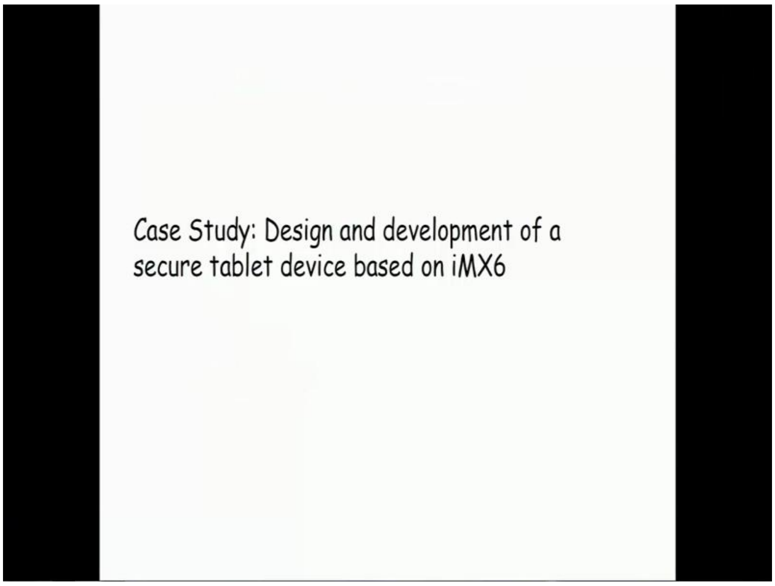
Information Security - II

Prof. V. Kamakoti
Department of Computer Science and Engineering
Indian Institute of Technology, Madras

Lecture - 39
Case Study: Design and development of a secure tablet device based on iMX6

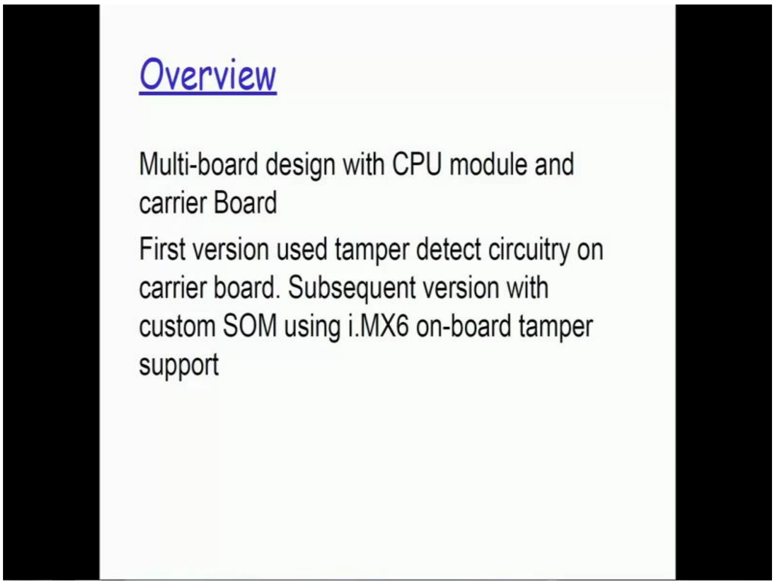
(Refer Slide Time: 00:09)



Case Study: Design and development of a secure tablet device based on iMX6

Right so just a very quick case study of what device we are actually built so with a i.MX6 processor.

(Refer Slide Time: 00:12)



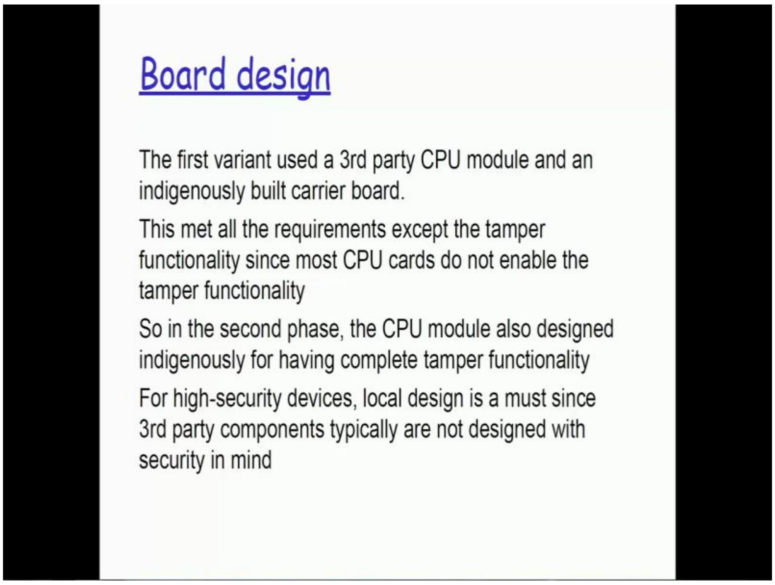
Overview

Multi-board design with CPU module and carrier Board

First version used tamper detect circuitry on carrier board. Subsequent version with custom SOM using i.MX6 on-board tamper support

Multi board design with the CPU module and a carrier board, we wanted to have it in this manner because we thought originally; we have a separate CPU module, we will be able to do a quick migration to the newer CPUs that might be coming in as compare to redesigning the complete hardware. We had a separate carrier board and then we had a plugin CPU module on that which could be swapped with later updated version will be coming in and all the peripherals will actually be on the carrier board. So, even if you have to update the CPUs to later versions, the peripherals will not be needing to be getting changed. So, the first version used a tamper detect circuitry on carrier board subsequent version we built up a custom SOM which actually had the i.MX6 processor tamper support itself available.

(Refer Slide Time: 01:08)



Board design

The first variant used a 3rd party CPU module and an indigenously built carrier board.

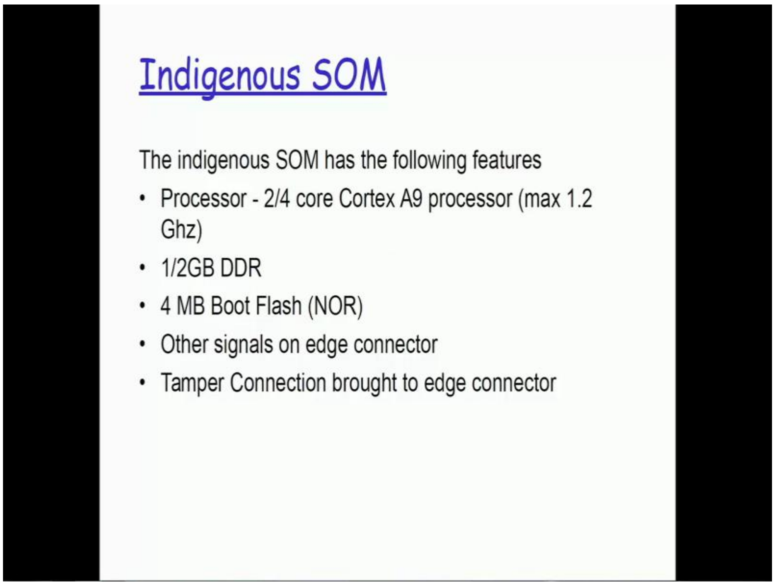
This met all the requirements except the tamper functionality since most CPU cards do not enable the tamper functionality

So in the second phase, the CPU module also designed indigenously for having complete tamper functionality

For high-security devices, local design is a must since 3rd party components typically are not designed with security in mind

So, that is basically the difference between the two versions.

(Refer Slide Time: 01:13)



Indigenous SOM

The indigenous SOM has the following features

- Processor - 2/4 core Cortex A9 processor (max 1.2 Ghz)
- 1/2GB DDR
- 4 MB Boot Flash (NOR)
- Other signals on edge connector
- Tamper Connection brought to edge connector

The indigenous SOM that we had actually developed internally had a 2 or 4 core processor, so we had two different variance in fact four different variance, a 2 core or 4 core processor and some of them having a 1 GB or 2 GB RAM, 4 MB boot flash it was a NOR flash which we actually used for dumping our image and then

Student: Excuse me sir.

Pardon, yes.

Student: SOM stands for

Yes.

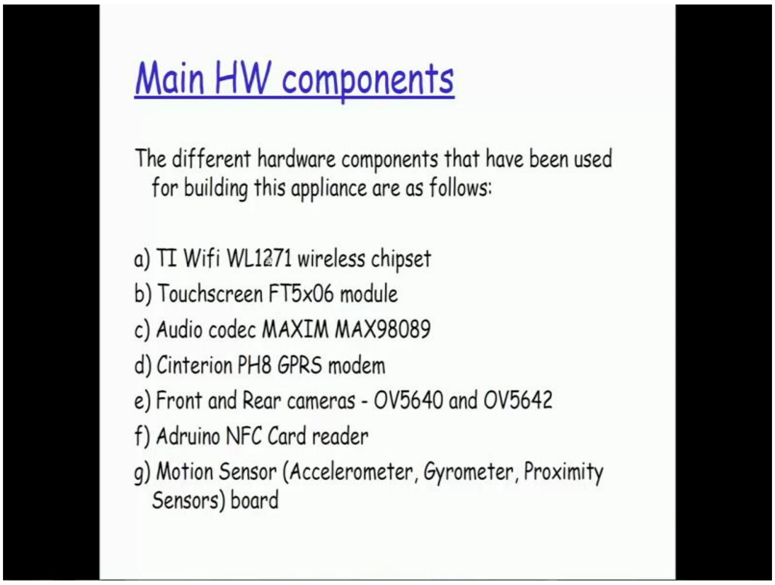
Student: SOM Sir.

SOM actually stands for System On Module.

Student: Okay Sir.

So, I will just show you, I have some pictures also of it. I will just show you that aspect of it.

(Refer Slide Time: 02:04)



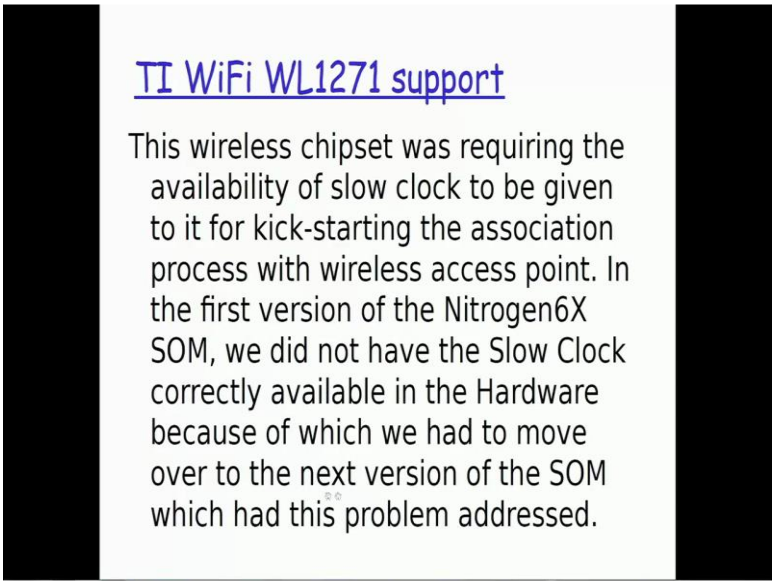
Main HW components

The different hardware components that have been used for building this appliance are as follows:

a) TI Wifi WL1271 wireless chipset
b) Touchscreen FT5x06 module
c) Audio codec MAXIM MAX98089
d) Cinterion PH8 GPRS modem
e) Front and Rear cameras - OV5640 and OV5642
f) Adruino NFC Card reader
g) Motion Sensor (Accelerometer, Gyrometer, Proximity Sensors) board

The different hardware components we had a wireless chipset, we had a touch screen, we had a audio codec for receiving and making calls, we had a GPRS module from cinterion, we had both front and rear cameras from omniview, we have a Adruino NFC card reader. So, this NFC card reader was actually used, to authenticate the person right. If the person was not using a valid NFC card for a certain number of tries. It was actually simulated it to be as a tamper event and the device was completely reset. So, we actually had used this NFC card reader for the authentication purpose, failing which after a certain number of tries, it would basically do a complete reset of the device and then we also had the complete motion sensors on the board accelerometer, gyrometer, proximity sensors all available on this board.

(Refer Slide Time: 03:04)

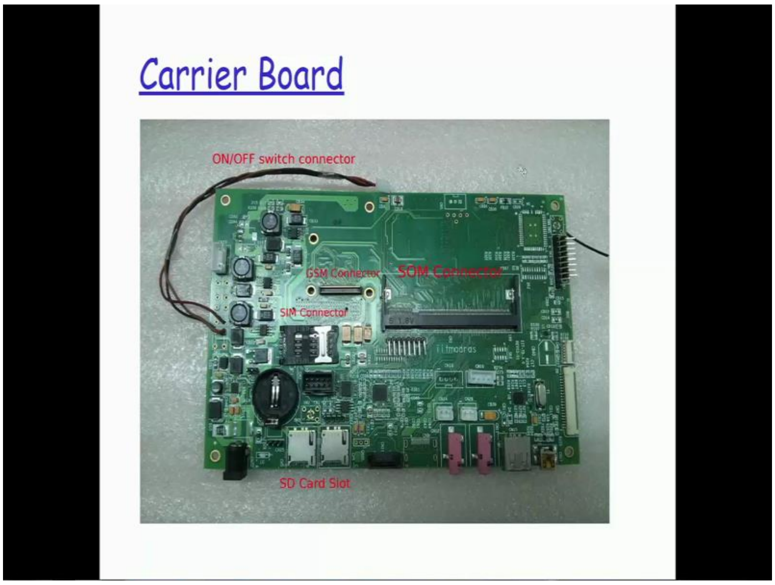


TI WiFi WL1271 support

This wireless chipset was requiring the availability of slow clock to be given to it for kick-starting the association process with wireless access point. In the first version of the Nitrogen6X SOM, we did not have the Slow Clock correctly available in the Hardware because of which we had to move over to the next version of the SOM which had this problem addressed.

I have actually documented here the different kinds of problems that we actually faced in integrating all these components, the kind of challenges that are there. So, for want of time right now, I will just do a quick pass through of this. Any way since you going to be having the presentation you can take a look at that separately. So, all the components that we are integrated in what kind of challenges we faced, I just given the documentation here, so that it becomes a record for us to not to make use the same things again.

(Refer Slide Time: 03:33)



Carrier Board

This is our entire carrier board so this is basically what I was telling, if you see here we have a SOM connector, on which our SOM piece will be connected and the SOM will have the processor inside that. All our peripherals, whether it be my SD card, USB, cameras, Wi-Fi, Ethernet, whatever I wanted to have as a peripheral, I will have only on this carrier board. So, tomorrow if I have to upgrade my processor to a later one, I do not need to spend my time in designing the carrier board again. The carrier board will continue to be as it is, I will just check out my existing SOM, build a new SOM only with processor and then plug it in, that was basically the reasoning behind this part.

(Refer Slide Time: 04:20)

SOM Module

SOM Module Rear View

SOM Module Front View

This is how the SOM looks like, so this is my the rare view of the SOM, this is my front view, this is my processor. So, all the components that we saw here are all inside this processor.

(Refer Slide Time: 04:40)

MIC/Sensor Board

MIC and Sensor Top View

Our MIC and sensor board, this was a digital MIC that we actually use for our codec. For the calls that we are making we actually had a digital MIC instead of an analog MIC. This is the sensor board that was actually connected on to our carrier board so this had all the sensors, the proximity, the accelerometer, the gyrometer, the front and the rare cameras that we are actually used from omniview. So, these components are actually again integrated into the board.

(Refer Slide Time: 05:06)

Feul Gauge

This was the fuel gauge, so the battery indicator right. So, was basically this component that helped us to tell, how much percentage of battery is right now available. This is basically what you see on your mobile phones also, the indicators so this the small piece that is actually used for that.

(Refer Slide Time: 05:25)

NFC

NFC Tag Reader

This is the NFC card reader, the Adruina NFC card reader that we had, then the LCD display.

(Refer Slide Time: 05:28)

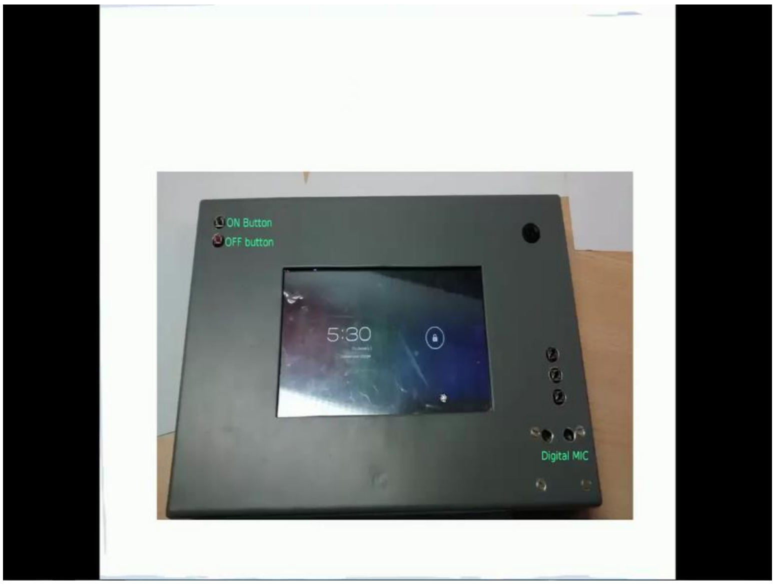
LCD Display

LCD Top view

.

So, this is the touch screen LCD display.

(Refer Slide Time: 05:32)

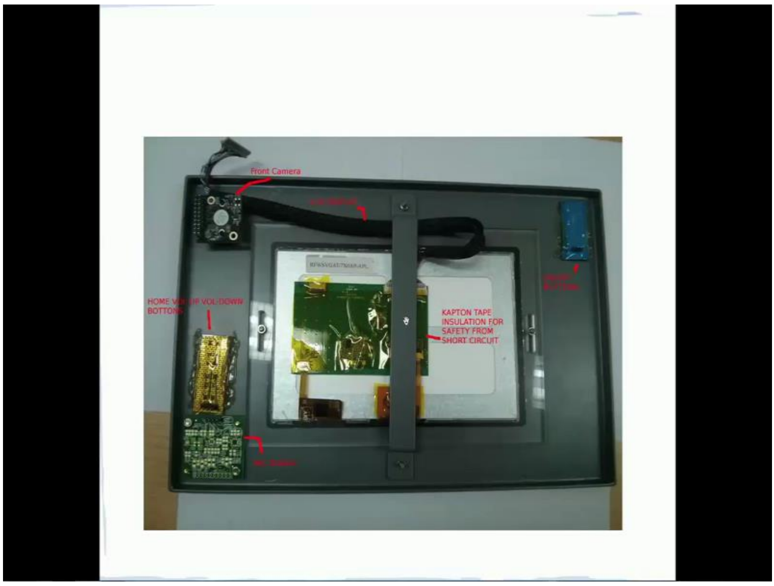


So, this was our final device that we had.

(Refer Slide Time: 05:35)

In which we were actually having this upgraded android image running with support for all these devices added into it so actually had titled it as ANURAKSHA device.

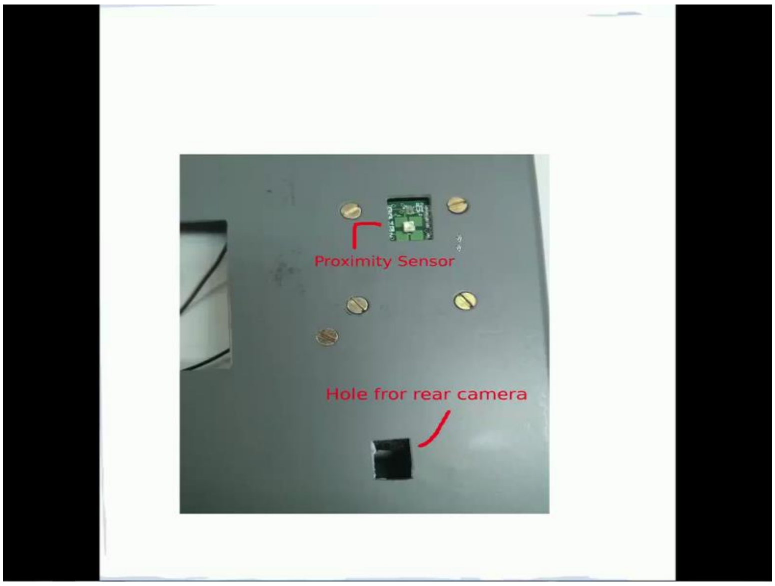
(Refer Slide Time: 05:50)



.

This is again the back side of the display where the proximity sensor and the rare camera is going to be looked at from the enclosure point of view.

(Refer Slide Time: 05:55)



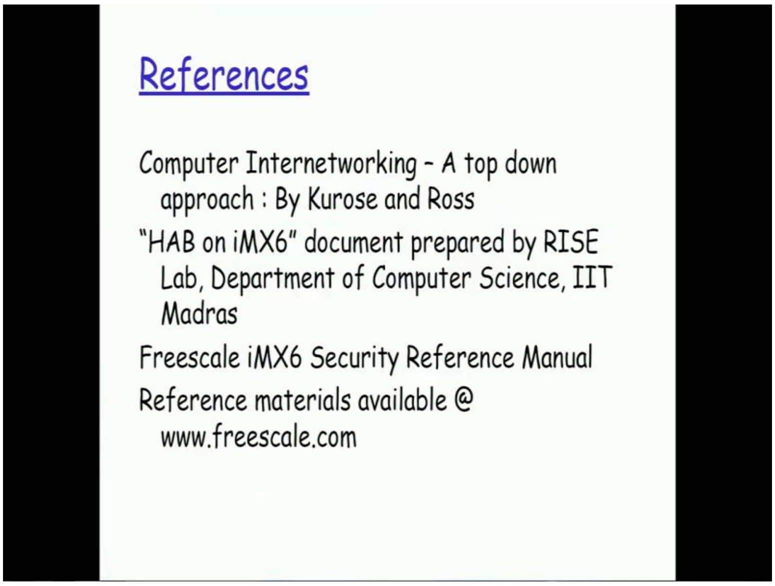
(Refer Slide Time: 06:00)

Insertion of SD card into SD card slot

.

Wherever SD card slot is available and inserted, so these are the components that are there.

(Refer Slide Time: 06:12)



References

Computer Internetworking - A top down approach : By Kurose and Ross

"HAB on iMX6" document prepared by RISE Lab, Department of Computer Science, IIT Madras

Freescale iMX6 Security Reference Manual

Reference materials available @ www.freescale.com

All the references that I actually taken for this presentation, the basic introduction I had taken from this book. As far as high assurance boot is concerned, we are actually prepared a complete document for this as part of the rise lab in computer science department. We were actually the first group in India, to understand high assurance boot and implement it on i.MX6 processor. So, it was actually this document was prepared and given back to free scale and free scale is internally circulating it all their new customers as of today.

That document was actually prepared and there were inputs from that just been taken also, I mean in fact it has been done by the team here. Then I had referred the i.MX6 security reference manual, which is again publicly available. So, if you are keenly interested to understand in more detail about each of these components at that, this particular processor is providing as far as security concerned, all those details are very elaborately discussed in the security reference manual and there are other training material also there is available on i.MX6 processor in free scale dot com.

Thank you very much it was nice talking to all of you.

Hope you found it useful. This is only a dessert course that we have actually started, it is a appetizer right. Now I should not use the world dessert, just an appetizer in such a short time I have tried to cover. So, I would very strongly recommend that you actually poke more details out of these references that I have given and then try to learn more.

Thank you very much, all the best.