Network Security

Professor Gaurav S. Kasbekar

Department of Electrical Engineering

Indian Institute of Technology, Bombay

Week - 01

Lecture - 01

Introduction to the Course

Hello, welcome to the course on "Network Security". My name is Gaurav Kasbekar. I am a faculty member at the Department of Electrical Engineering at IIT Bombay. So, what will this course be about? We know that communication networks, including the internet, are being extensively used by a large number of users for various applications.

We all use various popular applications such as email, web browsing, internet telephony, financial transactions, and so on. However, the downside is that malicious or hostile users seek to attack networks in different ways. For example, they often steal secret information such as passwords and credit card information. So, they may try to steal passwords of some legitimate users and try to log into their accounts. They may steal credit card information and make purchases online fraudulently.

Malicious users also install malware on the devices of legitimate users, and this malware can cause unwanted effects such as deleting files or occupying processor space and so on. They also disrupt communications. For example, they might send a large number of bogus packets to a communication link, thus occupying its useful bandwidth so that no useful bandwidth is available for legitimate users, or they may send some packets to a server and cause it to crash so that the server is not able to provide the intended service. So, in summary, malicious or hostile users seek to attack networks in a number of ways. So, the goals of the field of network security are, first of all, to understand how malicious users can attack networks and then, after gaining this understanding, to design various mechanisms for defending networks against such attacks.

So, this is clearly a very important field in today's times. The objective of this course is to provide a detailed exposure to this important field. So next, who will benefit from this course? That is, what is the target audience? This course is intended for students, faculty

members, and industry practitioners in the broad fields of electrical engineering and computer science. In particular, students at all levels can take this course: undergraduates, master's students, PhD students, as well as industry practitioners who would like to learn this field, and faculty members.

So, what are the prerequisites for doing this course? An understanding of the basics of communication networking and programming will be helpful. However, note that the background from communication networks that is required for doing this course will be reviewed in the first few lectures of this course itself. So, we now go over the course contents, what topics will we learn in this course? So first, as we just said, we'll provide a review of the basics of communication networks.

So, if you have already done a course on communication networks, then this will provide a refresher. Then, we'll study different types of attacks on networks, including stealing information, denial of service attacks, replay attacks, modification attacks, and so on. Then, an important part of network security is cryptography. That is when a sender sends information to a receiver; he or she disguises the information so that even if some eavesdropper intercepts that information, they cannot gain any useful information from it. So this is known as cryptography.

So first, we'll study the required mathematical background for cryptography, and then we'll study the principles of cryptography. There are two broad categories of cryptography: one is symmetric key cryptography, and the other is public key cryptography. We'll study each one of these. Then apart from cryptography, there are some other building blocks for implementing network security functions. These are message integrity, cryptographic hash functions, digital signatures, and authentication. So, message integrity means that when a user, Bob, receives a message from Alice, Bob has to check that the message was indeed sent by Alice and it was not modified during transit.

So, this is message integrity, and one of the mechanisms used to implement message integrity is cryptographic hash functions. Digital signatures is another mechanism that can be used for message integrity, and digital signatures also have a lot of other applications. So, we'll study these building blocks of network security. An authentication is also another fundamental building block. If two users, Alice and Bob, are communicating over a network, then Alice needs to prove to Bob that she is indeed Alice, and Bob needs to prove to Alice that he is indeed Bob.

So, this is the authentication function. We'll discuss various mechanisms for authentication. Then, as we said, one of the types of cryptography is public key cryptography, and for implementing public key cryptography, we need various components which are known as public key infrastructure. And one of the components that is part of public infrastructure is certificates. You may be aware of certificates.

For example, if you try to visit a website, you sometimes receive an error that the certificate has expired. So, we'll discuss public infrastructure and certificates. Then, after understanding the basic building blocks of network security, namely cryptography, message integrity, signatures, authentication, and public infrastructure and certificates, we'll study a number of practical systems which use all these mechanisms to provide security in the internet. So, we'll in particular study systems for securing email, including PGP and S/MIME. Then, we'll study protocols for achieving security at the transport layer of the protocol stack.

We'll study the protocols SSL and TLS, and we'll then study various mechanisms for network layer security, and in the same context, we'll discuss virtual private networks. Many of you may have used virtual private networks to access your organization when you are outside the campus. So, these virtual private networks are implemented using network layer security, which we'll discuss in this part. Then, wireless networks are an important kind of network. So, two popular categories of wireless networks are Wi-Fi and wireless cellular networks.

First we'll discuss security in wireless local area networks, in particular Wi-Fi security. Then, we'll discuss security in wireless cellular networks, including 2G, 3G, 4G, and 5G security. Next we'll discuss firewalls and intrusion detection systems. These are systems which often reside at the boundary of an organization's network, and they filter packets that are coming in and going out of the organization's network. Next we'll discuss cryptocurrencies and blockchain.

So, we read about cryptocurrencies such as Bitcoin regularly in the news. So these cryptocurrencies, including Bitcoin, are based on a concept called blockchain. So, we'll discuss cryptocurrencies and blockchain in this part. Then, the next topic we discuss is cloud security. We know that much of our computing and storage happens in the cloud.

So, we'll discuss various mechanisms for achieving cloud security. The Internet of Things extends internet connectivity from traditional devices such as desktop computers, laptops, and smartphones to resource-constrained devices such as sensors, actuators, appliances,

and so on. We'll discuss security of the Internet of Things and we'll also discuss hardware security. We'll discuss anonymous connections and onion routing. These are techniques using which users can communicate among themselves without others knowing who is communicating with whom.

Next we'll discuss post quantum cryptography. So, as you're aware, quantum computers are being developed, and many of our traditional cryptographic techniques are vulnerable to being broken by a quantum computer. In this part on post quantum cryptography, we'll discuss cryptographic techniques, which are robust even in the presence of cryptanalysis by a quantum computer. These are the references for this course. If you are interested in reading further, you are encouraged to read many of these references.

First reference is by Kaufman et al. It's a book on "Network Security". The third reference: Menezes et al. That is also another good textbook on "Cryptography, Network Security, and Cyber Laws". And the fifth one by Stallings is also another textbook on "Cryptography and Network Security".

So, we'll use these extensively throughout this course. The second reference by Kurose and Ross, we'll use mainly for the review of basic communication networks. It also has a chapter on "Network Security" which we'll use. Edney and Arbaugh is a book on "Wi-Fi Security". We'll use it for a part of the discussion of Wi-Fi security.

And Peterson and Davie is another popular textbook on communication networking. It has a chapter on "Network Security", which we'll refer to. And we'll discuss much of our content will be based on research papers, and we'll list the research papers which we'll refer to later on in this course. Thank you.