Hackers gonna hack: UH Gets $2.6m to protect next-gen 911 centers

November 13 2015

With $2.6 million in funding from the Department of Homeland Security, University of Houston computer science professors Stephen Huang, Omprakash Gnawali and Larry Shi are working to develop low-cost mitigation strategies to strengthen the resilience of emergency response systems against Distributed Denial of Service, or DDoS, attacks. Credit: Chris Watts

Cyberattacks are no longer a question of if, but when. It's become a regular occurrence to hear of breaches hitting private companies, the government, retailers, airlines, banks, law firms and, now, even 911 dispatch centers. Computer scientists at the University of Houston are joining forces with the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) to confront these threats. UH has been awarded $2.6 million to develop technology to help protect emergency response systems, such as current and next-generation 911 systems, against Distributed Denial of Service (DDoS) attacks. UH's award is part of a larger Distributed Denial of Service Defenses (DDoSD) program announce by DHS recently.

DDoS attacks are an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. Additionally, the attacks addressed by the UH computer scientists not only threaten to disrupt emergency services, but also hold them hostage by demanding a ransom.

"These hackers engage in blackmail, trying to extort payment in return for not launching an attack that would make access to 911 services unavailable," said Larry Shi, the principal investigator (PI) on the grant and assistant professor of computer science at UH. "Banks have been a big target, and emergency services have also been compromised. The FBI and DHS issued security alert warnings to call centers of the possibility of such attacks. While this has not yet taken place in Houston, it has happened in New York."

Used to render key resources unavailable, a classic DDoS attack usually seeks to disrupt an organization's website and temporarily block a consumer's ability to access it. A more strategic attack makes a key resource inaccessible during a critical period, which is what Shi and his colleagues are working proactively to prevent.

In Houston, for example, the largest one is the Houston Emergency Center and gets more than three million emergency calls annually. During inclement weather or large-scale, citywide special events, the average 9,000 daily calls the center receives can easily double. Citing examples of actual cyberattacks that have transpired in other cities, Shi noted a case in New York where service was lost from several hours to a day.

"This could become a life or death matter for callers in medical distress or reporting a fire," he said. "Whether it's a person experiencing a heart attack or an explosion at one of Houston's many chemical plants, every minute is critical in mitigating damage and reducing issues. We aim to address this now before it becomes a problem, as well as develop solutions to be better prepared in case a cyberattack does come to pass."

Another scenario that played out in California, he said, involved tens of thousands of prank calls. He explained how programs can be written to make calls with robots to easily overwhelm an emergency call center's resources. Adding to the problem is that many call centers are traditionally understaffed. He noted that even dead cell phones not connected to a service can be hacked to make 70 calls per minute, preventing those with valid emergencies from getting through.

Any organization that relies on network resources, even an emergency management system, is considered a potential target, and the current environment offers many advantages to the attacker. As 911 emergency services consolidate to share infrastructure and resources and as more systems become connected to and reliant upon the Internet, these systems become vulnerable to DDoS attacks. The next generation 911 system, NG9-1-1, will enable emergency calls from any wired, wireless or IP-based device, as well as allow multimedia sharing. This evolution may make NG9-1-1 more vulnerable to different types of existing or new cyberattacks.

Shi and his co-PIs professor Stephen Huang and assistant professor Omprakash Gnawali, also in the Department of Computer Science at UH, will be working to develop low-cost mitigation strategies to significantly strengthen the resilience of emergency response systems against DDoS attacks.

With the goal to develop technology that improves security, defense and resilience, Shi explained his group's three-tiered approach. They will first do a vulnerability analysis to proactively identify potential weaknesses that need to be fortified before those targets and holes are attacked. Secondly, they will develop mitigation strategies, solutions and best practices for how to respond if a security breach does occur. The third task is to make the results readily accessible and adaptable by emergency service providers, providing a layman-friendly plan with liaisons to help emergency call centers adopt and implement the recommendations developed by the researchers.

Yang Lu, another UH computer science researcher on the team and the program manager of the effort, said they will work with a variety of consultants and subcontractors, including SecureLogix, a firm specializing in solutions to address real-world problems in the enterprise voice security market; First Watch, a leader in real-time public safety data analysis used by police, fire, emergency medical services and public health organizations; and the Industry Council for Emergency Response Technology, or iCERT, a trade association focused on the commercial sector in the emergency response technologies field. Lu said they also will be working with reformed hackers, who now perform security consulting services for both private industry and the government, to sniff out vulnerabilities.

"With Wi-Fi in everything and the prevalence of smart devices nowadays, we must think out of the box," Shi said. "Even refrigerators can be hacked, and there was, in fact, a case where a refrigerator was

taken over by a hacker and used as a tool in a denial of service attack to extort money from a bank. Learning of cases such as this, it's not surprising, then, to hear 911 also is vulnerable."

Provided by University of Houston

Citation: Hackers gonna hack: UH Gets $2.6m to protect next-gen 911 centers (2015, November 13) retrieved 1 July 2024 from https://phys.org/news/2015-11-hackers-gonna-hack-uh-26m.html