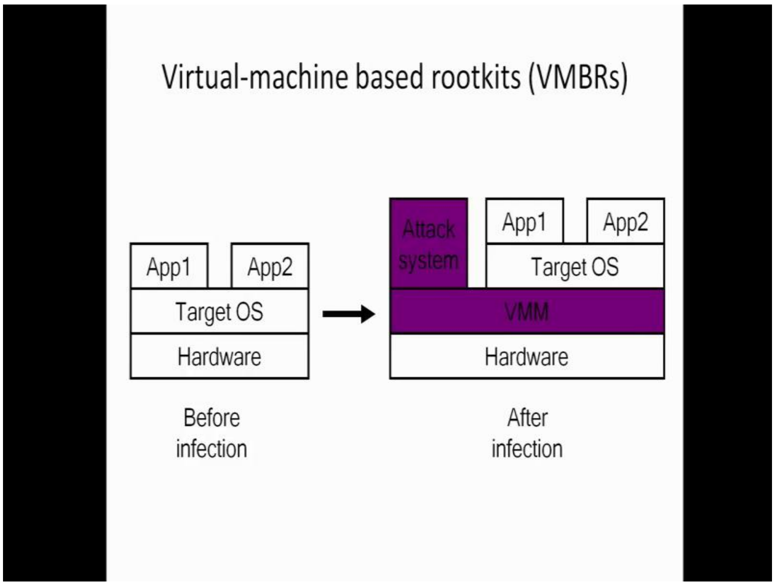
Information Security – II
Prof. V. Kamakoti
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

Lecture – 06
Architectural Aid to Secure Systems Engineering
Session – 5: Virtual Machine Based Rootkits (VMBR)

In the section, we will talk about what we mean by a Virtual Machine Based Rootkit. Why I am going to talk about this is that as we are going to explain architectural aids for security, we will again start with VMBR might be the real stuff that we would like to address when we build architectures for security. So, VMBR has been a very traditional way of trying to get access to the system and what unauthorized access to the system.

(Refer Slide Time: 00:51)

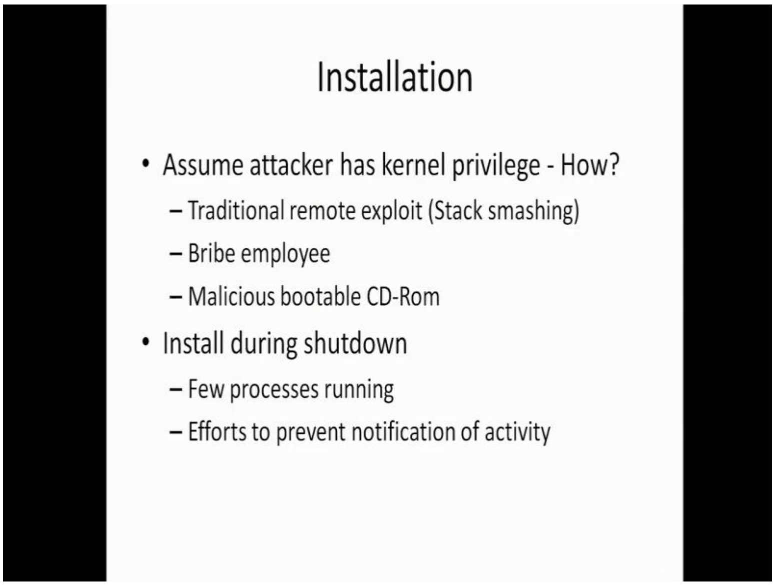

Virtual-machine based rootkits (VMBRs)

So, the way VMBR is conceived, is that some how I get into your system through your stacks machine and then immediately, I start dancing there right, as a code. Then you will find out that I am trying to, the interest in many of the attacks is not just to go and immediately, go and you know kill the system. The interest is that, I go and sit in the system and hide myself and keep you know, getting more, more information out of it, right. The interest is not in bringing down your system, the interest for me is to get access to lot of your credentials and start playing with it whenever; I want it, correct. You understand this, right. So, this is the thing. So, here it is not the thief who comes to your house, break your almirah, take the jewels and go off. Here, fellow who goes and stays in some place where you never go in some thing and keeps on watching you and then finally, do something to you which will be great damage at some point of time, right. So, this is specifically what VMBR also does.

So, what happens in a typical system? You have a hardware, there is an operating system running on top of the hardware; there are 2 applications, multiple applications running on top of the operating systems. So, this is how your normal environment look. Now, in your virtual machine based rootkit, even if you have just a virtual machine, what does a virtual machine do? There is a hardware, on top of it there is a virtual machine. On top of this virtual machine multiple OS can run today, right? So, there are lot of virtualization that is happening here. And, what I mean by virtualization? Every operating system will think that I own this machine and there can be multiple operating system running on a single machine, right and this intermediate layer which I call as a virtual machine, will permit many operating system to run on that machine. So, every operating system in very naively it looks like a process. So, I execute this process means, this operating system and all the related task in that, then go the next process where I execute that operating system and the other things. So, this is how a virtual machine basically operates.

If this virtual machine has a malaise, right? Then I am gone. That means, every operating system when a whatever; it is going to talk to the hardware, that entire conversation can be, entire flow of information that flows from the operating system to the hardware I will be in a position to capture. So, many, many attacks would love to have something that you see on the right hand side of your slide, where the attack system is something like a virtual machine monitor; which basically tries and goggles up as much information that is necessary, right. And, so, what is the nice way to get into this?

(Refer Slide Time: 04:05)



Installation

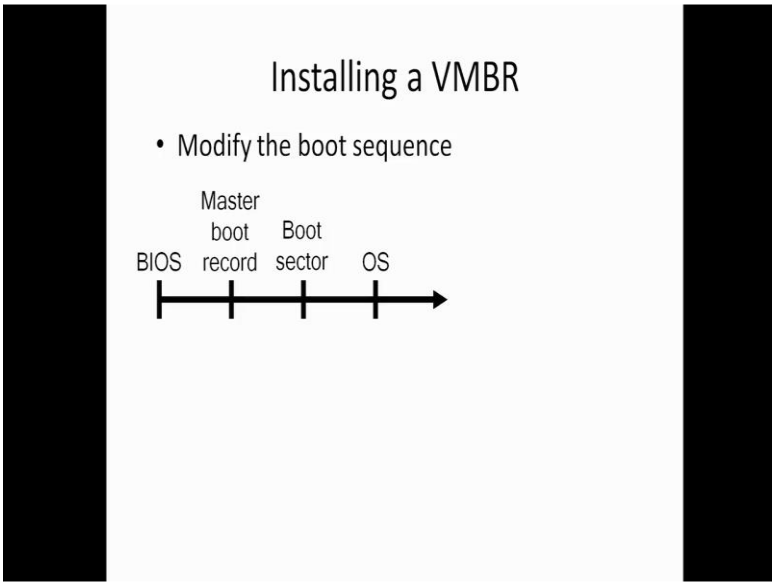
- Assume attacker has kernel privilege - How?
  - Traditional remote exploit (Stack smashing)
  - Bribe employee
  - Malicious bootable CD-Rom
- Install during shutdown
  - Few processes running
  - Efforts to prevent notification of activity

So, this is how can I get an attack system installed, this is how I can get in installed, right. I do something like stacks machine or I can go and even bribe an employee and get into my boot record. So, whenever I boot, I do not boot the target OS, but I boot this virtual machine. This virtual machine, in turn will boot the target OS. Now, if I have only one OS in the system what will happen is, when the system is booting you do not see the screen and all, right; screen will be very gobbled up and somewhere your screen just stays for another 2 milliseconds or 10 milliseconds or even 100 milliseconds we cannot even guess, this is a second.

So, what is 100 milliseconds do you know? One by 10th of this, you will not even notice it. So, what happens is, first when the system comes up your normal OS which is suppose to boot will not boot. This virtual, this you know attack system will first boot. It will sit then, it will now go and boot the OS and that transition you will never see on the screen. This humanly, the perception of this, it is not possible for the normal human being, right.

Then what happens now, then the target wise, then you think that the OS is working you never know the existences of this intermediate layer, correct and so whatever you do, that the virtual machine will monitor and it can do whatever it wants because; it finally, controls you. Correct? So, this is the concept of what you call as a virtual machine based rootkit. So, how does it come? This is very interesting. So, these are all somethings that you should know. When will a thief attack a house? When nobody is there in the house, right? So, similarly, when you are shutting; so when you do a stacks machine, come into the system, right and what you do there, you wait till somebody shuts it down. While you are shutting it down there is a shutdown process. Then, what will happen? Other point of time, I will go and write myself into the master boot record. So, when you shutdown what happens? First your screen will go blank, right and then only the LED goes, LED stops glowing after your screen goes blank. So, nobody will see what is happening, you would have shutdown the system and waiting, when it will that light will go off, I have to go home, right, correct. So, at that point of time I will go and write myself inside the software, in the master boot record, right.

(Refer Slide Time: 06:45)



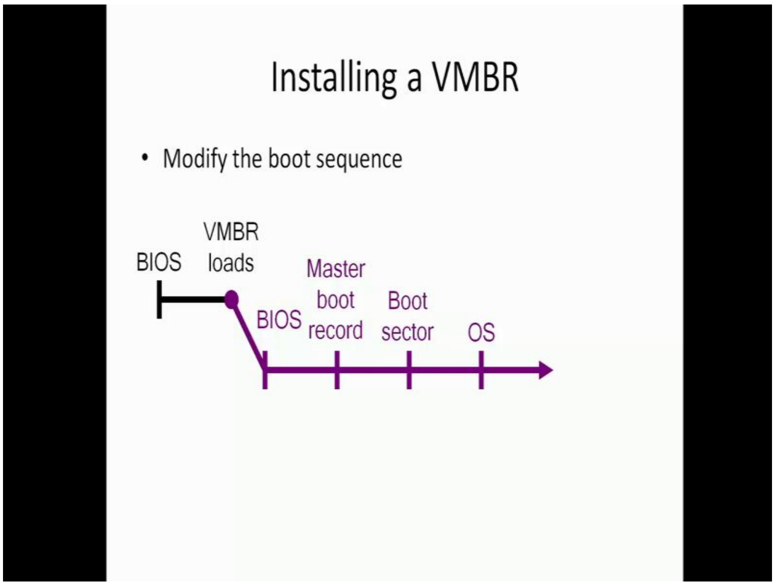
Installing a VMBR

- Modify the boot sequence

So, then what happens? So, this is how. There is a built-in operating system or basic IO system. There are 2 words by which you can talk of the bios. What is the responsibility of the bios? It will go and check memories, they are what sort of peripheral; there are lot of things it will do, bios will do.

Now, after that bios, the master boot record is copied from where? From whatever bootable device you have from that the boot sector is copied and then the control is given to the code that is copied from the boot sector and that will start executing. And, that is your OS, correct. So, this is the normal boot sequence.

(Refer Slide Time: 07:22)

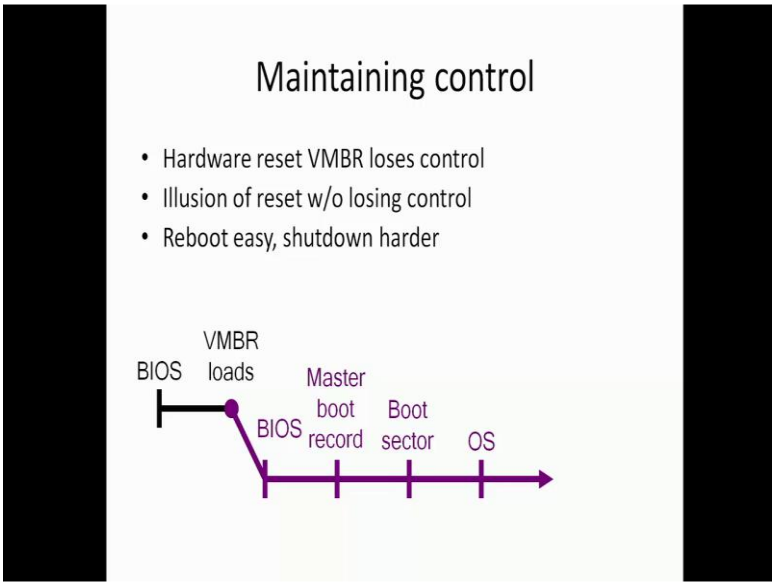


Installing a VMBR

- Modify the boot sequence

Now, what happens? Now, bios comes into existence and now, your VMBR loads. Instead of your master boot record, in that boot record now, what is there? Your virtual machine based boot kit is there. And then, what it does? It again runs the bios, code so that you get a feel that the normal thing is working, right. So, the entire thing now, there is a VMBR on top of it, again the system boots and this is like a soft boot and you will never notice; one time some sounds came, again it is coming, some times it booting, so you are happy you will hardly notice these things at the time of boot or shutdown.

(Refer Slide Time: 08:05)



Maintaining control

- Hardware reset VMBR loses control
- Illusion of reset w/o losing control
- Reboot easy, shutdown harder

BIOS

VMBR loads

BIOS

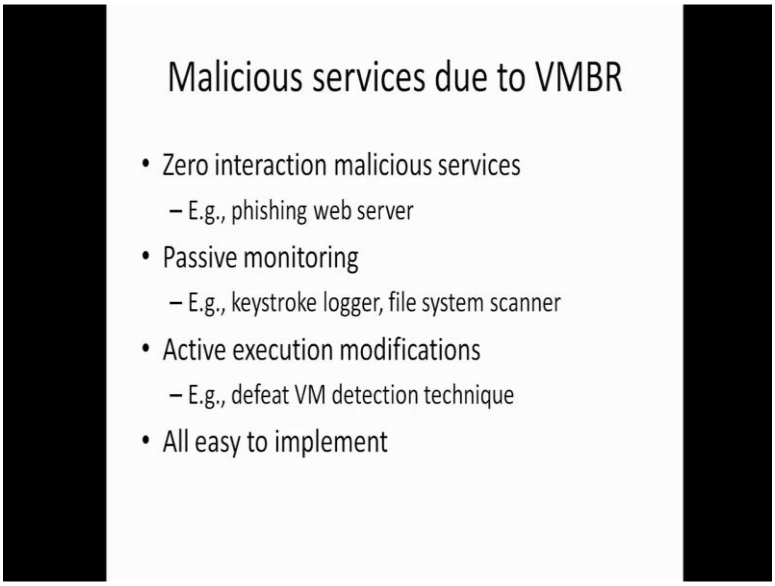
Master boot record

Boot sector

OS

So, if I do a hardware reset the VMBR again looses control. So, what it does is, it gives a illusion of a reset without loosing control. So, something like a rebooting, right. It is not that you shutdown and boot again there is a difference between that. So, there is a reboot which is much easier than a full shutdown and the VMBR will still exists and then some part of the code alone will, it will load the OS. And then, now what happens? Now, this particular thing that you see on the right hand side is now established, correct?

(Refer Slide Time: 08:54)



Malicious services due to VMBR

- Zero interaction malicious services
  - E.g., phishing web server
- Passive monitoring
  - E.g., keystroke logger, file system scanner
- Active execution modifications
  - E.g., defeat VM detection technique
- All easy to implement

Now, what happens here because of this? You will have, what can this VMBR do? Number one, it can be a zero interaction malicious services, right. What is a zero interaction? It will not interact with the main user. For example, it can be just a phishing web server. It can do, it can create a service which somebody else can keep accessing it, right. It can create a small web server, somebody else will be accessing. So, you do not know anything, like it will give you little start rendering service on behalf of the system, without you even noticing.

The next most critical thing is this passive monitoring. It will just keep scanning your file system. It will keep logging your keystrokes, right. You will never, you can basically never you will get into any of the, you will never notice it, but lot of things will come in and go out. So, that is another very interesting part. Then it can start being active also, right. It can go and say, it can defeat all, see somebody wants to detect if there is a virtual machine interpretant key, right. So, it can go and camouflage itself. So, if somebody wants to go and detect if there is a virtual machine, they will say no; it will say that hardware is direct, operating system directly running on the hardware, right. So, it can camouflage itself. And, it can stop you know, it can keep on put you know, it can go and start accessing your scheduler.

And, it can go and suppose this is happening on a networking system. It can go to the scheduler and then what it will do? It can go and screw up your entire QOS there. You have quality of service, right? Suppose, this is going on, we need a good quality of service. I can go and you know if this happens inside a network stack you know, today router. What is a router? It is actually very good, a very high end work station and it has processing. There is a processor sitting in a every network of planes. There is a stack, the same stack exist there also. There is an operating system, right. There are applications that are running on top of it. Now, I have to go into the router, I can go and I can start playing with your quality of service module, gone right. You will loose quality of service. So, lot of things can happens. So, essentially it can do a denial of service, meaning somebody can access you or it can go and kill your performance. So, many, many things are possible because of this virtual.

So, this is one way by which there could be a security penetration into your system. So, when we start why, so, what this case study tell you? Now, I have a problem which is basically originating; see please note here, that the fellow who wrote the code with that string-buffer cache is a very innocent guy, right. Now, from there what happened? I used that innocence is ignorance and we wrote a code by which we got and we got into, we smashed a stack, we enter the system and wrote one code which will be a VMBR code. And, we were waiting and when the system was shutting down we wrote that VMBR code into this master boot record and when next time when the system came up, I had, I now became a virtual monitor which is visual machine base rootkit, I am watching what you are doing.

Now, when you are actually logging in to your Gmail, then whatever, or your some email system, I take your password, right and this VMBR emails that password to some location somewhere and from there, I hack into your system. Now, whom will you blame? See, first and foremost, how do I establish this path? For me to start from the stack machine to this has been easy, but can I retrace it; is it a reversible way, can I go back say, OK, this vulnerability was exploited to get into this. Please note that, your email getting hacked and the reason for this email getting hacked are the 2 different ends of the story, right. I cannot go back from you getting hacked and trace the original source of why it happened. You got my point. So, that is the basic difficulty here. So, between the original cause and the actual effect the manifestation are so much different. It was a programming language compiler problem, which came into an architectural problem, then it came into a malicious code and then it looked at your keyboard and so.

So, whom are you blaming? So, your email account got you know, compromised, whom do you blame today now? Do you blame email? The email system, if your Gmail account got hacked, can you blame google for it? Or, you are going to blame the operating system for it? Or, you are going to get, you know the compiler for it or the fellow who wrote the code with buffer for it? Right, so, this is really the problem. You understand this.

And now, we have to solve this problem some how, right. And that is in front of us, that is why we are all computer science and the electronic engineers. Have to come out with the solution for this problem. We have created this problem and not only that we created a problem and with that problem we gave systems to the whole world and every fellow has this. And today, everybody is doing every email, e-commerce, transaction over mobile everything, you have enabled all these services. Now, there is a problem we cannot leave it, right and that is precisely what we will attempt over these set of courses.

First and foremost, in this course we will say what is it that we are going to build on architecture. In the architecture, I need these, these, these things, if these exist then I can build an operating system which will exploit this and go to the next stage. Then I will have compilers, somebody asked about canary bridge today, right. So, those type of features. Suppose, even I have those features still this stacks machine is going to be possible, that does not stop your stacks machine, right? So, even if I have a secure compiler, my operating system is stupid or still I can access it and if I do not have good access policies at the architecture level, still I can compromise this. So, things like this grow. So, we have to be extremely.

So, another thing I want to tell you here is that, if you really want to be a security expert; it is not just you know some aspect of security, right? So, to handle a situation like this you should know about operating systems, you should know about architecture, you should know about compilers, you should be sort of having a long large breath at least, about basics of each subject you should be thorough, so that you could start addressing this problem in a comprehensive way. So, this is why security becomes a very challenging field of show, right? So, set of this session what I have tried to tell you is that there is a problem in hand and that problem is sort of a very, very complex problem. I wanted to convince all of you that this is a complex problem.

So, from the next session on words, we will move on to you know, specifics of architectures, issues relating to security. Now, if there are any doubts in this session I will answer.

(Refer Slide Time: 17:29)

End of Session-5

Thank You

Student: Sir, I have one doubt related to that proxy server website. The (Refer Time: 17:43) of some services are locked, but that lock services run through proxy server website.

Ok.

Student: So, this proxy server website is a type of VMBR or it is different?

Proxy server that is again, what you want to configure the proxy servers. So, today, virtualization has become a very, very important aspect. Specifically; from a hardware utilization perspective and also from a Fault Alden perspective. See, suppose I have 2 serves today with me and I have say some 10 services, so even I have 2 services; the easiest thing is I put one fellow as a proxy server, another fellow as you know email server, but then both will be utilizing only 50 percent or 20 percent or 30 percent of this system. So, that is why you know virtualization is basically done.

And, when I do virtualization what happens? In one single server, I will put both the email and the proxy server for example, some set of services and I will have the another server as a back up to the server. So, whenever there is a issue I will switch on to this server. So, I get good hardware utilization, at the same time I will also get good amount of reliability. That is why many of the services which are not really time consumed, which are not really processor performance consuming, are today mapped on to a single server with virtualization. So, that is a decision that should be made by the organization on whether you use a virtualized server for doing some of the services. Have I answered your question?

Student: Sir, I have just doubt in that. Suppose Facebook is ban in our college and we are going and the students are logged in through using that proxy server by, but actually we really go through normal, directly Google where it cannot open, why like that?

That is a problem with your access ruled policies.

Student: Ok.

That is a problem with your access rule policies. So, you have to go and work on the access rules properly, Ok.

Student: Ok.

So, that is where somewhere indirection is basically allowed, but direct access is not allowed; something close to this. So, this is an access rule policy of how you configure your whatever fire wall. So, fire wall configuration we talked a bit about in the previous course, but we will have one dedicated information security 6 is going to talk about policies and one of the last session of this particular course we will talk about network appliances and the security for that network appliances. And subsequently, the operating system course will also talk about networking operating system and then the last course will talk about policies. So, if you understand the networking hardware in this course which will be the last session, then you go and understand the network operating system in one of the intermediate courses and then you also sit through the policy you will get broader guideline on, how to you want Facebook to be accessed or not accessed? That is my question. Are you student or a teacher?

Student: No, no sir, just asked an example. Sir, I am just asking.

No, no what do you want? I can teach that. You want Facebook to be accessed like that or not. So, I will teach both how to stop and how to enable also.

Student: No, no.

Yes, yes.

Student: We want to stop it.

No, no. Your student will hit me. I should be popular even among your students. So, I will teach you both.

Student: Ready, sir.

Yes, yes sure.

Student: Ok, sir.

Yes, yes.

Student: Thank you, sir.

Yes, any other doubts? Any other questions?

Student: Yes.

Yes.

Student: Actually, I had a doubt.

Yes.

Student: Sir, regarding this, the diagram where we show how (Refer Time: 22:11).

Yes.

Student: Can you change that slide?

Yes, I have put that. Yeah.

Student: Sir, so, once now may be (Refer Time: 22:24) memory.

Yes.

Student: Is it not (Refer Time: 22:29) executive the bios once again.

Yes.

Student: It would be very difficult again here. So, I did not get this point why VMBR again possible to, why is it possible for VMBR to execute bios?

See, bios today is not just basic, it has become see off, like it has become complex today. See, there are certain things that are very configuration specific, so when we deal with the operating system we will tell you more about it; I need to cover lot of background to basically tell you. But, as of now the answer is that there are certain configuration parameters that get us really screwed up because of the loading of the VMBR, instead of the master boot record. So, I need to do the entirely the same thing, but on top of the VMBR. So, when I execute the bios there are certain things, again setup and then the real master boot record also comes, so there is some sequence dependency between bios execution and the master boot record executing immediately after that, And, that I have to mimix so that I have to redo it, so that my operating system works perfectly well and there is lot of things that the operating system is dependent upon that.

So, this is basically to configure your system properly that I execute bios again, but it is like a soft reboot, soft reset. See, there is a difference between hard reset and soft reset. When we do the OS course, we will give you much more detail on that, but in both the cases there is some component of the bios that runs. In the hard reset, there are lot of things that are done including basic peripheral checking, but in a soft reset there is some prospect of bios that is run, but not the entire bios. So, this is precisely what we mean by this sequence.