Published on *Up Close* (http://www.upclose.unimelb.edu.au)

Episode 39: Detecting and Avoiding Online Threats

Detecting and Avoiding Online Threats

VOICEOVER
Welcome to Melbourne University Up Close, a fortnightly podcast of research, with personalities and cultural offerings of the University of Melbourne, Australia. Up Close is available on the web at upclose.unimelb.edu.au, that?s upclose.u-n-i-m-e-l-b.edu.au

SHANE HUNTINGTON
Hello and welcome to Up Close, coming to you from Melbourne University, Australia. I?m Dr. Shane Huntington and today?s topic is cyber security. As we enter the twenty-first century the use and application of computers and their level of connectivity continues to affect the majority of the world?s developed countries along with a large portion of the third world. The network age has brought us amazing access to information and resources, but the cost of these newfound resources is the threat of cyber crime and the subsequent need to advance cyber security systems.

Today on Up Close we are joined by an expert on cyber security, Associate Professor Chris Leckie from the Department of Computer Science and Software Engineering here at the University of Melbourne, Australia. Welcome to Up Close, Chris.

CHRIS LECKIE
Hi Shane.

SHANE HUNTINGTON
I had a conversation the other day which surprised me with an elevator repairman who said that the elevator he was working on was networked. This stunned me. We, are we that connected now?

CHRIS LECKIE
People these days, they think of the internet as the world wide web or using their email or maybe a social networking site, but increasingly it?s become part of the way we gather information about how critical systems are working. So for example,

monitoring the water supply or controlling the electricity grid. These increasingly involve the use of the internet and the protocols of that are used there: electronic commerce in business all depends on the internet. And that?s in many ways the bottom part of the iceberg that we don?t normally see imbedded in our everyday lives.

SHANE HUNTINGTON
In terms of security, why don?t we just for a moment look ten, twenty years ago ?cause I think that?s a good place to start. What was security on the internet like back then?

CHRIS LECKIE
Well, you?ve got to remember that back twenty years ago, the internet was a much more civilised place. It was largely being used by academics like myself, people in government research laboratories, and it was a very small community of users. And the range of services that people were using were fairly narrow - email and logging into computers, that sort of thing. So there wasn?t that much to be gained by hacking into a computer. And if someone did, generally you knew where they were coming from and you?d give them the rap over the knuckles or give them the boot if they did something wrong.

SHANE HUNTINGTON
Mm. And in contrast, today, where computers are reaching into every aspect of our lives, we have a very different security situation. Tell us a bit about that.

CHRIS LECKIE
In the current environment there?s been such a rapid growth in the take up of computers in countries all over the world, in particular each with their own legal system and their own way of managing networks, it?s become much harder to keep track of how networks are being set up, how users are being authenticated, and how well the computers on those networks are being upgraded with the latest patches to fix any security holes, or ways of checking for viruses. So as the computers that are available have been put in the hands of people who are less skilled managing their computers, so your average mum or dad isn?t an expert in cryptography. They just pull the computer out of the box, switch on the wireless modem and away they go, not really understanding all the potential security threats that could occur if they don?t activate the appropriate measures.

SHANE HUNTINGTON
Mm. Let?s talk about the individual just for a moment. How affected are we as individual consumers and I guess people with private health care records and so forth, as a result of cyber crime?

CHRIS LECKIE
I think where people have the most concern is probably in things like internet banking or financial transactions, electronic commerce over the web. And people worry about, ?Should I put my credit card number into a website?. Can I trust where it?s

going?? And I remember speaking a number of years ago to a European expert who worked in one of the major banks in Europe, and he said the sorts of crime that was occurring were often very small transactions that were too small for the banks to really pick up. Or they pick it up but, you know, why would a bank spend a thousand dollars chasing a forty dollar fraudulent transaction? But from the banks point of view if you add that up over a large number of customers and a large number of transactions, it?s a lot of money. But it became in some ways a cost of doing business on the internet. And they could pass it back on to consumers, I guess.

SHANE HUNTINGTON
Now you mentioned before that back ten, twenty years ago it was easy to I guess nail down who was doing something and their location. I suspect that was a result of knowing their IP address and having a physical association with that IP address. What has changed that has made this so much more difficult now to find these people?

CHRIS LECKIE
Well it comes back to the way the internet was designed. The philosophy behind the design of the internet, that it was meant to be a network that was open with ease of access so anybody could reach anybody. It was meant to be scalable so that it could grow. I mean it?s grown by orders of magnitude in terms of the number of hosts that are connected, and without any central control, so no single authority that?s responsible. So that means that the penalty for all of that is that in terms of ease of access, anybody can come knocking on your door. So anybody can reach your computer. In terms of scalability, it doesn?t keep information about where traffic was coming from, so where the packets, the messages that are used for transferring data, it doesn?t keep track of where they were coming from. That meant it was very scalable, but if something goes wrong, someone comes knocking on your door, there?s no easy way of telling ? do they really come from the address where they claim to have come from? And in terms of lack of central control, then if something does go wrong, who are you going call?

SHANE HUNTINGTON
Mmm. I?ve heard this phrasing where people talk of things ?being part of the cloud?. Explain that too me, what is meant by this?

CHRIS LECKIE
So the cloud refers to the idea, when we send a message on the internet it?s broken up into smaller messages called packets. And each packet specifies the destination address where the packet should be headed. And there are devices in the internet called rooters, or routers depending which side of the Pacific you come from. And their job is to look at that destination address and decide which output link, transmission link should they send the packets on. The router might not know ... might trace different packets to the same destination independently. So routes through the internet can change. And so from that point of view it?s not like the telephone network with a well-defined connection established. In the internet, the packets go into this, what seems like a rather amorphous network of routers, which

where they go, how they get there, whether they get lost along the way and have to be retransmitted, is in some ways opaque to us.

SHANE HUNTINGTON
Mm. When it comes to security, one of the things I find difficult to conceptualise is the idea that my home computer can be somehow safe. And let me explain why. There are, as you know, cyber attacks on the large banks, on very large organizations that have incredible levels of resourcing to protect against them. How is it that we can make our home computers safe with such minor resourcing relative to these sorts of organizations, when I?m assuming it?s similar people doing the attacks in both cases?

CHRIS LECKIE
Well the interesting part of that, those massive attacks, we tend to call them denial of service attacks, where an attacker is trying to flood a network such as a bank website or a major search engine or maybe the White House website, trying to flood that server with massive amounts of traffic. But that traffic?s got to come from somewhere. And often those servers, they have big network connections, very high capacity network connections. So they need a lot of traffic sources. And where they get the traffic sources from is from your computer. Well maybe not your individual computer, but by trying to gain control of a large number of computers that might be connected on a high bandwidth like a cable modem connection. And they can then become very efficient sources of large amounts of traffic. In fact often I?ve heard it said that the most secure computers on the internet are the ones that have been taken over by would-be attackers. Because once they take over a computer, they don?t want to lose that. They want to hang on to that, so they make sure they close up any other security holes that happen to be on that computer.

SHANE HUNTINGTON
That?s certainly a shame that we would need that as the ultimate security measure.

You?re listening to Melbourne University Up Close. I?m Dr. Shane Huntington and we?re speaking with Associate Professor Chris Leckie about cyber security.

Chris, let?s move on to your particular area of work because your interest, as you stated, was in the artificial intelligence and application of that to cyber security. How do we go about that? What?s involved?

CHRIS LECKIE
So, let?s take that example of a denial of service attack. If you?re running a website and one day you suddenly see a flood of traffic that?s stopping other people, normal legitimate users from using your website, What you need to do is to filter out the good packets from the bad. One approach just would be to throw packets away at random. But that penalises the legitimate users as much as the malicious users. One of the things we try and do in our research here at Melbourne University, is to use techniques from what?s called the data mining community, or pattern recognition or machine learning communities, to try and learn the signature or some identifying

features that help us discriminate the good guys from the bad guys, the good traffic from the bad traffic. And in many cases what we do is combine that with a deep understanding of how do the two, how do the communication protocols work? So for a particular type of attack, is there some invariant property that characterises the traffic, that is an essential part of the attack that we can use the basis for discriminating the good from the bad traffic.

SHANE HUNTINGTON
I assume that this has to be, with the idea I guess of artificial intelligence, has to be evolving ? cause I can imagine a scenario where my, the hackers become aware of this version of things, and they start to mimic the type of traffic that you?re allowing through. How does the AI approach deal with that?

CHRIS LECKIE
That?s one of the challenges - not only the attackers changing but normal usage changes as well. So what we try and do is an approach called anomaly detection, where rather than trying to characterise what attack traffic looks like because the attackers are always trying to change the way their attacks are conducted. In the anomaly detection approach we?re trying to characterise normal behaviour and then throw away anything that?s too far from normal. Or at least treat it differently. So, we use techniques known as clustering techniques which try and group together similar types of traffic, and say we?ll treat that? that traffic?s seems to have behaved normally on the website, we?ll treat that as normal traffic. And then the traffic that doesn?t fit our profile of normality, then we might put that through a stronger authentication process. Or we might put it into what?s known as a computational puzzle. Something that slows down the response of that source so that they can?t be generating any new accesses until they?ve gone through some sort of computationally difficult task.

SHANE HUNTINGTON
Would it be fair to say then the goal is more about detection than prevention? Is that the focus on knowing the attacks are occurring rather than trying to stop something that inevitably will happen?

CHRIS LECKIE
Ultimately prevention would be ideal, and I guess the area that I?ve been working in, because of my expertise in network traffic analysis, has been more on the detection side. But if we really want to get serious about stopping these types of attacks then ultimately we need to try and make the sources of the attacks, the home computers, much more secure. With these types of attacks, the human in the loop becomes the weakness and they become the subject of what?s called a social engineering attack. When someone sends you a web ?an email that you think might be from your bank, or in this case, someone sends me an email and they claim to be from Melbourne University, I click on the website and that downloads some code that manages to infect my computer. Or they convince me to giving away my user name and password. Usually I?m pretty suspicious of those sorts of things, but there?s plenty

of users who are new to the internet and humans being what humans are like, they tend to be fallible.

SHANE HUNTINGTON
Mmm. It?s amazing to me that the primary mechanism by which these attacks occur is to use peoples? home computers, which is, which is quite phenomenal. With regards to the types of attacks that are going on, are they generally for financial gain? Are they just to bring down infrastructure? Where are the attacks occurring across the world?

CHRIS LECKIE
So the early types of attacks, if we go back to an historical perspective, in many ways were driven by curiosity and fame. Some curious technical person trying to see, ?Hey wouldn?t it be cool if I could get into this particular site?? Or trying to gain some sort of notoriety. Then increasingly as the attacks became more sophisticated, people realised there was money it. And so, for example with denial of service attacks, what?s really driven a lot of these attacks has been the ability to make money through blackmail. Think. If you?re an online betting agency, you might make most of your money within the last ten minutes before a big horse race. Like in Australia we have The Melbourne Cup, where most of the money goes onto the horses in the last few minutes. That creates a very critical window during which people can be attacked. So they might launch an attack a week or two weeks in advance, demonstrate what they?re able to do, and then say ?Well either you pay up or we?ll launch it at a more critical time.? So that?s become a major motivation, the trying to gain revenue through blackmail. The other thing that?s starting to appear increasingly now is attacks as a form of political demonstration. There was a case in 2007 in Estonia where a statue was being removed, a Soviet era, memorial I think to the Second World War. This caused a lot of upset amongst the local Russian community within Estonia. Now there were riots and protests and, bear in mind, someone was actually killed in one of those riots. But the other aspect of it was, there was a large number of denial of service attacks on businesses and government institutions within Estonia which caused enormous disruption and this has become a new example.

SHANE HUNTINGTON
Chris, let?s turn our attention now just to the future because computers are changing at such an alarming rate and networks as we perceive them are changing at an incredible rate as well and there are so many things happening that weren?t happening ten years ago, such as file sharing and so forth. Can I assume that the types of threats we?ll be facing will be changing into the future in ways we just haven?t imagined?

CHRIS LECKIE
Oh I can guarantee that. What I would expect to see as a trend in the future is new targets for attacks. For example, we have increasingly sophisticated mobile phones that have internet capabilities and blue tooth connections. There are already starting to be reports of different types of malicious codes - attacks that can be downloaded

onto mobile phones inadvertently. Another area is again to do with telephony, in the area of what we call ?Voice over IP?, where we make telephone calls over the internet and people might have some experience of that either through their work or through services such as Skype. And previously, the telephone network has been reasonably immune to attack. Now as people are making telephone calls effectively through a computer and those calls are connecting via gateways into the traditional telephone network, this I think has the risk of being a way of spilling over some of the traditional attacks into the telephone network. Think, for example, of email spam where you come in the morning and there?s two hundred emails trying to sell you something that you really don?t want. Imagine now that rather than having two hundred emails that you can delete, you have got two hundred voice messages sitting in your voice mailbox. Or you?ve got your telephone ringing every five minutes. Or from a security point of view, if all those calls were directed to the emergency service number, this I think is one of the new generation of threats that we?re going to have to deal with.

SHANE HUNTINGTON
Associate Professor Chris Leckie from the Department of Computer Science and Software Engineering here at the University of Melbourne, thank you very much for being our guest today on Up Close. And I would rapidly return you to your laboratory to deal with this particularly invasive problem.

CHRIS LECKIE
Thanks very much Shane.

SHANE HUNTINGTON
Relevant links, a full transcript and more info on this episode can be found on our website at upclose.unimelb.edu.au.

We also invite you to leave your comments or feedback on this or any episode of Up Close. Simply click on the Add New Comment Link at the bottom of the episode page.

Melbourne University Up Close is brought to you by the Marketing and Communications Division in association with Asia Institute of the University of Melbourne Australia.

Our producers for this episode were Kelvin Param and Eric van Bemmel. Audio recording by Craig McArthur. Theme music performed by Sergio Ercole.

Melbourne University Up Close is created by Eric van Bemmel and Kelvin Param.
I?m Dr. Shane Huntington, thank you for listening. Goodbye.

VOICEOVER
You?ve been listening to Melbourne University Up Close, a fortnightly pod cast of research, personalities and cultural offerings of the University of Melbourne, Australia.

Up Close is available on the web at upclose.unimelb.edu.au
That?s upclose.u-n-i-m-e-l-b.edu.au

© The University of Melbourne, 2008. All Rights Reserved.
