Phone Hackers: Britain's Secret Surveillance

Description

IMSI catchers (international mobile subscriber identity-catcher) are portable surveillance tools used for spying on thousands of phones in a targeted area, tracking their location and even intercepting calls, messages, and data. They are supposed to help identify serious criminals, but cannot operate without monitoring innocent people too. UK police have IMSI catchers, but they refuse to tell the public how and when they are used. This has privacy campaigners worried…

Further References

van den Broek, F., Verdult, R., & de Ruiter, J.. (2015). Defeating IMSI Catchers. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security – CCS '15 (pp. 340–351). New York, New York, USA: ACM Press

Plain numerical DOI: 10.1145/2810103.2813615
DOI URL
directSciHub download

Show/hide publication abstract

"IMSI catching is a problem on all generations of mobile telecommunication networks, i.e., 2g (gsm, gprs), 3g (hdspa, edge, umts) and 4g (lte, lte+). currently, the sim card of a mobile phone has to reveal its identity over an insecure plaintext transmission, before encryption is enabled. this identifier (the imsi) can be intercepted by adversaries that mount a passive or active attack. such identity exposure attacks are commonly referred to as 'imsi catching'. since the imsi is uniquely identifying, unautho-rized exposure can lead to various location privacy attacks. we propose a solution, which essentially

replaces the im-sis with changing pseudonyms that are only identifiable by the home network of the sim's own network provider. con-sequently, these pseudonyms are unlinkable by intermedi-ate network providers and malicious adversaries, and there-fore mitigate both passive and active attacks, which we also formally verified using proverif. our solution is compati-ble with the current specifications of the mobile standards and therefore requires no change in the infrastructure or any of the already massively deployed network equipment. the proposed method only requires limited changes to the sim and the authentication server, both of which are un-der control of the user's network provider. therefore, any individual (virtual) provider that distributes sim cards and controls its own authentication server can deploy a more pri-vacy friendly mobile network that is resilient against imsi catching attacks."
Dabrowski, A., Pianta, N., Klepp, T., Mulazzani, M., & Weippl, E.. (2014). IMSI-catch me if you can. In Proceedings of the 30th Annual Computer Security Applications Conference on – ACSAC '14 (pp. 246–255). New York, New York, USA: ACM Press

Plain numerical DOI: 10.1145/2664243.2664272
DOI URL
directSciHub download

Show/hide publication abstract

"IMSI catchers are used in mobile networks to identify and eavesdrop on phones. when, the number of vendors in-creased and prices dropped, the device became available to much larger audiences. self-made devices based on open source software are available for about us$ 1,500. in this paper, we identify and describe multiple methods of detecting artifacts in the mobile network produced by such devices. we present two independent novel implementations of an imsi catcher catcher (icc) to detect this threat against everyone's privacy. the first one employs a network of stationary (sicc) measurement units installed in a geo-graphical area and constantly scanning all frequency bands for cell announcements and fingerprinting the cell network parameters. these rooftop-mounted devices can cover large areas. the second implementation is an app for standard consumer grade mobile phones (micc), without the need to root or jailbreak them. its core principle is based upon geographical network topology correlation, facilitating the ubiquitous built-in gps receiver in today's phones and a network cell capabilities fingerprinting technique. the latter works for the vicinity of the phone by first learning the cell landscape and than matching it against the learned data. we implemented and evaluated both solutions for digital self-defense and deployed several of the stationary units for a long term field-test. finally, we describe how to detect recently published denial of service attacks."
Norrman, K., Näslund, M., & Dubrova, E.. (2016). Protecting IMSI and User Privacy in 5G Networks. In Proceedings of the 9th EAI International Conference on Mobile Multimedia Communications. ACM

Plain numerical DOI: 10.4108/eai.18-6-2016.2264114
DOI URL
directSciHub download

Show/hide publication abstract

"In recent years, many cases of compromising users' privacy in telecom networks have been reported. stories of 'fake' base stations capable of tracking users and collecting their personal data without users' knowledge have emerged. the current way of protecting privacy does not provide any protection against an active attacker on the air-interface, claiming to be a legitimate network that has lost the temporary identity. moreover, there is also no

protection against passive eavesdroppers who are present when requests for international mobile subscriber identity (imsi) are made. this paper presents a new method for protecting the imsi by means of establishing a pseudonym between the user equipment and the home network. the pseudonym is derived locally at the user equipment and the home network without affecting existing universal subscriber identity modules (usims). we analyse the solution from a technical perspective , as well as from a regulatory and operational perspective. the presented method protects the imsi from passive and active imsi-catchers as well as honest but curious serving networks. moreover, it can recover from lock-out situations where one party has lost the pseudonym."
Ney, P., Smith, I., Cadamuro, G., & Kohno, T.. (2017). SeaGlass: Enabling City-Wide IMSI-Catcher Detection. Proceedings on Privacy Enhancing Technologies, 2017(3), 39–56.

Plain numerical DOI: 10.1515/popets-2017-0027
DOI URL
directSciHub download

Show/hide publication abstract

"Cell-site simulators, also known as imsi-catchers and stingrays, are used around the world by governments and criminals to track and eavesdrop on cell phones. despite extensive public debate surrounding their use, few hard facts about them are available. for example, the richest sources of information on u.s. government cell-site simulator usage are from anonymous leaks, public records requests, and court proceedings. this lack of concrete information and the difficulty of independently obtaining such information hampers the public discussion. to address this deficiency, we build, deploy, and evaluate seaglass , a city-wide cellsite simulator detection network. seaglass consists of sensors that measure and upload data on the cellular environment to find the signatures of portable cell-site simulators. seaglass sensors are designed to be robust, low-maintenance, and deployable in vehicles for long durations. the data they generate is used to learn a city's network properties to find anomalies consistent with cell-site simulators. we installed seaglass sensors into 15 ridesharing vehicles across two cities, collecting two months of data in each city. using this data, we evaluate the system and show how seaglass can be used to detect signatures of portable cell-site simulators. finally, we evaluate our signature detection methods and discuss anomalies discovered in the data."
OHanlon, P., Borgaonkar, R., & Hirschi, L.. (2017). Mobile Subscriber WiFi Privacy. In 2017 IEEE Security and Privacy Workshops (SPW) (pp. 169–178). IEEE

Plain numerical DOI: 10.1109/SPW.2017.14
DOI URL
directSciHub download

Show/hide publication abstract

"—This paper investigates and analyses the insufficient protections afforded to mobile identities when using today's operator backed wifi services. specifically we detail a range of attacks, on a set of widely deployed authentication protocols, that enable a malicious user to obtain and track a user's international mobile subscriber identity (imsi) over wifi. these attacks are possible due to a lack of sufficient privacy protection measures, which are exacerbated by preconfigured device profiles. we provide a formal analysis of the protocols involved, examine their associated configuration profiles, and document our experiences with reporting the issues to the relevant stakeholders. we detail a range of potential countermeasures to tackle these issues to ensure that privacy is better protected in the future."
Ekene, O. E., Ruhl, R., & Zavarsky, P.. (2016). Enhanced User Security and Privacy Protection in 4G LTE Network

. In 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC) (pp. 443–448). IEEE

Plain numerical DOI: 10.1109/COMPSAC.2016.108
DOI URL
directSciHub download

Show/hide publication abstract

“Although the evolved packet system authentication and key agreement (eps-aka) provides security and privacy enhancements in 3rd generation partnership project (3gpp), the international mobile subscriber identity (imsi) is sent in clear text in order to obtain service. various efforts to provide security mechanisms to protect this unique private identity have not resulted in methods implemented to protect the disclosure of the imsi. the exposure of the imsi brings risk to user privacy, and knowledge of it can lead to several passive and active attacks targeted at specific imsi’s and their respective users. further, the temporary mobile subscribers identity (tmsi) generated by the authentication center (auc) have been found to be prone to rainbow and brute force attacks, hence an attacker who gets hold of the tmsi can be able to perform social engineering in tracing the tmsi to the corresponding imsi of a user equipment (ue). this paper proposes a change to the eps-aka authentication process in 4g long term evolution (lte) network by including the use of public key infrastructure (pki). the change would result in the imsi never being released in the clear in an untrusted network.”
Lilly, A.. (2017). IMSI catchers: hacking mobile communications. Network Security, 2017(2), 5–7.

Plain numerical DOI: 10.1016/S1353-4858(17)30014-4
DOI URL
directSciHub download

Show/hide publication abstract

“You’re travelling, working on a new deal that’s just about to close. you’re involved in the final negotiations. you need to check a few points with colleagues back at base. you call them from a quiet place, away from eavesdroppers, from your mobile. but what about electronic eavesdroppers? these days a voice call is just another piece of data and it can be easily intercepted without you ever knowing. the apps you use on your mobile devices might claim to be secure – but is the device itself? what might it be giving away about you? the way our mobile networks function means that information can be intercepted and harvested by so-called imsi catchers. this could have a significant impact on your security and privacy. so what are these devices, what dangers do they pose and how can you protect yourself? andy lilly of armour communications provides some answers.”
Category

1. General

Tags

1. IMSI
2. mobile
3. Privacy
4. security
5. tracking
6. WiFi

Date Created
April 2019
Author
web45