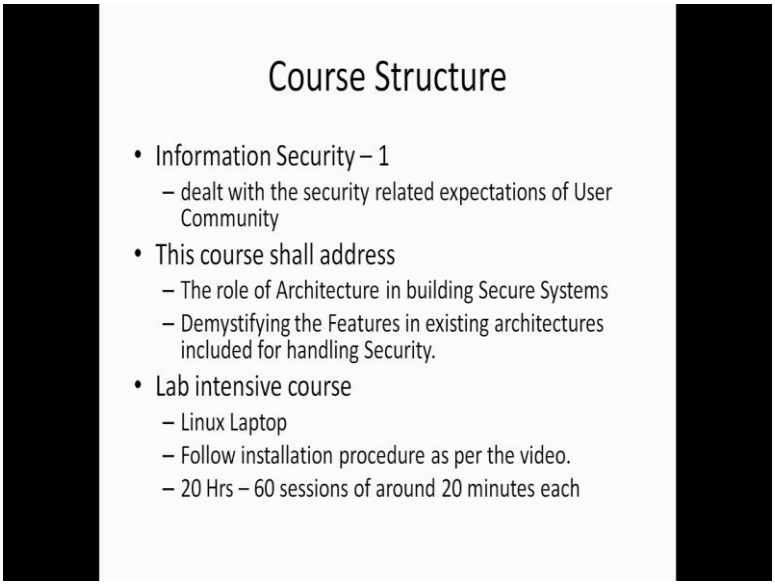
Information Security - II
Prof. V. Kamakoti
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

Lecture - 02
Architectural Aid to Secure Systems Engineering
Session – 1: Need For Secure Systems

The topic that we will be covering is on Architectural Aid to Secure Systems Engineering and we have 60 sessions, each of 20 minute duration, (Refer Time: 00:25) over 20 hours in this course and this is session-1. And, in this session we will talk about the Need for Secure Systems.

(Refer Slide Time: 00:39)



So, when we look at the previous course; the Information Security-1, it is actually dealt with the security related expectations of the user community. So, at this point we would love to have a look at, what computer science has in front of us as a challenge? If you look at computer architecture. The evolution of the computer architecture over the last 4 decades, the real commercial evolution of the computer architecture. The first decade was actually talking about, performance. How many Mibs a system can give me?

The second decade, actually started talking about applications of this, right. Can I use it for multimedia? Can I use it for video? Can I use it for you know animations? Right. The third decade, actually started talking about power and you know area. The mobile technology came up very prominently in the last say, 2000 to 2010. The next 2 to 3 decades, we will be talking about security. Why 2 to 3 decades about security? That is what I expect is that, security is like a habit, right and when you are born at the age of 5, you start inculcating an habit that will come till your last minute. But, suddenly at the age of say 30, you want to develop a new habit it does not come very easily. So, when I start to retrofit security into all the mess that I have done in the past, it is not going to be a easy joke. And so, at the same time I am so much involved in my system, this computers have become so personal to us, right? That you know it is not very easy to throw a fall all the legacy and start everything from scratch. We essentially will become paralyzed if you trying do that.

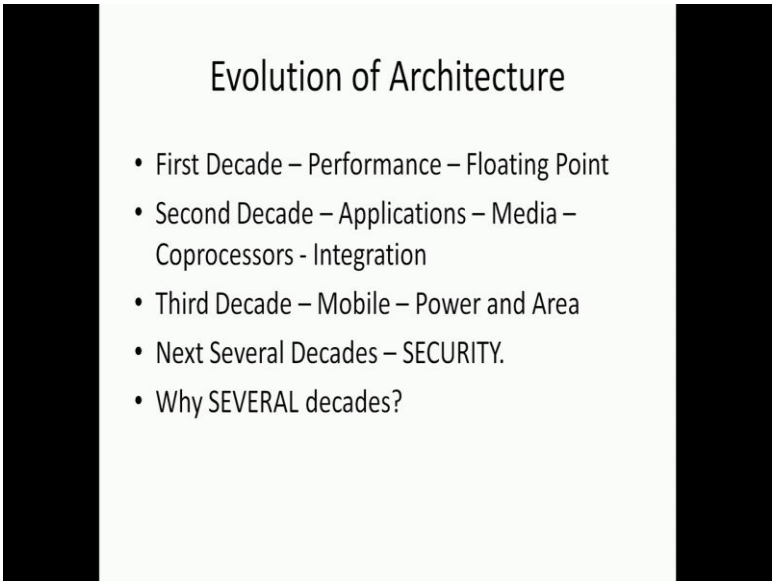
So, this is fair the sort of you know interesting scenario that we are in. And, we should say that we are in interesting scenario because if at all this problem did not come, probably many computer scientists like us who have invested our career in computer science may not have open problems to solve. So, this will keep us busy for at least till my retirement, I am sure I will be busy handling information security in some form of other, to the best of what I have understood about it. And, that is true with all of you. So, that is why this course is very, very important right? If you want to make a big contribution to computing, the many of those big contributions will come through information security. So, if you are a B.Tech student, if you are a M.Tech student, if you are going to be a professional, if you going to be a professor, you are going to be a scientist, you are going to be a policy maker, a good understanding of information security is always good. So, that is why this course is also important and we are trying to do this course.

Now, what this course will address is the role of computer architecture in the building of a secure system. And, we also want to demystify some of the existing features that were included in the architecture as late as 20 to 25 years before. There are lot of features in the architecture, existing architecture, we are going to enumerate those things and these exists for a last 2 decades. But; unfortunately, many many software including operating

systems that have been grown on top of this, I have not used these features, right. And, if you start using these features, then you can get reasonable amount of security. So, we want to demystify those things, these things exist, but the software did not use it for whatever reason. So, that is one of the important thing that we want to do. It is not that, I need to invent something very new in terms of hardware, there are some small extensions that we need to do in hardware. But, there are lot of infrastructure; fortunately, which has been developed in the past, which I can use it now to build the secure systems, right? So, what are those infrastructure? That is what we are going to study here and for us to appreciate the infrastructure, the traditional text book education that we get is not sufficient, we need to go much deeper, right? We have to go much deeper into the architecture. We have to use a bigger lens to look at the architecture and what is that depth, we will go and deep dive into it and that is what we will do here.

So, this is a lab intensive course. So, we need to have every participant here, should have a Linux laptop or a Windows laptop does not matter. But then, there is a video that will be uploaded on the site and it will be shared to you, you follow the insulation procedure this is a 5 minute video, you follow the insulation procedure and get the environment that is there on the video, installed. We have at least 100 students have installed that in the past and we have refined that video over a period of time so, it becomes very self sufficient. So, you just follow the video procedure and install the environment on your laptop. And, after the first 6 hours of lecture starting from the 7 to the 18th hour, right or 7 to the 16th hour, those 10 hours of lecturing you have to bring your laptop or whenever you are viewing the lecture please, have the laptop by your side because, I will be demonstrations, that will happen as a part of this. So, this course, as I mentioned earlier has 20 hours and that is 60 sessions each of 20 minutes each and we are in session number 1.

(Refer Slide Time: 06:44)



I have already talked about evolution of architecture and this slide sums up that. The first decade was on performance because engineering community was using it, it was all of floating point Mibs and all these terminologies came up. The second decade was applications, there were media co-processors that came. One of the interesting media co-processors is the graphics co-processor, and there were network cards which are now network processing cards. Actually, there are some small processors, glorified micro controllers, that is it, even over network cards. So, the second decade was, how to use the computers for non computing applications? The third decade was essentially the mobile era, where we are talking about power and the area. Now, several decades from now on we are going to talk about security. It is going to be several decades and I explain why it is several decades. I move on to the next slide.

(Refer Slide Time: 07:49)

So, let us see how computer architecture has evolved. So, what was yesterday. So, you had camera, torch light, media player, phone, video game, alarm clock, remotes all these things got integrated in to one system namely called the mobile phone.

(Refer Slide Time: 08:05)

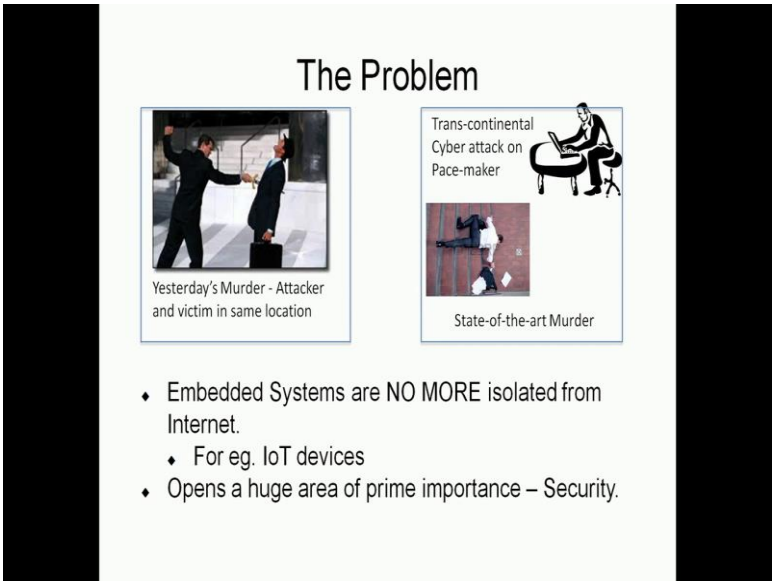
In 1998, when mobile caught up with some form, where each incoming call was 20

rupees and out going call was 30 rupees, right. Nobody even dreamt that we will use a mobile phone for anything other than talking. But today you use the mobile phones for everything other than talking, correct? And, that is what you know the way the computers are evolved. The fascinating way the computers have evolved.

(Refer Slide Time: 08:32)

Now, what is going to happen today and tomorrow, this is it. Now, your mobile is going to be used, it becomes more and more personal. If I keep on talking over the my mobile phone my wife says, why do not you call it the wife? Because, it is also if you keep it in your pocket it is very close to your heart, right? So, mobile is becoming more and more personal, it becomes much more closer to you. So, now you see, your mobile is going to be used for even monitoring many of your parameter. Already, there are mobile phones which can monitor your blood pressures, can monitor your pulse, right.

(Refer Slide Time: 09:08)



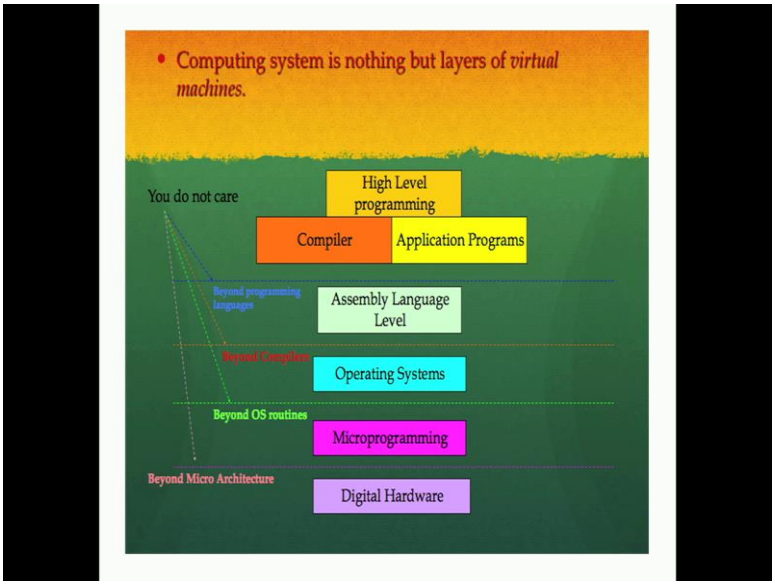
And, everything else is going to become here. And, moment you bring something more and more close to you, more and more personal to you, you go start living with it, right? Then you land up with more vulnerabilities. If somebody can instead of attacking you, if he can attack the system he can cause more damage than attacking you personally. And, this is one thing which is not, we cannot say that this is a fiction; whatever, you see in the slide. So, it is the difference between yesterday's murder and today's murder. In yesterday's murder, the victim and the attacker should be in the same point, right? I have to go and the attacker has to go and kill the victim. But today, I can do what you call as a transcontinental cyber attack on a face maker, I can do a trans continental murder. I can set somewhere in some place X and some several wide kilometers away I could go and attack the face maker of a guy and I can kill him, correct?

Because, the face maker is now connected to the internet in some form because the doctor is viewing your face maker. If there is a problem, the face maker gives a feedback and immediately you many not even know that the problem is coming, an ambulance will come and take you and go. So, this is what you know health monitoring is going to happen and you call it smart, you call it intrusive, you know whatever you call it, but that is what is something envisaged here, right. So, please note that embedded systems are no more isolated from the internet. So, you have got internet of things, right and so, this

internet of things, these are all the internet of things and they are all going to be connected. So, everything that is going to be of some significance to your life is going to be on the internet and this opens a very huge area of prime importance namely, Security, right.

So, even to protect yourself and you work very hard that your grandchild get protected because of some infrastructure that you create is a very big importance and more and more. As you see computers and electronic devices are going to become much more closer to you in life, right. And, it is not that you can hide away from them.

(Refer Slide Time: 11:30)



Now, when I want to look at security. So, the next question you may ask, what you mean by security? What I should do here? So, this is the structured computer organization that you see in many of the text books. I have a digital hardware, this is the real electronics, on top of it there is a layer called as micro architecture. When you go and try to categorize your digital hardware, you see some micro architectures and beyond that micro architecture there is a layer which is called the Operating System. On top of the operating system, there is the compiler which you called as the assembly language level. And, on top of the assembly language level you see there are application programs, there are application development environments, right; your compilers, your desktop, your

guise, etcetera, which helps you develop these applications. And, on top of it the application you as a user right. So, when I want to use a computer there are at least 5 layers that you see, that I put on the screen. Now, each layer by design has been isolated from the next layer, right.

Now, when I write an application I do not know which compiler is going to be compile, which hardware is going to execute, what is the processor number. So, you all have a mobile phone today, do you know the exact part number of your processor? Abhinay, do you know what is the exact part number of your processor? Do you know who made that processor? Nothing you know, right? Who compiled that android code, do you know? What is the version of the android that is being used? Is it android or a IOS? Sharada? You know what is android or can you tell me the exact version of your android that is running on your mobile phone today? Who wrote that device driver? Nothing, right. Lot of things are hidden, right. If you are a little inquisitive you go and do some 5 percent of this, right. Now, why is it like this? Suppose, I say that I will not isolate this layer, you have to know about everything before you start writing a program. Then just to make you write the hello world program, it will take 8 semesters.

So, I instead of having a B.Tech in computer science and engineering, I should have B.Tech in hello world program. Because, to write hello world, you need printf, to know printf you should need how to write device driver, if you have a device drive you should need a what is graphic card is? Then you should need how to interface with that? I know you should talk about PCI express everything. So, I have to cover architecture, I have to cover everything before you write one single program. It is impossible even to teach a course, without the subtractions. So, if I am working at layer A, I do not know what is happening about layer B. So, that is a complete isolation between digital hardware, micro programming, operating system, assembly language level and you know compiler application program and high level program.

Note, that this is the isolation which becomes a very, very good soft target for the hacker. You are writing a program, you do not know what is going to happen beyond it. So, you obviously, do something without understanding it is implications and you are at the application software level, and I go and hit you at the micro programming level or your

operating system level and I can go and crack your software, right. So, the isolation that has been imposed voluntarily, by system developers to ensure that you go and start executing programs with ease, you start using the system with ease. That isolation has become the major stroke for vulnerability, right. So, every layer that we are talking of is now today something like a virtual layer, right. It is something like a virtual layer and you do not have anything, you do not know anything about the sides of this layer and that becomes a major source of vulnerability.