JULIE McCROSSIN: Ladies and gentlemen, if you could get your numbers. I'm calling them in just a moment. We are just in warm-up time as the last people come in. Can explain the RFID? Remember the Minister made reference to a probe inside a person? One of you must know about RFIDs? You do, don't you? I remember you from last time. Come out the front quickly. Just while the last few people come in, then we'll pull the lucky door prize. Do you want to introduce yourself?

>> Holly, I don't know everything. I don't know what it stands for. But it is a chip you put in little things - in a department store or whatever and people are worried about the fact you are going to take something out, a little chip will set off an alarm saying, "You haven't paid for me".

JULIE McCROSSIN: That's true, I don't think they are putting it inside people inside DJs yet. Can you introduce yesterday?

>> Keith, I was going to say it stands for radio frequency identifier.

JULIE McCROSSIN: Perhaps you can help me, Sir, there are companies already chipping their humans in the manner we chip our dogs and the people are consenting to this?

>> Yep.

JULIE McCROSSIN: What's the purpose?

>> Makes it easier coming into a building without having a pass is the main purpose. There's more sinister purposes but that's the utilitarian one.

JULIE McCROSSIN: Thank you. Hand up if you knew that? Most of you. It's an educated crowd. Ladies and gentlemen, have your numbers ready. If the person is not here, it is redraw. Our first prize, Peabody, if you could run the prize to the winner, give a round of applause to Peabody please.

(APPLAUSE)

>> That was limp. This is a young woman working! The winner is F2. Hello. Excellent. Congratulations! If you want to squeal with delight and break down, that'd be great.

(LAUGHS)

Ladies and gentlemen, thank you for coming in and welcome to our second session. We are going to talk about hacking your house and it is my enormous pleasure to welcome Professor Vijay Sivaraman from University of NSW. His current interests include cyber security and Internet of things. He is leer to talk about research funded by an ACCAN Grants Scheme.

(APPLAUSE)

VIJAY SIVARAMAN: Thank you for the introduction. It is a pleasure to be here to be talking about the work that was funded by ACCAN. I'm Vijay. This is work with a couple of colleagues. I would like to start by thanking ACCAN most profusely for supporting this week and Narelle and Tanya who have spent a lot of time with us to make sure what we are doing is understandable by people who don't necessarily spend every day working with such technologies so thank you again very much for that.

We have already had a good segue into the stock by both the Telstra speaker John and by Amanda earlier. I don't need to retread the importance of IOT and explosion of expedience in the next few years but I want to focus on the darker side of IoT and the security threat. We have seen baby monitors were hacked and used to shout obscenities at a kid. We have seen logistics firms hacked, vehicles taken over, smart cities disrupted, transport systems. Household IoT devices were used to compromise web sites and bring down many services in the US including Twitter. Barbie Dolls have been hacked, power grids have been taken down. Earlier this year a large number of computers were compromised by a person called Stack overflowing. This year, a university campus was brought down by its own vending machines. We have seen this in the news but the project is about how real is it if we want to do it ourselves? Is it easy, difficult, what kind of devices are vulnerable to these kind of security threats? The object was to try it ourselves in our lab with a bunch of students. They are not ordinary students, students who are very smart. Information. The objective is to see how real and widespread the threats are, how typical they are. We did it in a rigorous manner. We identified various pillars of security, divided them into how safe is the confidential data going across, can anybody spoof the data, can somebody take over your device and do nasty things and can somebody use your device to attack others so make it looks like the attack comes from you. We classified various attacks into four different aspects to come up with the estimated posture of security and privacy of the devices we work with. We evaluated a fairly good number of devices. 20-25. We are still doing it actively. Devices ranged, typical household devices where you expect lots of security cameras, printers, smoke alarms, medical devices, light bulbs, photo frames and so on. In order to give it a narrative so that it doesn't become like a dry laundry list of going through a long list of devices, we created four personas. The same way as we heard John Chambers from Telstra talk about the various cases around safety security and energy management and so on, our first persona was a person who is worried about safety and security in their house so you'd expect them to have video cameras and motion detectors and smoke alarms and the lights. Sure enough, we did find some rather serious problems. A motivated attacker could actually get in and get a feed of the video from that device. They could see if you were home or not by looking into the data that was being sent by the motion sensors. Not every device but many of the devices in there were fairly insecure as an attacker could easily snoop into the data, thereby compromising the privacy.

There is obviously a lot of technical detail here which I am glossing over! We have posters that are outside. Four of them explain these personas in more detail and two of our brilliant students can tell you the details of how they hacked them. It is in the report. The second persona was around an elderly couple that has blood pressure monitors, air quality monitors and the like. We found the medical devices to be more secure. Though the skill was sending information in plain text but that was fixed by the manufacture this year. This kind of house was a good launching pad for attacking other services on the internet. In that sense, even though the couple by themselves may not be under attack, they could be implicated as attackers on other services.

Our third persona was around energy management. A family which wants to make sure the lights are not left on and the air-conditioners and so on. They have a range of light bulbs and energy management devices, power switches and the like. We found many of these devices to be very insecure. Not just is the privacy compromised in terms of being able to see what's happening but, also, these devices could be controlled by an attacker. So that's fairly serious.

Our last persona was around a hip, young couple that has a bunch of entertainment devices, they like their Smart TVs and smart printers and the like. In this case, we could show we could actually print documents on to your printer. That could scare you. They could extract scans of what you printed in the past. On your Smart TV, which was using Google chrome cast, the attacker could not just see the videos you were watching but could post a video on to your Google chrome cast which can be frightening if you are at home watching things on your TV. Technical details, the report is fairly high level and the posters are explaining the outcomes but we have followed a very vigorous process in our testing and it has been published in three conferences run. Those of you who are a bit more technologically savvy, "I'm inside my house, I'm protected by the home routers", we have bad news for you. We put an app on smartphone on the Apple app store which looks like a survey app but internally it is inside your house, past the fire work, snooping and finding the devices in your house, able to report it to an external entity, disable the firewall so an attacker can gain access inside your house. Even though the firewall does give you some protection, don't be too complacent because there are ways to break into your house and get inside through smartphone apps with malware but also websites and the like.

We also quantified the levels of attack that can take place using your house as a reflector. An attacker could reflect the attack off your house so it looks like it is coming from your house and also amplify it. Sometimes the amplification factors are going up in the 20s which means, for every bite of attacker they send you, you are sending 20 biter attacks on the internet. You are helping them amplify the attacks. This was a paper presented in the US last month. We have another paper that's very recently been accepted, going to be presented in November, giving a more systematic methodology to evaluate the security of IoT devices.

As I mentioned, the report is a good read, hopefully, gives a narrative to it but in terms of the technical details, we have a whole bunch of papers for those who are interested, they can go and read them. The really difficult question going forward is that - okay, so we have established that security with IoT is a big issue. Many devices on the market are fairly insecure. The next question is, however, the tough one. What do we do about it? That is really an open question which I'm hoping will be discussed at forums like this maybe in the next panel session included. There are many stakeholders in this. Consumers, obviously, need to be protected. They need to be informed. Maybe there is a role for some kind of security or trust star rating system. That might be worth discussing. Manufacturers, obviously, have a big role in this. What are their obligations when they put a product on the market? Should there be regulation which ensures at least a minimum standard of safety and security? How is the regulation going to keep up with the rate at which the market is moving in IoT? Lastly, how about insurers? ? Is insurance another instrument to use in ensuring devices put into homes are actually safe? If it is not secure, will your insurance company trust a house that is using an IoT-based door lock that is not secure? Many stakeholders in this - I think that's the part that's going to be the tough one going forward, figuring out how to tackle the problem. The objective was to show the problem is real. It is not just in the news. You could be in the news in the sense the devices you use in the house could be both the target and the source of attacks. But the next step forward is something we look forward to seeing how it evolves and it will require engagement across the community. Thank you.

(APPLAUSE)

JULIE McCROSSIN: Was that interesting or what? Can you give him another clap? Professor Vijay, if I may call you that, is going to join us on the panel. Could I invite Greg Killeen to come up and also Professor Katina Michael? While the panel position themselves, I just wanted Narelle to come out. I have to be honest with you, I have spent a bit of time at conferences in child protection and domestic violence and that unmitigated enthusiasm for control slightly spooked me. I was also one of five children in the 50s and we ran amok with a level of joyous freedom in Sydney, cutting ourselves to shreds on oyster beds, drowning and falling off cliffs around the Georges River everywhere that was pleasurable. I was heartened by a brief anecdote by Narelle. You are a rather tall person, there is a comic visual in this protection.

>> I'm Narelle Clark, I run the Grants Scheme and had a wonderful time with Vijay with a bunch of devices!

>>

JULIE McCROSSIN: We will let that go to the keeper!

(LAUGHTER)

>> You tried the home work process, didn't you? She is bit of a nerd, got a capacity with devices as we have already heard. What did you try with your children and how did that evade you?

NARELLE CLARK: My eldest daughter was doing her HSC, she was on Facebook, I set up the firewall to allow access to Facebook a couple of hours. If they tried to access Facebook, they got a message that said, "Darling, you should be doing your homework". I found another child on the veranda with their laps. What's going on here? The neighbour's wi-fi is not secured. What do I do? Obviously it is probably using default user name and password, do I log in and fix it? Or do I leave a note in the letter box saying, "You need to secure your wi-fi". What do you do?

JULIE McCROSSIN: This is the danger of giving women education. Mothers are fiendishly clever at controlling their children. Please give Narelle a round of applause.

(APPLAUSE)