Next generation 911 services are highly vulnerable to cyberattacks

11 March 2020

Credit: CC0 Public Domain

Despite a previous warning by Ben-Gurion University of the Negev (BGU) researchers, who exposed vulnerability in the 911 system due to distributed denial of service attacks (DDoS), the next generation of 911 systems that now accommodate text, images and video still have the same or more severe issues.

In the study published by *IEEE Transactions in Dependable and Secure Computing*, the BGU researchers evaluated the impact of DDoS attacks on the current (E911) and next generation 911 (NG911) infrastructures in North Carolina. The research was conducted by Dr. Mordechai Guri, head of research and development, BGU Cyber Security Research Center (CSRC), and chief scientist at Morphisec Technologies, and Dr. Yisroel Mirsky, senior cyber security researcher and project manager at the BGU CSRC.

In recent years, organizations have experienced countless DDoS attacks, during which internet-connected devices are flooded with traffic—often generated by many computers or phones called "bots" that are infected by malware by a hacker and act in concert with each other. When an attacker ties up all the available connections with malicious traffic, no legitimate information—like calling 911 in a real emergency—can make it through.

"In this study, we found that only 6,000 bots are sufficient to significantly compromise the availability of a state's 911 services and only 200,000 bots can jeopardize the entire United States," Dr. Guri explains.

When telephone customers dial 911 on their landlines or mobile phones, the telephone companies' systems make the connection to the appropriate call center. Due to the limitations of original E911, the U.S. has been slowly transitioning the older circuit-switched 911 infrastructure to a packet-switched voice over IP (VoIP) infrastructure, NG911. It improves reliability by enabling load balancing between emergency call centers or public safety answering points (PSAP). It also expands 911 service capabilities, enabling the public to call over VoIP, transmit text, images, video, and data to PSAPs. A number of states have implemented this and nearly all other states have begun planning or have some localized implementation of NG911.

Many internet companies have taken significant steps to safeguard against this sort of online attack. For example, Google Shield is a service that protects news sites from attacks by using Google's massive network of internet servers to filter out attacking traffic, while allowing through only legitimate connections. However, phone companies have not done the same.

To demonstrate how DDoS attacks could affect 911 call systems, the researchers created a detailed simulation of North Carolina's 911 infrastructure, and a general simulation of the entire U.S. emergency-call system. Using only 6,000 infected phones, it is possible to effectively block 911 calls

from 20% of the state's landline callers, and half of the 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," Dr. Guri says.

The countermeasures that exist today are difficult and not without flaws. Many 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 blacklist or 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.

"Many say that the new NG911 solves the DDoS problem because callers can be connected to PSAPs around the country, not just locally," Dr. Mirsky explains. "Nationally, with complete resource sharing, the rate that callers give up trying—called the 'despair rate'—is still significant: 15% with 6,000 bots and 43% with 50,000 bots.

"But the system would still need to communicate locally to dispatch police, medical and fire services. As a result, the despair rate is more likely to be 56% with 6,000 bots—worse than using the original E911 infrastructure."

According to Dr. Guri, "We believe that this research will assist the respective organizations, lawmakers and security professionals in understanding the scope of this issue and aid in the prevention of possible future attacks on the 911 emergency services. It is critical that 911 services always be available—to respond quickly to emergencies and give the public peace of mind."

More information: Yisroel Mirsky et al, DDoS Attacks on 9-1-1 Emergency Services, *IEEE Transactions on Dependable and Secure Computing* (2020). DOI: 10.1109/TDSC.2019.2963856

Provided by American Associates, Ben-Gurion University of the Negev