Insecurity of Operational Cellular IOT Service: New Vulnerabilities, Attacks, and Countermeasures.

Rahavee Prabakaran

The research paper deals with the security vulnerabilities when IOT services are integrated with cellular networks, devices two proof of concept attacks, validates them experimentally, evaluates them based on a prototype. The steps as mentioned above is used to address several attacks on IOT cellular services. Five vulnerabilities are discovered in the paper which are from system-integrated and service integrated for security attacks. When system-integrated aspect is addressed, there are two vulnerabilities - remote identification of cellular IOT IP addresses(V1) and cellular IOT PSM-unaware charging(V2). Talking about the service-integrated aspect there are three other vulnerabilities namely leakage of phone-number device type from VoLTE Signaling(V3), leakage of phone-number status from SMS signaling(V4), and insecure pushed text service(V5). In one of the attacks called Data Spamming, the attacker launches a Man in The Middle attack, where the adversary is assumed to operate on public communication channels from the network route between the cellular IoT devices and the IoT servers. The paper then moves on to addressing the second part, that is devising proof of concept attack using vulnerabilities V1 and V2. The attackers obtain a list of IP addresses owned by their target carriers using free online databases and probe the IP addresses and send spam traffic to the identified addresses. Then follows the third step, that is to experimentally validate the spamming attack. Three carriers US-I, US-II and US-III are used test with TCP and UDP traffic. For each carrier, the test application on each of those devices connects to the IoT server. CloT-Prober identifies the IP-addresses used by the IoT devices and sends spam traffic to each identified IP address. The paper then studies the results of this experiment, one being observed is that there are no false positive cases, IoT devices did not receive any spam traffic but are charged for it, US-I, US-II imposes charging volume caps in observed TCP spam results and US-I imposes charging volume caps as observed from UDP spam results. IoT spamming attack leads to excess bills and denial of IoT service. The second attack addresses on this paper id “Text Spamming” where the attacker has full control of a rooted smartphone that has the VoLTE and text services enabled. For IoT spamming text attack, proof of concept attack is devised based on the service-integrated related vulnerabilities. Phone numbers belonging to the target carriers with vulnerability - insecure pushed text service is collected using some online databases. The attack is evaluated by reducing the number of IoT numbers to one. IoTNumProber developed checks if the given phone number is an IoT number and TextSpamSender developed generates a large number of spam text messages to the given IoT number. Vertically integrated IoT security is proposed to address vulnerability V1, and Horizontally Integrated IoT security is proposed to address vulnerability V2, Privacy-aware voice and text services for V3 and V4, and finally Spamming-resistant cellular IoT text service for addressing V5.

Three strong points:

1. The paper deals with exceptionally well-defined steps for identification, devising proof of concept attacks, validating and evaluating them experimentally and based on a prototype.
2. Devising proof of attack for Android devices is explained well.
3. Each of the vulnerabilities is explained in detail, including their validation and root cause.

Three weak points:

1. The paper did not explain how each of the components in the Cellular IoT Network architecture perform functions to identify attacks, evaluate attacks.
2. The paper did not address how proof of concept Attack is devised and experimented with iPhone devices, Window phones.
3. The answer if all types of phones with different operating systems have the same type of vulnerabilities when integrated with IOT networks is not addressed in the paper.