Denial-of-Service Attacks to UMTS

Elisa Bertino, Purdue University

This installment of Computer's series highlighting the work published in IEEE Computer Society journals comes from IEEE Transactions on Dependable and Secure Computing.

Cellular communication networks are among today's most critical infrastructures, making possible important applications including location-based services, emergency management, and continuous healthcare monitoring. Consequently, cellular communication networks have been extensively analyzed to identify security threats and devise corresponding mitigation techniques. However, because achieving 100 percent security is impossible and new attacks are continuously being reported, it's crucial to research and identify new threats and vulnerabilities to improve network defenses.

In "A Denial of Service Attack to UMTS Networks Using SIM-Less Devices" (*IEEE Transactions on Dependable and Secure Computing*, vol. 11, no. 3, 2014, pp. 280–291), Alessio Merlo and his colleagues make an important breakthrough in cellular network security as they identify a novel *denial of service* (DoS) attack against universal mobile telecommunication system (UMTS) infrastructures. A DoS attack is disruptive and typically prevents legitimate users and applications from accessing networks.

The new attack operates at the user level and thus doesn't require hacking a network's intra-operator facilities. It also doesn't require that mobile devices be equipped with a valid subscriber identity module (SIM), making it fairly easy to carry out. This attack specifically targets the functionality of the home location register (HLR) database, which stores information about mobile subscribers and rules for call blocking and forwarding. Because the HLR is a central component of a cellular network, its inability to respond to legitimate users' requests makes the network's communication services unavailable to these users, disrupting network coverage. The article provides details about the attacking devices' design and an in-depth analysis showing that this new attack can reach cellular networks with an order of magnitude fewer resources than previous attacks.

It's crucial to research and identify new threats and vulnerabilities to improve network defenses.

What distinguishes this new attack from previous attacks is that it doesn't require using a *botnet*. A botnet is a network of mobile devices owned by legitimate users that can be coordinated by a comman-and-control center to perform attacks unbeknownst to these users. The article shows that unlike botnet-based attacks, the new attack isn't impacted by user mobility, so the attack can be placed very precisely. The article doesn't propose a solution to protect against these attacks, so further research should look into identifying defenses, such as those based on anomaly detection.

This article is an important reference for researchers in academia and industry interested in securing cellular networks, as it demonstrates the importance of identifying all bottlenecks in a network infrastructure and making sure these bottlenecks can't be exploited by attackers. It's also a must-read for anyone interested in testing the robustness of HLR implementation solutions.

ELISA BERTINO is a professor in the Computer Science Department, Cyber Center, and the Center for Education and Research in Information Assurance and Security (CERIAS) at Purdue University. Contact her at bertino@cs.purdue.edu.

0018-9162/15/$31.00 © 2015 IEEE