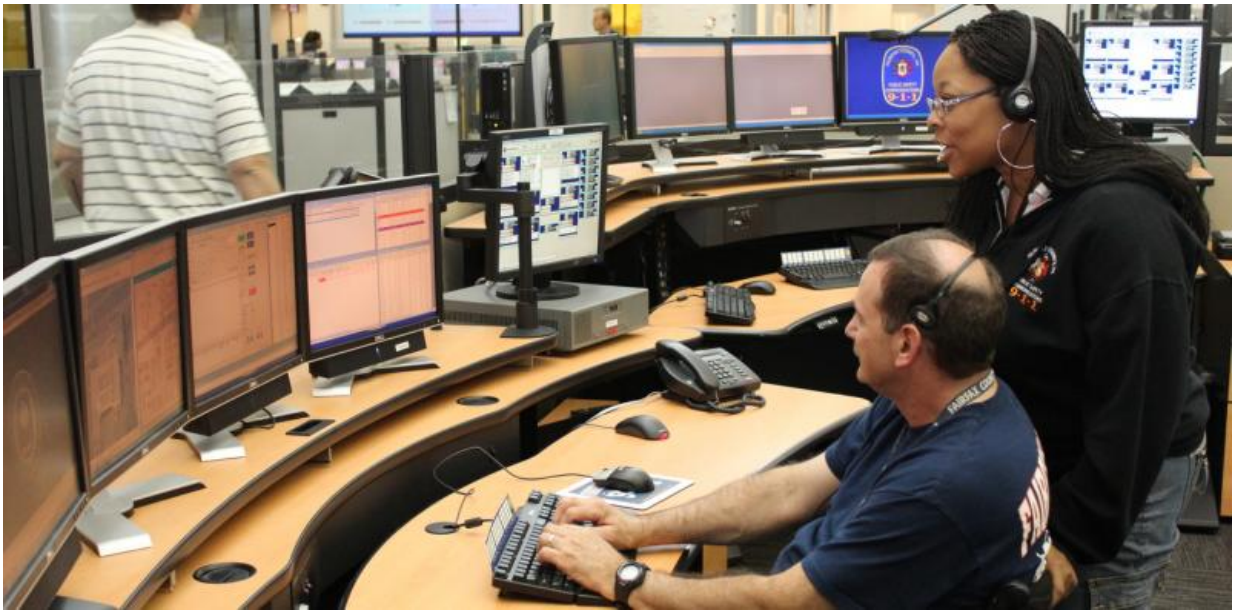
Attackers can make it impossible to dial emergency services

January 5 2017, by Mordechai Guri, Yisroel Mirsky And Yuval Elovici



When calling these people, you want to be able to get through. Credit: Fairfax County, Virginia

It's not often that any one of us needs to dial 911, but we know how important it is for it to work when one needs it. It is critical that 911 services always be available – both for the practicality of responding to emergencies, and to give people peace of mind. But a new type of attack has emerged that can knock out 911 access – our research explains how these attacks occur as a result of the system's vulnerablities. We show

these attacks can create extremely serious repercussions for public safety.

In recent years, people have become more aware of a type of cyberattack called "denial-of-service," in which websites are flooded with traffic – often generated by many computers hijacked by a hacker and acting in concert with each other. This happens all the time, and has affected traffic to financial institutions, entertainment companies, government agencies and even key internet routing services.

A similar attack is possible on 911 call centers. In October, what appears to be the first such attack launched from a smartphone happened in Arizona. An 18-year-old hacker was arrested on charges that he conducted a telephone denial-of-service attack on a local 911 service. If we are to prevent this from happening in more places, we need to understand how 911 systems work, and where the weaknesses lie, both in technology and policy.

Understanding denial of service

Computer networks have capacity limits – they can handle only so much traffic, so many connections, at one time. If they get overloaded, new connections can't get through. The same thing happens with phone lines – which are mostly computer network connections anyway.

So if an attacker can manage to tie up all the available connections with malicious traffic, no legitimate information – like regular people browsing a website, or calling 911 in a real emergency – can make it through.

This type of attack is most often done by spreading malware to a great many computers, infecting them so that they can be controlled remotely. Smartphones, which are after all just very small computers, can also be

hijacked in this way. Then the attacker can tell them to inundate a particular site or phone number with traffic, effectively taking it offline.

Many internet companies have taken significant steps to guard against this sort of attack online. For example, Google Shield is a service that protect news sites from attacks by using Google's massive network of internet servers to filter out attacking traffic while allowing through only legitimate connections. Phone companies, however, have not taken similar action.

Addressing the 911 telephone system

Before 1968, American emergency services had local phone numbers. People had to dial specific numbers to reach the fire, police or ambulance services – or could dial "0" for the operator, who could connect them. But that was inconvenient, and dangerous – people couldn't remember the right number, or didn't know it because they were just visiting the area.

The 911 system was created to serve as a more universal and effective system. As it has developed over the years, a 911 caller is connected with a specialized call center – called a public safety answering point – that is responsible for getting information from the caller and dispatching the appropriate emergency services.

These call centers are located in communities across the country, and each provides service to specific geographic regions. Some serve individual cities, while others serve wider areas, such as counties. When telephone customers dial 911 on their landlines or mobile phones, the telephone companies' systems make the connection to the appropriate call center.

To better understand how denial-of-service attacks could affect 911 call

systems, we created a detailed computer simulation of North Carolina's 911 infrastructure, and a general simulation of the entire U.S. emergency-call system.

Investigating the impact of an attack

After we set up our simulation, we attacked it to find out how vulnerable it is. We found that it was possible to significantly reduce the availability of 911 service with only 6,000 infected mobile phones – just 0.0006 percent of the state's population.

Using only that relatively small number of phones, it is possbile to effectively block 911 calls from 20 percent of North Carolina landline callers, and half of mobile customers. In our simulation, even people who called back four or five times would not be able to reach a 911 operator to get help.

Nationally, a similar percentage, representing just 200,000 hijacked smartphones, would have a similar effect. But this is, in a certain sense, an optimistic finding. Trey Forgety, the director of government affairs for the National Emergency Number Association, responded to our findings in the Washington Post, saying, "We actually believe that the vulnerability is in fact worse than [the researchers] have calculated."

Policy makes the threat worse

These sorts of attacks could, potentially, be made less effective if malicious calls were identified and blocked at the moment they were placed. Mobile phones have two different kinds of identifying information. The IMSI (International Mobile Subscriber Identity) is the phone number a person must call to reach that phone. The IMEI (International Mobile Station Equipment Identity) is used to track the

specific physical device on the network.

A defense system could be set up to identify 911 calls coming from a particular phone that has made more than a certain number of 911 calls in a given period of time – say more than 10 calls in the last two minutes.

This raises ethical problems – what if there is a real and ongoing emergency, and someone keeps losing phone reception while talking to a dispatcher? If they called back too many times, would their cries for help be blocked? In any case, attackers who take over many phones could circumvent this sort of defense by telling their hijacked phones to call less frequently – and by having more individual phones make the calls.

But federal rules to ensure access to emergency services mean this issue might be moot anyway. A 1996 Federal Communications Commission order requires mobile phone companies to forward all 911 calls directly to emergency dispatchers. Cellphone companies are not allowed to check whether the phone the call is coming from has paid to have an active account in service. They cannot even check whether the phone has a SIM card in place. The FCC rule is simple: If anyone dials 911 on a mobile phone, they must be connected to an emergency call center.

The rule makes sense from a public safety perspective: If someone is having (or witnessing) a life-threatening emergency, they shouldn't be barred from seeking help just because they didn't pay their cellphone bill, or don't happen to have an active account.

But the rule opens an vulnerability in the system, which attackers can exploit. A sophisticated attacker could infect a phone in a way that makes it dial 911 but report it does not have a SIM card. This "anonymized" phone reports no identity, no phone number and no information about who owns it. Neither the phone company nor the 911

call center could block this call without possibly blocking a legitimate call for help.

The countermeasures that exist, or are possible, today are difficult and highly flawed. Many of them involve blocking certain devices from calling 911, which carries the risk of preventing a legitimate call for help. But they indicate areas where further inquiry – and collaboration between researchers, telecommunications companies, regulators and emergency personnel – could yield useful breakthroughs.

For example, cellphones might be required to run a monitoring software to block themselves from making fraudulent 911 calls. Or 911 systems could examine identifying information of incoming calls and prioritize those made from phones that are not trying to mask themselves. We must find ways to safeguard the 911 system, which protects us all.

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

Provided by The Conversation

Citation: Attackers can make it impossible to dial emergency services (2017, January 5) retrieved 6 May 2024 from https://phys.org/news/2017-01-impossible-dial-emergency.html