Ethical Hacking
Prof. Indranil Sengupta
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture – 46
Elements of Hardware Security

In this week we shall be starting our discussion on a slightly different kind of topic which relates to hardware security. Now when we talk about a product, when we talk about securing a product there are actually two aspects to it. One is of course, the software that goes into it and the conventional ways to secure things, to talk about security, to talk about breaking into a system, we actually implicitly talk about the software part of it.

But, also there is a hardware involved and there are some unconventional ways in which people can try and break into a system through the hardware backdoors. So, in this lectures we shall try to talk about a few things about that; so the topic of our discussion is Elements of Hardware Security, ok.

(Refer Slide Time: 01:09)

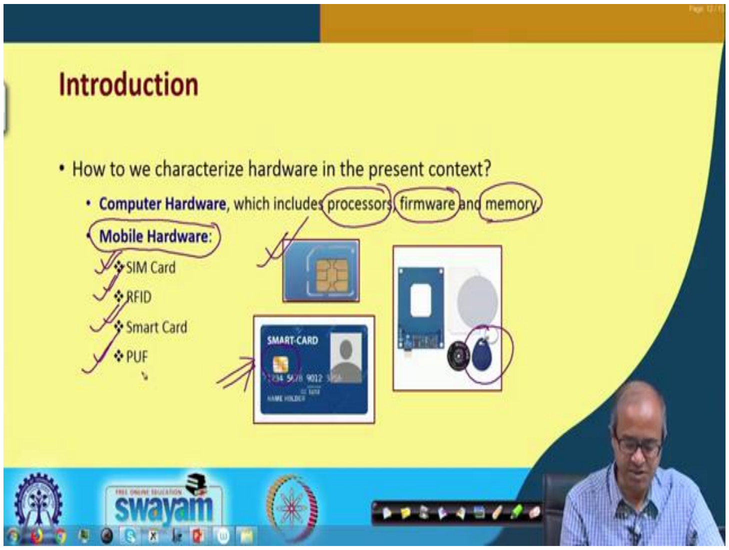
CONCEPTS COVERED

❑ Attacks on hardware

❑ Typical countermeasures

Now, in this lecture we shall be talking about some general attacks on hardware and some of the typical counter measures that we talk about ok.

(Refer Slide Time: 01:21)



Introduction

- How to we characterize hardware in the present context?
  - **Computer Hardware**, which includes processors, firmware and memory
  - **Mobile Hardware:**
    - ❖SIM Card
    - ❖RFID
    - ❖Smart Card
    - ❖PUF

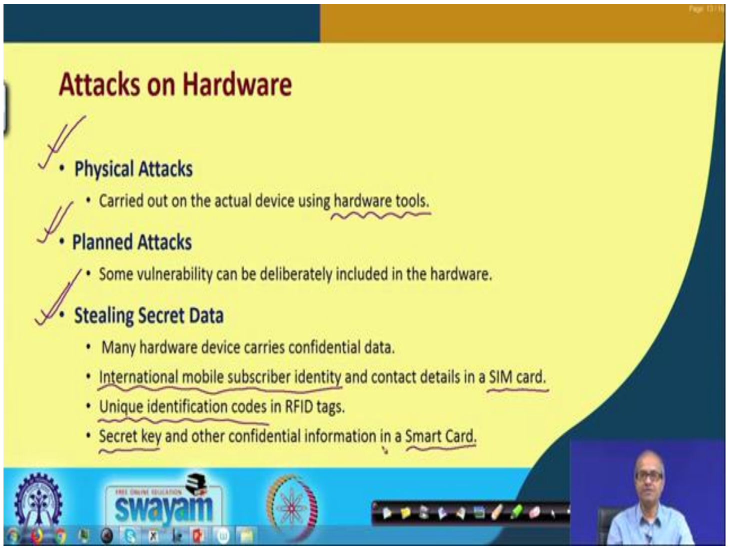
Now, let us see what do you mean by hardware security in the generic sense? When you talk about hardware, well most of the time when we talk about hardware, we actually referred to computer hardware, the computer system. Now, in a computer system what are the things that are there? We talk about the processor, the CPUs, the different levels of software and of course the memory systems. Broadly speaking a computer hardware involved these three things. Firmware means some memory devices where some software are stored.

So, it is a combination of hardware and software you can say. Nowadays we are seeing a great proliferation of mobile, handheld devices. So, this mobile hardware is also coming in a big way in terms of their applications and applicability. Now we all use SIM cards in our mobile phones and various kinds of device today, so you have all seen how was SIM card looks like. A SIM card is a small micro chip where a lot of information is stored in addition to some sophisticated micro chips where also some local processing can be done.

There is something called Radio Frequency ID or RFID devices, these are the so called RFID tags; so you can attach RFID tags to various kind of devices and you can monitor you can locate those devices offline without any physical touch. In a wireless way, you can search for those devices. Then of course, we all use different kinds of Visa or Master Card, ATM card; these are generically called smart cards. Now in a smart card again there is a small microchip you must have seen where there are some circuitry and also some computation capability; when you insert a card some computations can also happen locally in this microchip.

Well and we shall see later, we shall talk about this later; there is something called physical unclonable function in short PUF which can be used to secure hardware products in a very flexible way. This is a new concept and people have been increasingly using this concept of PUF to have better security with respect to this hardware devices, ok.

(Refer Slide Time: 04:08)



Attacks on Hardware

- Physical Attacks
  - Carried out on the actual device using hardware tools.
- Planned Attacks
  - Some vulnerability can be deliberately included in the hardware.
- Stealing Secret Data
  - Many hardware device carries confidential data.
  - International mobile subscriber identity and contact details in a SIM card.
  - Unique identification codes in RFID tags.
  - Secret key and other confidential information in a Smart Card.

So, moving on; talking about the various attacks on hardware that are possible, let us try to make a categorization. Firstly let us talk about physical attacks where we are actually making some kind of intrusive attack on the device. What do you mean by intrusive attack? Let us say we are breaking the device, we are breaking open, we are removing the cover or the protective layer on top, something like that; we are making a physical kind of an intrusion in the device, physical attack. These are typically carried out on the actual device like for example, if I have my SIM card and I want to see what is inside the SIM; I can break open my SIM, I can scratch some upper layer and so on and so forth.

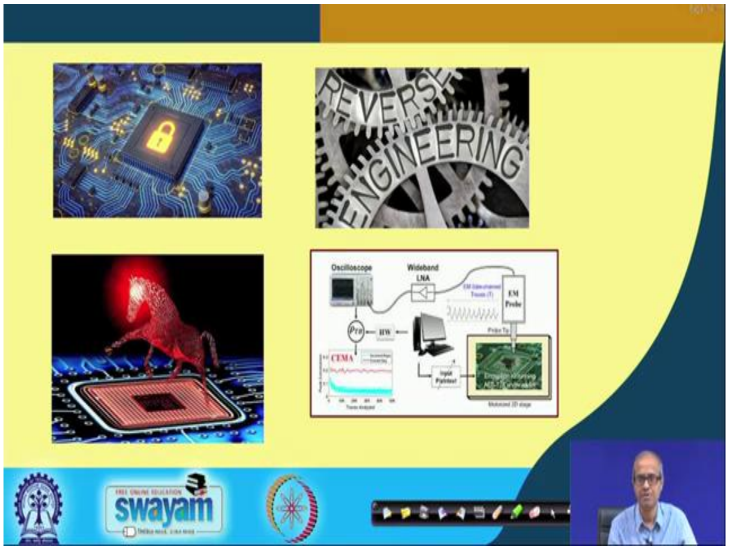
And this required some sophisticated hardware instruments and tools ok. These are not very easy to do; this is required very sophisticated tools. There is another kind of an attack which, ok; here we are all talking about hardware based attacks; these are called planned attack. Planned attack means suppose I am deploying or I am marketing some devices; let say I am manufacturing TV sets; I am selling them in the market. Now, what I do? Deliberately, I am inserting some vulnerability in my TV sets, so that I can remotely do something which the customer who is buying the TV set is not aware of.

For example, if the TV comes with the built in camera, I can switch on the camera and see what is going on in the living room whenever I want to from a remote place, ok, something like this. These are called planned attack, because these kind of vulnerabilities are put inside the manufactured hardware well in advance in a planned way. These are deliberately included in the hardware right. And of course, there is another kind of an attack where you are trying to steal some data from some device where some data stored. For example, in SIM card lots of contacts are stored; in my credit card my credit card number and other credentials may be stored and so on.

So, there are many hardware devices which can carry this kind of confidential data. And when you talk about stealing, it means how someone is taking out the data from this kind of devices. Like when you talk about SIM card, there is something called International Mobile Subscriber Identity: IMSI. This is a unique number; someone can steal that from my mobile number, so that someone can try to clone it; then for RFID tags also there is something called unique identification code. Every RFID tag has a unique code associated with it; someone can steal that; someone can forge an RFID code with the same code to duplicate it.

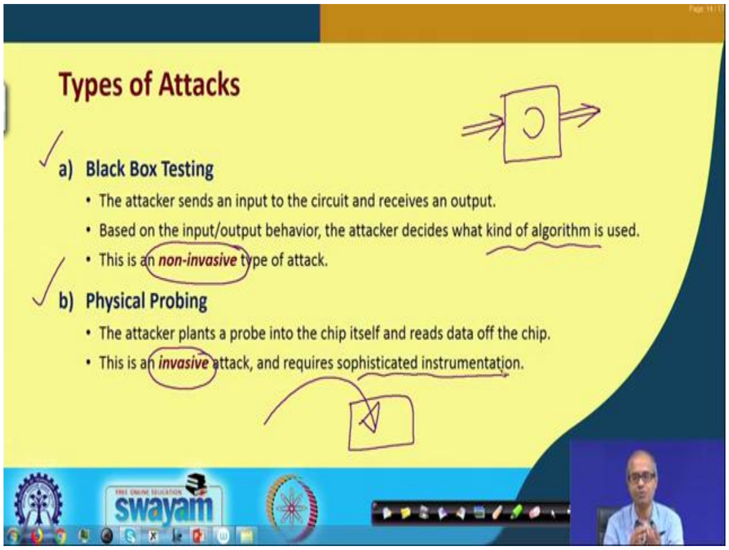
And, again insert a smart card there can be some secrete key information and other confidential information like my CVV number, my card number, etc. ok. All this things can be there. So, when I am saying stealing secrete data, they involve trying to take out or steal these kind of data ok.

(Refer Slide Time: 07:53)



So, here have some pictures; this is a pictorial depiction of a Trojan; something called Trojan we should be taking about. This is a pictorial depiction of how you are securing a hardware; this is a very commonly used concept we shall be taking about. This called reversed engineering and this is some kind of a planned attack which we carry out on a device using some laboratory instruments, as you can see like an oscilloscope, like some other probing devices and so on ok. These are something which we shall we talking about in some detail in the later lectures.

(Refer Slide Time: 08:34)



Types of Attacks

a) **Black Box Testing**

- The attacker sends an input to the circuit and receives an output.
- Based on the input/output behavior, the attacker decides what kind of algorithm is used.
- This is an *non-invasive* type of attack.

b) **Physical Probing**

- The attacker plants a probe into the chip itself and reads data off the chip.
- This is an *invasive* attack, and requires sophisticated instrumentation.

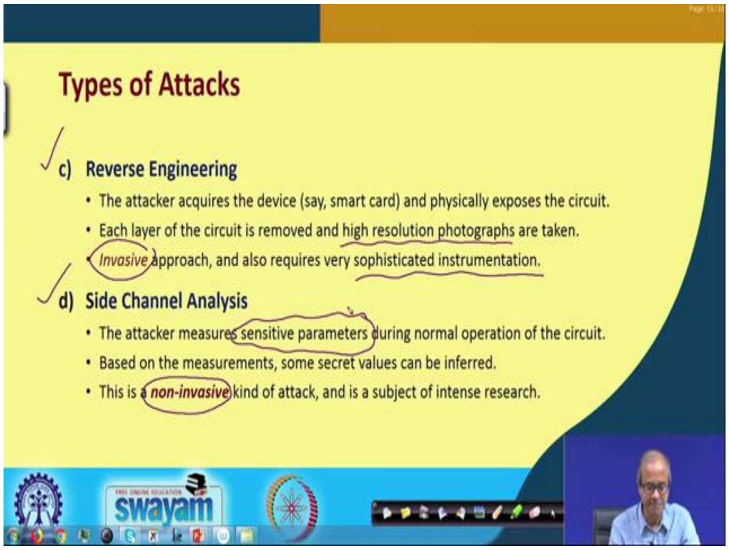
Now, the types of attacks that can be mounted on a hardware device; depending on the complexity first we can talk about black box testing where you do not know or we do not know anything about the internal details of the circuit or of the device. We are not carrying out an invasive attack; we are not breaking it open. So we have a device; we leave it as it is. What you can do? We can apply some input from outside and you can see what output it is generating; just from the input output behavior we can try to obtain some information about the device ok. This is black box attack or black box testing.

The attackers sends an input to the circuit or device and gets the output, depending on this input/output behavior the attacker can decide what is going on inside. What kind of algorithm is being run and if it is a cryptographic operation sometimes the attacker can also try and guess what is the secret key that is being used. This kind of an attack is a so called non-invasive type of an attack, because we are not disturbing the device; we are not breaking or damaging the device ok. These kind of attacks are called non-invasive attacks.

Secondly, comes physical probing where I have a device with me and I am actually breaking it open in some way, so that I can probe inside and see what is happening. Maybe I have an IC chip; I am removing the top plastic cover on the IC chip and using a very powerful microscope or using some kind of a probe, I am seeing what is there inside the chip. This is called physical probing ok.

Here the attackers plants some kind of a probe, it depends on the sophistication of the mechanism; what kind of probe you are talking about into the chip itself and tries to read or retrieve some information that is present inside the chip ok. Since here you are breaking open the chip; you are making some kind of a damage in the physical packaging of the chip, this is a kind of an invasive attack. And obviously, this required very sophisticated instrumentation; if we try to break open a chip with an hammer your entire chip will get destroyed; you cannot do anything alright ok, fine.

(Refer Slide Time: 11:31)



Types of Attacks

c) **Reverse Engineering**

- The attacker acquires the device (say, smart card) and physically exposes the circuit.
- Each layer of the circuit is removed and high resolution photographs are taken.
- *Invasive* approach, and also requires very sophisticated instrumentation.

d) **Side Channel Analysis**

- The attacker measures sensitive parameters during normal operation of the circuit.
- Based on the measurements, some secret values can be inferred.
- This is a ***non-invasive*** kind of attack, and is a subject of intense research.

Now, the third kind of an attack which is very sophisticated, this is called reverse engineering. Now, for those of you who have some idea regarding how an IC chip is fabricated; you may be knowing that you start with the silicon base that is called an wafer and on a silicon wafer layer by layer we put lot of depositions. There are various layers which are put like diffusion, polysilicon, metals, contacts. So, it is like a building that is being constructed on top of that silicon wafer.

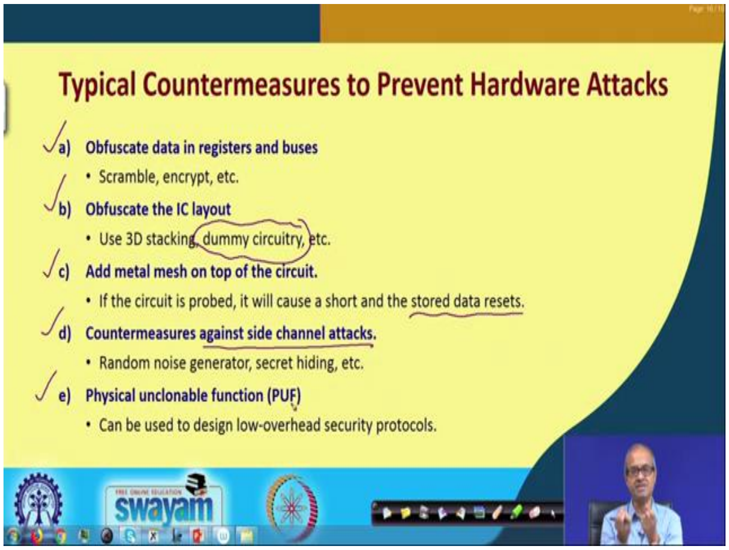
And, if someone using a very powerful microscope takes a picture of the chip from the top, the picture that will be getting is only about the uppermost layer, because the others layers are hidden inside right. Reverse engineering says you take a picture from the top; you get the picture of the uppermost layer; how the layer is made; then using some kind of chemical you remove the top layer.

Then you took another picture; you get the picture of the next top layer again remove it, again take a picture you get the next layer. So, layer by layer you are exposing the chip, you are exposing the design. So, once you do this; someone can replicate the fabrication process and can clone a chip. So, you can steal the design of a chip and you can make a duplicate; you can fabricate it yourself if you want. This is called reverse engineering. And of course, removing the layers one by one and taking photographs and getting information is an extremely sophisticated process. And, you need very sophisticated instrumentation for this reason and you need very high resolution photography ok.

Well and a relatively new and very interesting, and of course, reverse engineering is obviously invasive because you are destroying everything layer by layer. The last one we talk about is called side channel analysis; this is relatively new. Side channel analysis is also non-invasive, we are not damaging the device. What we are doing? We are saying that let the device operate; we are not, we are watching the device from outside. And, we are doing some measurement; we are measuring some sensitive parameters; we shall see later what these parameters are.

These parameters can be temperature; it can be power consumption, current drawn from the power supply, electromagnetic radiation and so on and so forth. We are trying to do some measurement; and variations in this measurements trust me we will give you lot of information about what is going on inside the chip. Particularly for cryptographic algorithms that are running inside the chip, you can very easily break the algorithm in many cases, if the designer is not careful enough, ok. This is what is meant by side channel attacks or side channel analysis.

(Refer Slide Time: 15:00)



Typical Countermeasures to Prevent Hardware Attacks

a) Obfuscate data in registers and buses
   - Scramble, encrypt, etc.
b) Obfuscate the IC layout
   - Use 3D stacking, dummy circuitry, etc.
c) Add metal mesh on top of the circuit.
   - If the circuit is probed, it will cause a short and the stored data resets.
d) Countermeasures against side channel attacks.
   - Random noise generator, secret hiding, etc.
e) Physical unclonable function (PUF)
   - Can be used to design low-overhead security protocols.

Some of the typical counter measures that people have talked about or have come up with to prevent this kind of hardware based attacks; some of which I have just listed here. The first one says obfuscate data in registers and buses. Obfuscate means to hide them, to crypt them in some way. Suppose I am trying to store some data; I am not storing the data just like that; I am storing it in some kind of an encrypted form so that even if someone reads it will not understand what is that ok. This is called obfuscation.

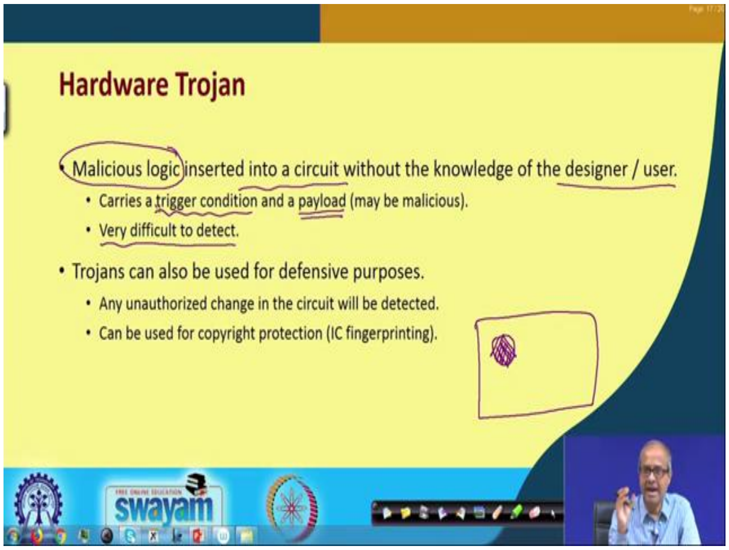
We try to obfuscate this sensitive data that we are storing inside the chip. We do some kind of scrambling, encryption stuff like that. Not only that to prevent this reverse engineering we just now talked about, we can also obfuscate the IC layout. For person who will try to do this kind of reverse engineering, we were trying to confuse that person. We are using 3D stacking that means instead of a single chip we are putting chips one on top of the other.

So, that the problem of reverse engineering becomes more complicated; there are a lot more number of layers to go through. And secondly, we can introduce some dummy circuitry which can confuse the person who is trying to reverse engineer. As a designer I am deliberately putting some dummy circuitry and I know how to activate it, how to deactivate it. But the person who is attacking may not be knowing that; that is how I can secured the device to some extent.

The third one is interesting; we can put some kind of a metallic mesh on top of the IC, so that if some kind of a probe is tried to be put in; some kind of an invasive attack is tried; there will be an immediate short circuit in that mesh, metallic mesh. And, whenever there is a short circuit all this stored data will automatically get deleted; that is how the chip is designed. So, the person who is trying to probe to get out some data, the entire purpose will get defeated ok.

Similarly, there are some counter measures which have been proposed against side channel attacks; some of these we shall be talking about in some detail, random noise generation, secret hiding; we shall talk about this later. And of course, physical unclonable function, we talked about this; just the name we mentioned PUF. PUF is a concept, a device which can be used to design this kind of hardware security measures in a very robust and safe way; we shall see all this is later, how these are done.

(Refer Slide Time: 17:58)



Hardware Trojan

- Malicious logic inserted into a circuit without the knowledge of the designer / user.
  - Carries a trigger condition and a payload (may be malicious).
  - Very difficult to detect.
- Trojans can also be used for defensive purposes.
  - Any unauthorized change in the circuit will be detected.
  - Can be used for copyright protection (IC fingerprinting).

When there is another thing called hardware Trojan which is also becoming important. Trojan, you know from the ancient story of Greece, you know the Trojan, the story of the Trojan horse, the name came from there. Something is hiding inside something else; there is some kind of malicious logic let us say; malicious logic that is inserted inside a circuit. Suppose I am designing a circuit which is supposed to perform some functions. I deliberately add some additional circuit; means I or someone else; may not be I; may be some malicious entity is adding some extra circuit to my original circuitry.

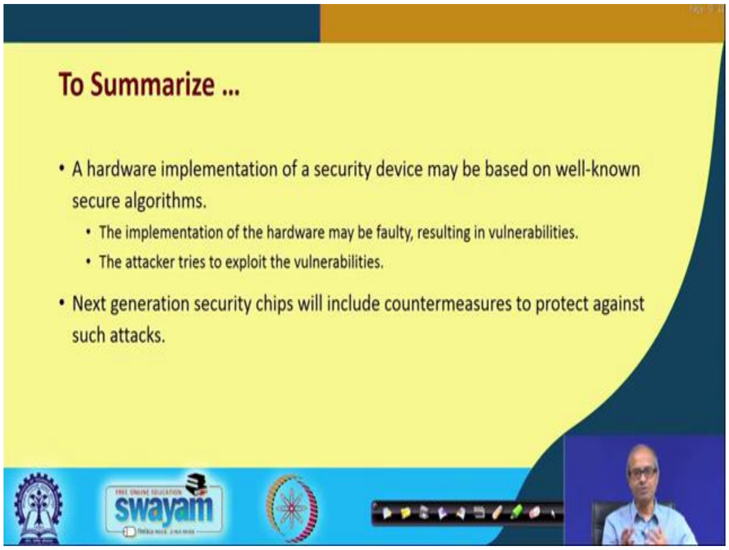
Well without the knowledge of the designer or the user let us say; that as a user I do not know that this has happened where someone else put some additional circuits inside my design. Now, when I am using my circuit, using my system, it may happen that there can be some triggering condition when this hardware Trojan can wake up. This hidden circuitry can wake up and some payload, payload means some action which will be initiated, which will be a malicious action, may be something will get deleted, something else will happen which is not intended.

This is something which is the purpose of this so called hardware Trojans. Something is, something is hiding inside a hardware; sometimes it can wake up and it can carry out some malicious activities. Because, it is hiding inside the hardware without the knowledge of anybody, this is extremely difficult to detect. Of course, there are some attempts to detect it, but in general it is very difficult, ok. This is how we, I mean an attacker can use Trojans to do something malicious. Well, this Trojans can also be used from the other side; from the ethical side also; like you can also use it for defensive purpose. Like when your design an IC chip, you want that someone should not steal your design.

So, you deliberately insert a Trojan yourself whose behavior will only be known to you. So, someone else who is copying your design will also coping the Trojan along with that. So, whenever the Trojan wakes up that person will not know what to do with that Trojan ok. So, it will be unusable; the circuit will become unusable. And, also as I said this is used for copy right protection; some time it is called IC fingerprinting. Well, I suspect someone has copied my design, but I have no way to prove it.

But if I have a Trojan that I planted in my design, I can always find out whether that design where which I am suspecting is a copy of mine also has that copy of Trojan there. If I find then I can always say that well it is a copy of my design. So, I can use some kind of copyright protection of my design using this kind of techniques ok.

(Refer Slide Time: 21:32)



To Summarize …

- A hardware implementation of a security device may be based on well-known secure algorithms.
  - The implementation of the hardware may be faulty, resulting in vulnerabilities.
  - The attacker tries to exploit the vulnerabilities.
- Next generation security chips will include countermeasures to protect against such attacks.

So, to summarize the hardware implementation of some algorithm that goes inside the security device, this is of course, based on some well known algorithm; typically some cryptographic algorithm. The point is these algorithms are known to be very good, but the way they are implemented in hardware that may not be very proper; that may have some vulnerabilities or weaknesses.

So, this is the implementation that we are targeting; implementation of the hardware may be faulty in some way which results in vulnerabilities. And, attackers try to attack vulnerabilities in various ways, just like software vulnerabilities. Whenever someone designs software there will always be some bugs; the attacker always tries to find out bugs and tries to exploit that ok.

So, the next generation security chips that will come out already people are working on it. They will include counter measures to protect against as many of this kind of attacks as possible; this is the basic idea ok. So, in the next few lectures we shall be going into some more details about the various kinds of hardware based attacks and some of the counter measures.

So, with this we come to the end of this lecture, where we have just giving a bird’s eye view, a very brief introduction to various kinds of hardware based attacks and some of the countermeasures people have talked about in this regard.

Thank you.