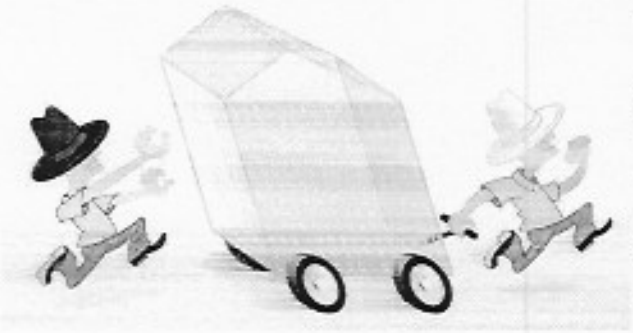
PHYS.ORG

Researchers keep networks moving to stay safe from hacker attacks

17 May 2016, by Michele Mcdonald



GMU researchers keep critical tasks on the run, one step ahead of hackers. Credit: Marcia Staimer/George Mason University

Imagine burglars have targeted your home, but before they break in, you've already moved and are safe from harm.

Now apply that premise to protecting a computer network from attack. Hackers try to bring down a network, but critical tasks are a step ahead of them, thanks to complex algorithms. The dreaded "network down" or denial of service message never flashes on your screen.

That's the basic idea behind new research by George Mason University researchers, who recently landed some $4 million in grants from the Defense Advanced Research Projects Agency (DARPA). George Mason's researchers are leading an effort that includes Columbia University, Penn State University and BAE Systems.

"Our research is vital as a real-world solution to these attacks, which are one of the most critical cybersecurity threats today, crippling online businesses with downed websites, financial losses and damaged client relationships," said Angelos Stavrou, who leads the research team and teaches in Mason's Management of Secure Information Systems Program.

Mason is positioning itself at the forefront of cybersecurity research.

"It definitely gives us a leg up because we're looking at the next generation of defense," saidDaniel Fleck, who's part of Mason's Center for Assurance Research and Engineering.

Widespread problem

Cyber criminals take down a website by overwhelming it with traffic. The most common approach is to flood a server with requests because servers can only handle so much traffic before shutting down.

Denial-of-service attacks hit record highs last year, up nearly 150 percent, according to cybersecurity firm Akamai. These attacks last between 6 and 24 hours and cost $500,000 or more, another survey notes.

Responding to this threat is akin to an arms race, Fleck said. Companies and governments put scores of servers into play to fight off the attacks. Seconds count for mission-critical systems, especially for the military. Hackers step up their efforts to counter the numerous servers.

"It's an arms race no one wants to be in," he said.

Researchers feel your pain

Fleck knows what it feels like to be on the receiving end of a denial-of-service attack."It happened to me a couple of days ago," Fleck said. "It's very frustrating. I need to get something done and I can't. As a security person, I'm always wondering if it's a security problem."

What's next

Mason researchers are working on the next step in fending off computer hackers. It's a method called "shuffling" in which hackers and regular users are quickly separated through a series of splits that eventually isolate the bad actors.

Solving one problem means another will spring up, making the field an exciting one.

"In security, you actually have an adversary," Fleck said. "You wonder what they're going to do when you solve the problem."

Provided by George Mason University

APA citation: Researchers keep networks moving to stay safe from hacker attacks (2016, May 17) retrieved 19 May 2016 from http://phys.org/news/2016-05-networks-safe-hacker.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.

PHYS.ORG

How to stop your phone from being hacked

25 May 2016, by Ali Dehghantanha, The Conversation



Credit: Horoscope/shutterstock

If you've ever forgotten your phone or left it at home for the day, you will have realised just how much you use it. On average, we check our mobile phones about 110 times a day. Using them for just about everything, from summoning an Uber car and paying for our latest Amazon purchases, to receiving prescriptions and even tracking shares and trading on the stock market.

Unsecured mobile phones are among the top seven major causes of security breaches and your mobile number is all a hacker needs to start the attack. Using your number, hackers can send you a text message containing a malicious link, which when clicked allows them to read your texts, listen to your calls and even track your whereabouts.

Smartphones are valuable targets for hackers – more so than laptops or personal computers. This is because they can be used as a "pivot point" to attack heavily protected environments such as banks or critical national infrastructure. Hackers can redirect their malicious traffic through your phone and store collected data on it. This means that all forensics traces would point to you as the hacker rather than the real culprit.

On top of this, most phones are open to attack 24 hours a day, seven days a week, often with only limited security features in place. Combine this lack of security with the fact that most modern phones now contain more processing power than the computers that landed Apollo 11 on the moon, and it's not hard to see why they are a hacker's weapon of choice.

Under attack

The worst case scenario? You could wake up one morning to the police kicking down your door, investigating a sophisticated cyberattack with all the evidence pointing to you. Regardless of how ridiculous it may seem, in the absence of any cyber-monitoring or cyber-defence solution you would have a very hard time proving that you were not guilty. And it is not just hackers you need to worry about, even the US National Security Agency and the UK's GCHQ have secretly used innocent people's devices to cover their malicious activities.

In my career as a cyber forensics investigator, I have not only seen many of these cases but also scenarios where hackers have been hired by organisations to deliberately frame employees by planting material such as child pornography onto their work phones. The person in question is then accused, for example, of selling secret company information to competitors and when the legal team investigates their phone, they find the child pornography. It is a scary prospect.

Many people wrongly believe that their mobile service providers should deploy cyber-protection mechanisms for their users. But if you read the terms of service, you will clearly see that as the owner and user, it is solely your responsibility to protect yourself. Exactly in the same way that you protect your laptop when you surf the internet.

If you are reading this and you are yet to install at least an anti-virus application on your phone, stop reading immediately and install one – there are many good anti-virus applications that are completely free. You should also make sure to only install applications from well-known app markets such as Google Play or the Apple or Windows

Stores. Never "jail break" or root your phone to install free apps unless you are a security expert and know what you are doing.

And it may sound like common sense, but do not click on the links you receive from unknown sources. It is also a good idea to have all your phone data encrypted and to install a logging or monitoring solution on your phone to have records of all activity. It could well turn out to be your "get out of jail free card" – just on the off chance anything were to happen.

This article was originally published on The Conversation. *Read the* original article.

Provided by The Conversation
APA citation: How to stop your phone from being hacked (2016, May 25) retrieved 26 May 2016 from http://phys.org/news/2016-05-hacked.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.