100 percent guarantee for privacy, although there are secure technologies. And politics means, you know, so there is a ruling party and opposition in democracy. The ruling party would like to have control because they have to govern and the opposition would always question that.

And when the opposition comes to the ruling party, they will actually change their stance. So my take on this is a political party while in power will stress on national security and while in opposition will advocate privacy rights. You can observe this as power changes hands. So there is, there is grey area in privacy, which we all would see as we go and we also discuss cases. You must be familiar with this term, the big brother.

Big brother was coined by George Orwell and I referred you to 1984. And it is in the book 1984 that he coined this term, big brother as the government or the one in power. So there is a huge power asymmetry between the government or the power centre and the governed people. And that gives certain benefits to the government because they can know and they can use technology for security and welfare, they can also abuse technology for political gains.

Both are hard fights. I am not criticizing any political party or individual or any particular entity. These are possibilities. These are actually, you know, these are all human systems. So you see, in India we have an Indian Telegraph Act, which was enacted by the British in 1885. That is the act which gave access for government to communication between individuals.

Government was able to actually, if they wanted they could actually tap the mails or letters sent by individuals, one individual to the other individual. There are so many cases in history where government actually took or tapped mails between private individuals. So you can call it a draconian act. But has any government changed this? We have two, you know, two political parties at the moment. So has any government changed this? So

this is convenient for governance.

So you need actually, you need access to information to make decisions. But the downside of it is that it could be misused. This could be misused. So we live with that reality. So these concepts at a philosophical level, Michael Foucault, the French philosopher was the first one to write about technology and power and the asymmetry of power and of course, George Orwell, 1984.

So how many of you would agree if IIT Madras installs a CCD camera in your room? IIT would say that well, we want to ensure that girls are secure. Say there is some incident, some, there was some theft in some room and somebody got into a girl's room. So after that the institute decides we will keep a camera in each room. Would this be okay with you? No? Uncomfortable.

Uncomfortable, okay. But it is for your security. Then you are saying two things, one is that we want to be secure in the campus, other is that we also want privacy. Let the girls speak. Actually this is the real case. Some years ago, the institute initiated this CCD camera installation in girls hostels, in all hostels, even in our apartments in each floor there is a camera now. So they came with this camera to the girls hostel corridor and the girls went on Dharna, "No CCD camera here.

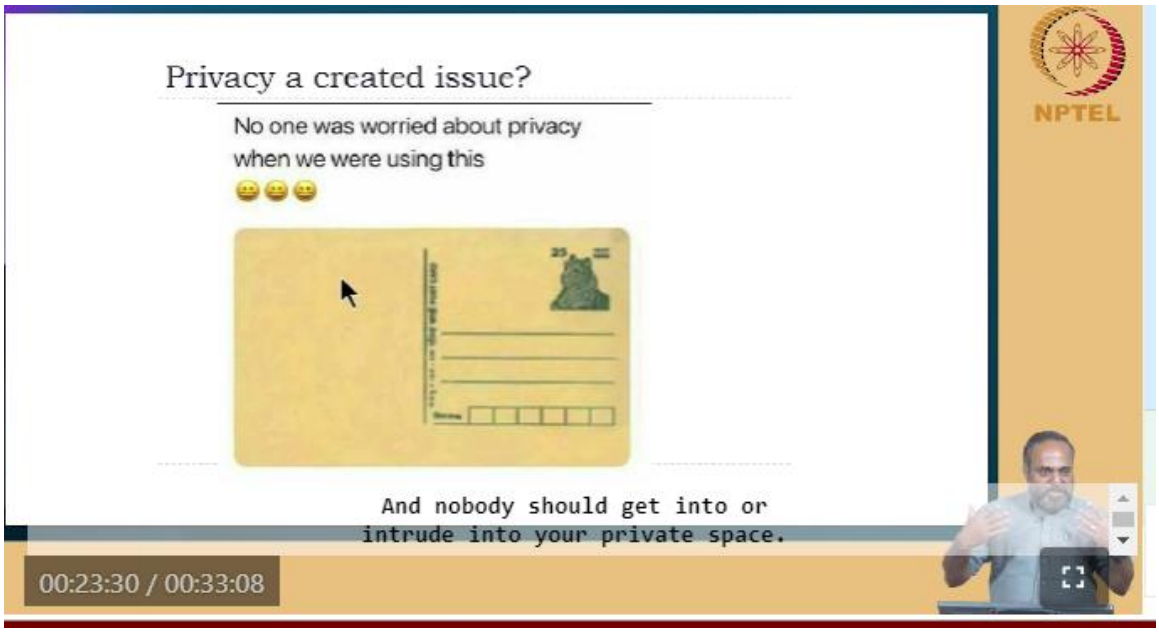
" And what happened? Do you have a camera now in the hostels? You have, right? They won and you lost. So but don't you see it as an intrusion into your private space? No, this is called panopticon. The term is panopticon. There is one point sitting where you can actually have control over the entire infrastructure. You know for this system, surveillance system there is one point where all this information is displayed.

You know this is called panopticon or being observed while the subject does not know. You do not really recognize. So privacy advocates actually at least have brought this topic to the point that if there is a CCD camera, it should be written and it should be known to people that you are under surveillance. It is mandatory.

It is informed to you that you are under surveillance. So it is up to you whether you want to be there or not. So that is sort of compromise but administration has the rights to monitor its space, without really getting into your rooms. If you, if it gets into your room then actually it becomes a private space. The corridor is not a private space, it is a public space.

That is the argument. Which is difficult to get through when it comes to students. There was a hard time of negotiation. I think one of my colleagues was involved in it. Now the

other side of privacy. Is not privacy as a topic just a talk? Who cares? Have you used a postcard for sending messages? That was our communication in the 80s.



You might have. Yeah, we have used. Yeah. So in postcard we used to write every story. Probably the postman of the location would know everything about everyone. Right? And there are movies on this. So Marykutty delivered. That is a typical message that will go from one family to the other when there is a delivery or when there is a function.

So you write almost everything personally. But then the writer was aware that it is in his own liability actually. Yeah, yeah. You know in our society we function in a particular way. Till the time somebody came to us and made us conscious, this is privacy.

You are an individual. You have a private space. This is your life. And nobody should get into or intrude into your private space. We have become more and more, we have been made conscious of privacy.

This is my observation. So there is an era. So I belong to Gen X. So 70s and 80s, privacy is not something, we do not talk about privacy. What? You know, you talk about everything in groups. And so as our connection to the western world increased, where a society which is very individualistic and researchers would say that we are a collectivist society. So we have joint families, we have communities, religious communities particularly, where sharing of information is like, you know, information is a public property.

Everyone knows everything about the other, you know. So same with, you know, social scientists argue that we were not very caste conscious in India. So Indian society functioned by caste.You all belong to a caste.

I do not know what is my caste. But we have caste based on work. What kind of work you do. So just like all the engineers or IT professionals get into one group, because they have common things to share, you know, common, most of your day you spend on your work. So they became communities, you know, this is my observation again. So these are natural group formation. So natural affinities, you know, people form into groups, which per se is not wrong.

But when caste became a hierarchy, there is abuse and there are so many other evil effects of it. But just to say that everything about caste is wrong, may not be very appropriate. But that is again the Western school of thinking. Look at our society through the lens of the Western theory or Western concepts.

So we became caste conscious, we became privacy conscious of late. Now when did, what is the origin of it? When did this discussion on privacy became, become very prominent? If you read literature, particularly management literature and law, you will find that it traces back to 1890. Somebody defined what is privacy. Till that time, well, there may be situations when privacy matters or somebody got into someone's home or private space, etc. But it became an important issue for, for, at a national level, I would say. In the 1890s, when two scholars, Samuel Warren and Louis Brandies published a paper titled 'The Right to Privacy' in Harvard Law Review.

That was 1890. 1890 has something to do with technology. That is the same decade when a company, a company which functioned for successfully 400 years and now of late in the digital era closed down. That company began in the 1890s. And it was an outcome of the product that that company produced, their privacy was intruded. And it was a, it was a dominant player all throughout 400 years.

But in the digital era, they could not survive. No. It is a product. Not Nokia. Nokia, I do not think it is that old. Cell phones. So let me give you more clues.

So what happened is one of them, you know, they were entrepreneurs also. So one of them actually went for a evening party, a party. And it was actually a private party. So where, you know, it is the United States, so they were again celebrities and one of them sat close to a woman.

And that appeared in an evening newspaper next day. And this guy was shocked. Well,

I had a private time or a private chat with someone. And here is my picture, Photography. So camera, photography camera, Eastman Kodak began as a company in the 1890s and photography became possible. And not only photography, photographs could be, could appear in newspapers, where it goes public. That is the point in time, the power of technology to intrude into private space became very, very clear.

So that is when they started thinking, well, this can happen again, this can happen to anyone. Photography is something that captures a moment. We, today, you know, the social media is, you know, flooded with pictures which we want to transmit, but the moment it affects us negatively, we are all concerned about privacy. So technology or the era of technology, computer technology and photography and so on, actually brought in this issue of privacy. And that is when there was a paper and these people defined privacy as the right to be let alone.

And that continues to be a classical definition for privacy. Every individual has a right, that is a right to privacy. Essentially, if you actually look at it through the lens of social science or an individual as an entity, there is something called freedom. An individual has a freedom and every constitution, every democratic constitution ensures that individuals have freedom. And that freedom is a part of an individual's autonomy. That is basically the question or the matter at stake in privacy is autonomy of the individual.

Autonomy is something that you want and a constitution grants to individual. Because at any cost, even if I do not have food for one time, I would still like to have control on where I go, what I do, whom I talk to. I need to have that decision right with myself, it should not be taken away by somebody else. So when I have a private conversation, it is my private conversation. And nobody, including government has any right to get into that space. See a quote from William Pitt in 1763, even if the poorest of poor is sleeping in his hut, no government has the right to get in there.

And of course unless by warrant, that is a legal aspect. You simply cannot enter into someone's private space. That is intrusion into privacy. So privacy, your privacy in a general sense as you see here is about an individual's right to autonomy or individual's right to freedom. So the overarching concept is freedom. And some scholars say therefore, why talk about privacy separate from freedom, it is already embedded in freedom.

So they say, there is no distinct concept, but others say it is called coherent delism. So if you read literature, so there is a coherent concept called privacy distinct from freedom, you know, that is the other argument. And this public versus private debate, of course it is the Greeks who thought a lot about everything. So it is Aristotle who articulated that there is a public space called poilis and there is a private space called oikos, you know the

Greek words. So these two distinct words, public space versus private space was actually given to us by the Greek scholars. And ever since the idea is to separate these two spaces and give an individual the freedom to conduct oneself the way one wants in the private space, but in public space, since it is not just you, but there are others.

So there is need for governance, there are, there are need for rules and regulations and all that. Therefore you cannot say I will do whatever I want to do on the street or in a classroom. It does not work because it is a private, public space. So this is what I said Reductionism versus Coherentism, meaning that there is a distinct concept versus there is no distinct concept debate. Let us leave that there.