Advanced IoT Applications
Dr. T V Prabhakar
Department of Electronic Systems Engineering
Indian Institute of Science, Bangalore

Lecture – 28
Device Security Part -1

So our next goal in this course is to understand: what are the current trends in security of IoT networks and therefore, IoT devices. So, you may be wondering that why am I talking about networks first and then why am I talking about devices in the next step. Thing is the IoT networks where you know an network of IoT devices are communicating; is a well understood area people have looked at DDOS attacks for instance: Denial of Service and Distributed Denial of Service.

You know vulnerabilities arising due to stealing of keys and so on and so forth. Recent story if you look at which happened in October 2017 appeared in a article is related to the vulnerability of you know Wireless Protected Access 2: WPA 2. And the authors there demonstrated that you can reinstall the key right. And such a vulnerability was referred to as the KRACK vulnerability, KRACK; k r a c k KRACK vulnerability. If you Google you will find lot of literature on this particular vulnerability. And there it is interesting that you know like wireless WEP as it was called, forget the expansion. WEP was something that it was it called Wired Equivalent Privacy, I think so it was called wired equivalent privacy was broken.

And people made a huge noise about tenset its doomsday and it is going to be a problem, because several Wi-Fi devices use WEP and all that, but nothing happened. Then came in WPA they were vulnerable vulnerabilities in WPA soon replaced with WPA 2 right wireless protected access. And, now this KRACK vulnerability that appeared seem to have shaken up several people and said what do we do with this; this is a something that a quick patch has to be released. So, that the four way handshake with which WPA starts off is a source of vulnerability where the key can be reinstalled ok.

So this is a so this is going to keep happening. You will see if it is today if it is KRACK as a vulnerability, tomorrow it is going to be something else. So, I do not think there is much you can do as and when. So the problem with KRACK; if you look at very carefully it is not so much with respect to any human related problem. It is a problem

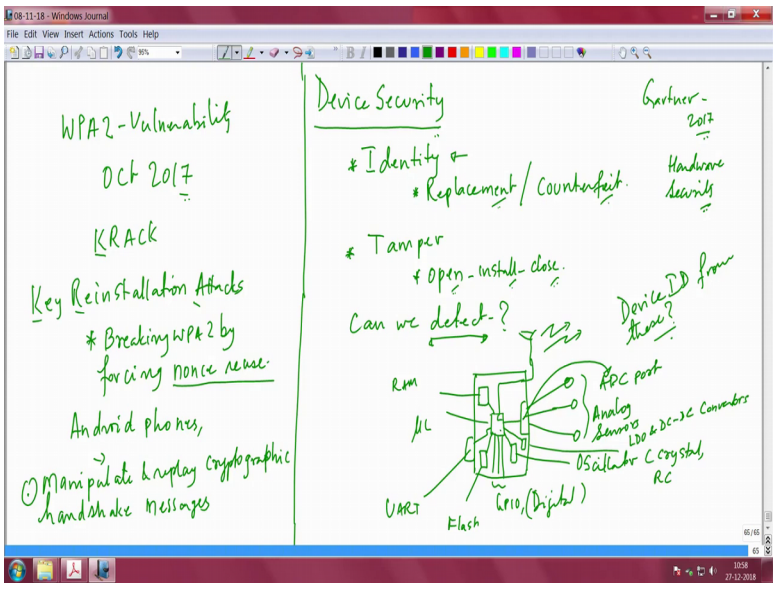
with the WPA standard itself, WPA 2 standard itself. It is more a protocol vulnerability it is a standard vulnerability, it is a WPA standard based vulnerability.

Like GSM in the old days when GSM had vulnerabilities right. The base station in the GSM world always trusted the mobile phone always ensured that the mobile that is connecting to it is really the right one the genuine one. But there was no way for the mobile phone to check whether it was one way authentication; so that was an issue. So, that is nothing you can do about it because that is part of the, it that was part of the GSM standard.

Quite like that KRACK is also like a standard vulnerability and tomorrow or something else will come. So, I do not think you can do much in that space and it is not in your control on inventing something and then trying to change the way things are happening in on a global front. But what you can do is what we should worry about.

What is within your purview and what is your ingenuity in trying to solve local problems at the nod problem. At a IoT network maybe you cannot do much because that is all about CPS security CPS research and all of that. But at least at the device level is there something you can think of seriously ok.

(Refer Slide Time: 05:39)



So, if you look at device security there are two things that occur to me right. One thing is related to identity, you want to ensure that the device is indeed the right one ok; which

means it should solve problems of if you have a unique identity it should solve the problem of replacement, it should solve the problem of counterfeiting.

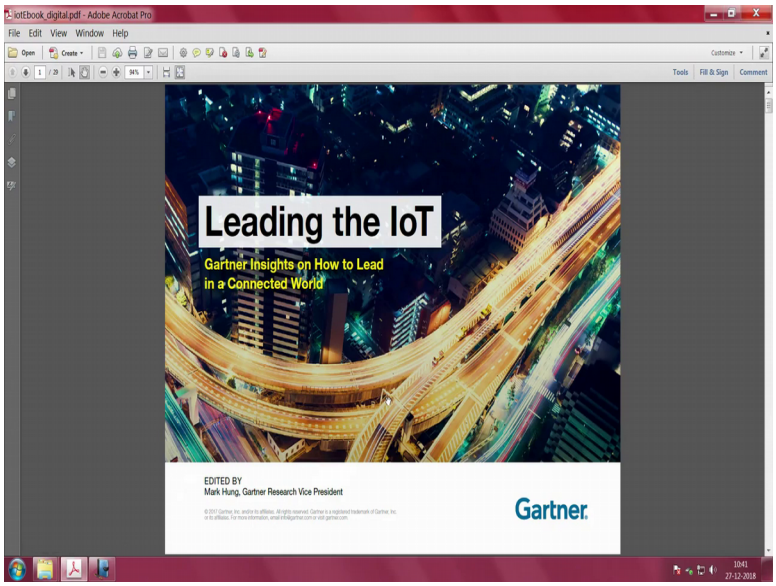
So, counterfeiting and all; that means, it is the right one it is indeed there is no replacement hardware identical exactly looking hardware is not replaced. And therefore, you know that it is indeed this device and nothing else. Is there something in this space in device security that you can think about that is one part.

The second part is on tamper can you do anything with respect to tamper resistance ok. Essentially open install something and close it back right. So, this is what would typically happen in a tamper case. So, you should be able to detect this in the in the lowest possible time. And then you should be able to say yes here is a device which is compromised something was opened something was installed and people have put back the screws.

And therefore, this is not the not to be trusted anymore because there is a compromise on the device. These two things is what we should perhaps focus on and understand what can you do in this space. In fact, this is an area which is becoming extremely hot and people are trying to look at solutions in the space. I will show you I recent IoT Gartner report Gartner ok.

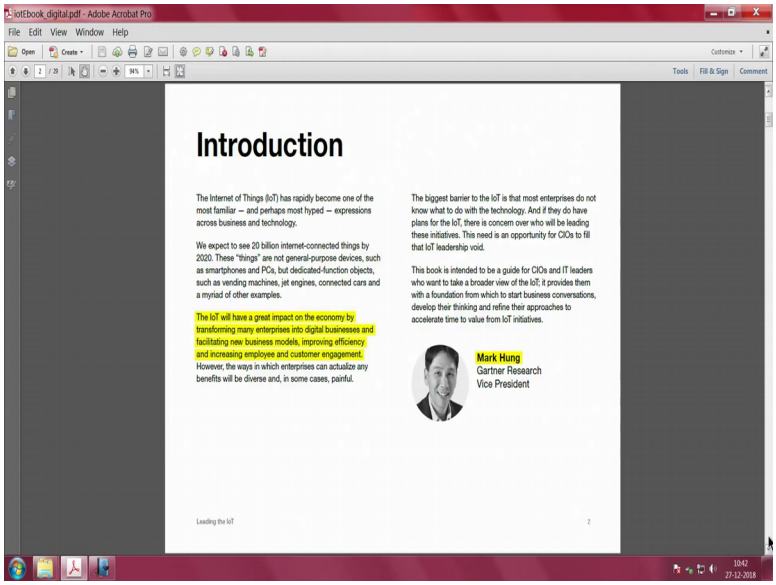
There is a Gartner report which was published in 2017 which essentially brings to forefront this problem of device security; which essentially means hardware, hardware security essentially about hardware security um. So, let us see that article and go through it in detail which will give you some idea.

(Refer Slide Time: 08:09)



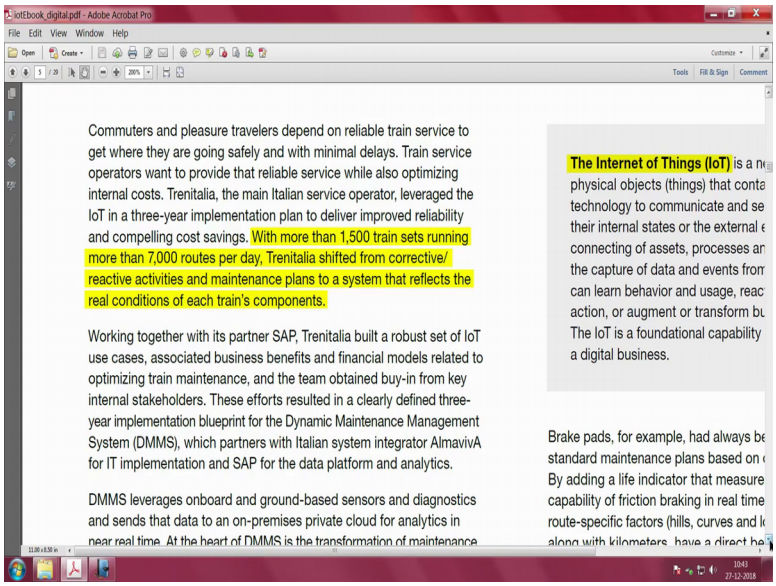
This is the article which was published by Gartner as I said it was published in 2017 you can easily download this and read it ok.

(Refer Slide Time: 08:19)



There is a lot of stuff out there which is not important for this course, but nevertheless it is a good read.

(Refer Slide Time: 08:31)

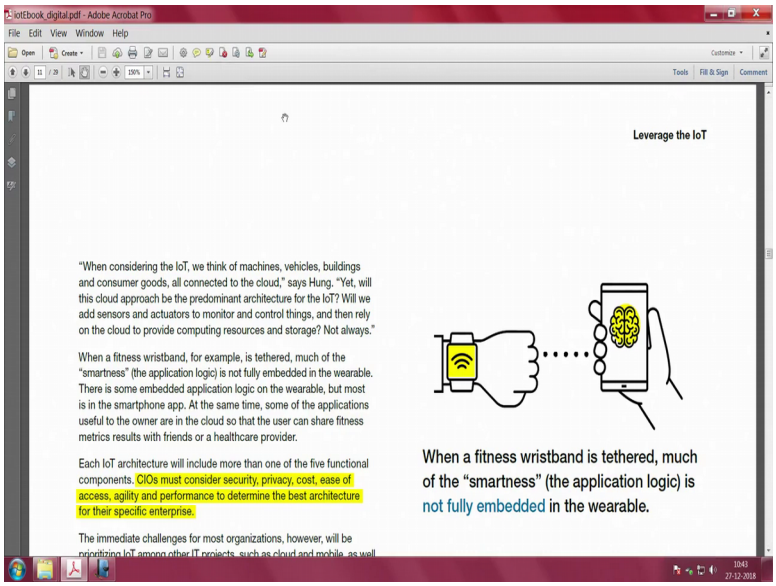


Let us go to where all IoT has been applied and where people are seeing fast returns. This is the left side here the one that is highlighted here maybe I should expand it a little bit let me make it 150 percent or even maybe a little more 200 percent. This will allow you to read little bit in detail what is written here it says this is a company which is a railway company Trenitalia it is using a 3 year implementation of IoT.

And it is basically for improved reliability and cost cuttings and cost savings. You can see more than 1500 train sets running more than 7000 routes per day, Trenitalia shifted from corrective or reactive actives. And maintenance plans to a system that reflects the real conditions of the of each trains component.

So, even in critical sectors transportation sectors like mass transport and trains IoT has been applied. So, so the impact of device security on when you install such devices in a where places where mass transport is involved is indeed a very important aspect ok. So, it goes on with this you can read this article and we will just go to the most important aspect of this article.

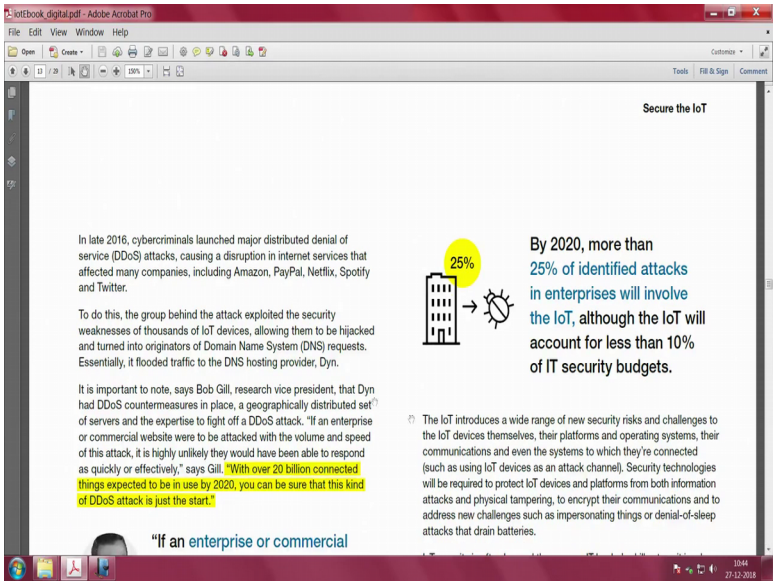
(Refer Slide Time: 10:03)



Here is an important sentence which perhaps allows you to get a feel of what is being said. Each IoT architecture will include more than 1 of the 5 functional components which is already described in this article CIO's must consider security privacy cost ease of access agility.

And performance to determine the best architecture for their specific use for their specific enter enterprise. So this is giving you a precursor on what is being said and then comes the security.

(Refer Slide Time: 10:39)



Here in this sentence I can expand it a little bit several cyber criminals who launched attacks and all that DDoS which I already mentioned to you. By the way before I move on I will just write down this the if you are if you are interested in further reading please look up WPA 2 vulnerability which was brought to our notice in 2017 right.

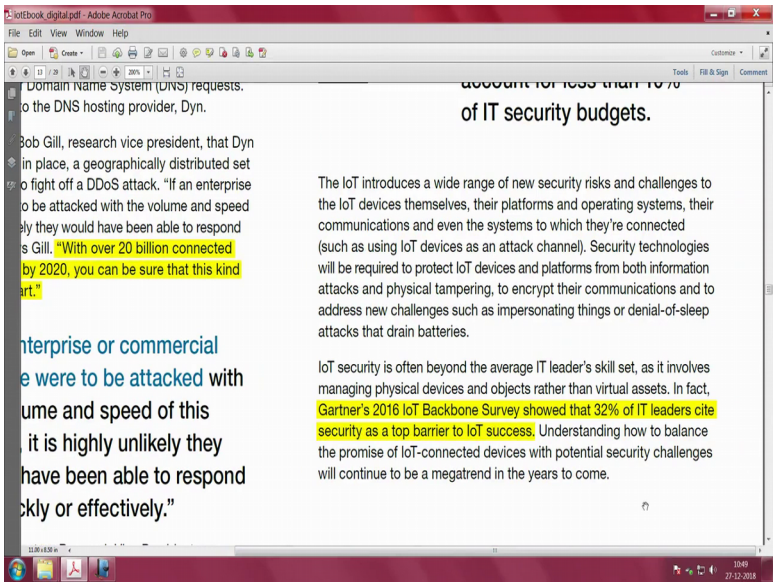
And, essentially this the vulnerability people talk about is KRA KRACK right. Key re installation attacks right this is you can look up this article and this article will exactly tell you what is the vulnerability associated with the WPA 2. And how one have the authors have shown that you can break they call it breaking WPA 2 by forcing nonce reuse.

So, this will already tell every experts what exactly this attack is all about and please read an article carefully. Why is this important to be read? Because this affects IoT devices particularly Android phones, Linux, Android all of them you can see that they have this vulnerability and you can bypass WPA2; so, it is an important thing.

So, please do spend time reading about how the how one manipulates, how you can easily manipulate, manipulate and replay crypto graphic handshake messages ok. So, you can look up the four way handshake in WPA 2 and what is it is practical impact and all of that. So, please do spend time because I do not want to get into the detail of KRACK as this is not really the focus of this module.

So, let us come back to this IoT security; here you can see that with over 20 billion connected things expected to be by 2020 you can be sure that this kind of attack is just the start. So, several problems are going to be there in all these IoT devices. And so CPS kind of attacks are something that you cannot do at all, you cannot KRACK will be replaced by something else as I said.

(Refer Slide Time: 14:59)

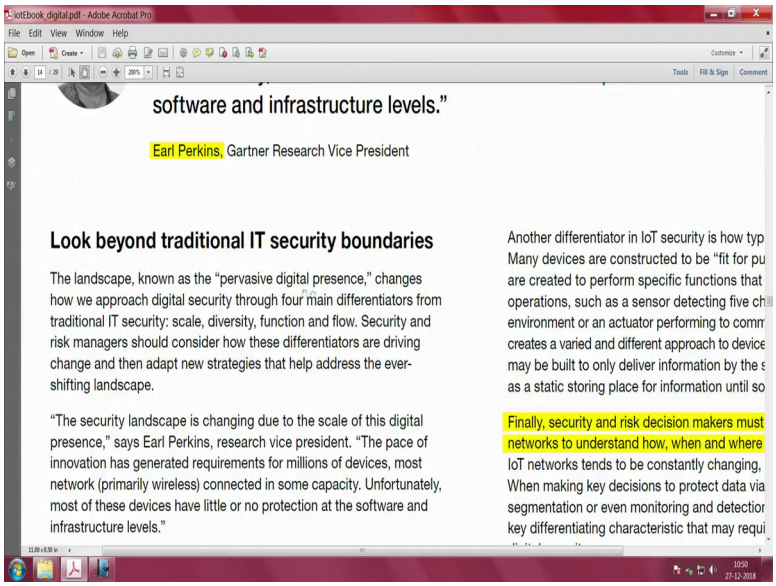


So, you cannot do much and you just have to ensure that somehow patches you have to follow the area apply patches as and when they are announced. And ensure that your devices are kept as secure as possible ok. Then the also you should make efforts to see how one can solve this problem right; having said that the real focus in this module is not that so I do not want to spend too much time there.

But here is a very important statement and perhaps the biggest problem and biggest hurdle for IoT deployments; is 20 billion devices that people are talking about is not likely to happen at all by 2020 it is not going to happen. At best you may get 6 billion or 7 billion devices 20 billion will not happen, why? Security is a major problem in IoT, anything you do any you know IoT solution you are looking at it has to be a core design with security.

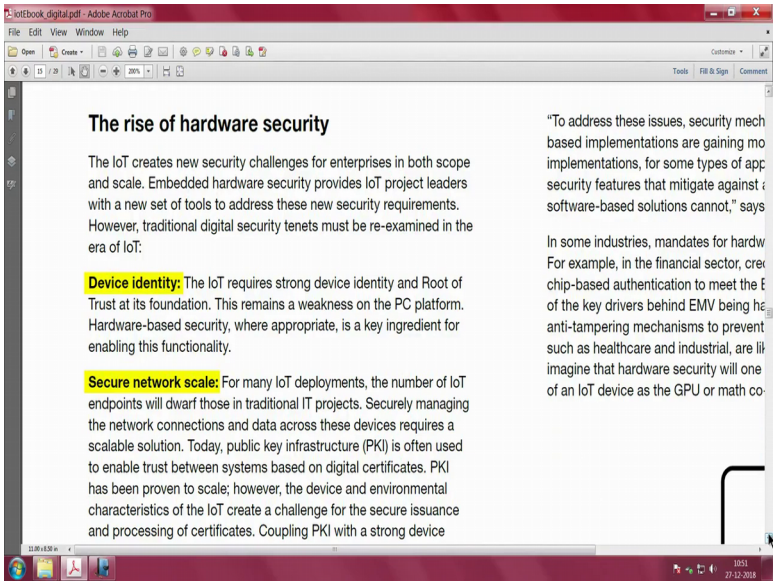
There is no way by which you can build an IoT application without security already built into the system. Therefore, the focus eerily is that code design part. What is it that you as a designer can actually do to ensure that this core design is included in our in your applications. So, this article is actually saying the same thing. Gartner's 2016 IoT backup backbone survey showed that 32 percent of it leaders cite security as the top barrier to IoT success.

(Refer Slide Time: 16:41)



What is the solution right? Here is something that look beyond traditional it security boundaries. Essentially saying that these are all there you have problems you have CPS solutions, you have you have attacks of different natures. What more can you do? How can you prevent this?

(Refer Slide Time: 17:03)



Here is the nice conclusion; to what Gartner also says. The rise of hardware security; this is where you should focus on. The IoT creates new security challenges for enterprises in both scope and scale. Embedded hardware security providers us provides a IoT project

leaders with a new set of tools to address these security requirements. However, traditional digital security tenets must be re-examined in the era of IoT look at this beautiful sentence devise identity.

IoT requires strong device identity and route of trust at it is foundation. This remains a weakness on the larger systems. Hardware base security where appropriate is a key ingredient for enabling this functionality. Secure networks scale for many IoT deployments the number of IoT endpoints will dwarf those in the traditional it projects.

Securely managing the network connections and data access to these devices requires a scalable solution. Today a PKI is often used to enable trust between systems based on digital certificates. PKI has been proven to scale; however, the device and environmental characteristics of the IoT create a challenge for the secure issuance and processing of certificates.

Coupling PKI with a strong coupling PKI with a strong device identity is a solution to this problem. So, you can think in a slightly different way PKI is known to scale; can I now bring in device identity the first part and somehow combine this device identity with secure the most scalable solution PKI.

And then see if I can bring out a unique way of addressing the problem of device level security so this is really the focus. So, what are the so this is about this article, forget this article. Now let us more where are the what shall I say where are the levers and hooks in a device that will allow you; where are the you know hooks and livers in an IoT device that you can really exploit to get to this device identity is the question.

If you take an embedded system just look at the different blocks you have the microcontroller right, then you have a port where sensors are connected, multiple sensors are connected. So, I would call this analog sensors these are all sensors which are analog; which means this must be an ADC port.

Typically an ADC port is built into the microcontroller that is why it is also called an SOC or system on chip which has several integrations. The SOC also has a radio component right. So, let me bring out the radio, but ill move this ADC I will write it here, show it here and show this radio here.

They can also be a UART right. And UART is also part of the SOC and the several GPIO ports, these are digital by nature. And these are where digital sensors can be used these are say for interfacing to other peripherals if any. Then there is memory block right there is a RAM and then there is a flash, flash memory and RAM. I will call them either I can put them as separate blocks or I can ill put them as separate blocks maybe that makes sense.

This is RAM and this is flash also part of the microcontroller. So, so you have and then there is the oscillator circuit. Oscillators can be also you can have crystal oscillators you can have RC oscillators. If it is an RC oscillator it is built into the chip itself directly. Then there is also another block which perhaps is appearing now quite commonly and that block indeed is the power supply block.

You have LDO and DC convertors and that is also now integrated into the system. So, you can see that it is rich in so many of these peripherals. Somehow you should be able to use these different elements to generate the device id. This is indeed a rich area it is an upcoming area and we will discuss some of the ideas that have appeared in the recent past; on how to generate a device Id device identification unique device identification.

So, that you will be able to identify replacement and counterfeit are any counterfeiting that happens to devices. But before that it is useful to know; what is the impact of counterfeiting like what is it is impact? Why is this important at all? So, let us look at another article, and try to understand it from that article the importance of the importance of you know replacement device identity and counterfeit.