Haktuts

All About Ethical Hacking,Hacking News,Security News,Privacy Issue,Cyber Crime,Pentesting Tools,Open Sources,Cyber Security,How-To,Tips And Tricks And Dark Web News

MIT invents untraceable SMS text messaging system that is even more secure than Tor

Computer scientists at the Massachusetts Institute of Technology (MIT) have developed a new SMS text messaging system that is untraceable and apparently even more secure than the Tor anonymity network, in order to create truly anonymous communications.

In July, researchers from MIT and the Qatar Computing Research Institute (QCRI) succeeded in cracking a security vulnerability affecting the Tor anonymity network to make it possible to identify hidden servers with up to 88% accuracy.

The researchers did this by looking for patterns in the number of packets passing in each direction through Tor nodes, and they found that they could tell with 99%

accuracy whether a circuit was for a regular web browsing request, an introduction point (which gives a user access to a hidden website) or a rendezvous point, which is used when another user wants to connect to the same hidden website at the same time as the first user.

Confusing would-be attackers with fake messages

Learning from this discovery, several researchers from MIT's Computer Science and Artificial Intelligence Laboratory (CSAIL) have developed a new system that permits the exchange of text messages between two parties at roughly once a minute.

Their open-access paper, titled Vuvuzela: Scalable Private Messaging Resistant to Traffic Analysis, was presented at the Association for Computing Machinery Symposium on Operating Systems Principles in October. Unlike Tor, the Vuvuzela system provides a strong mathematical guarantee of user anonymity by drowning out any visible traffic patterns that could lead to identification of the parties through issuing lots of spurious information.

Also See: How to Hack wpa wpa2-psk wifi using social engineering technique

To make the system work, one user leaves a message for another user at a predefined location, such as a memory address on an internet-connected dead-drop server, while the other user retrieves the message. So for example, if there were three people using the system but only two of them were sending text messages to each other, it would look obvious that the two people were talking to each other, as the only traffic on the server would come from exchanges between the two people.

To hide this, the system makes all the users send out regular messages to the dead-drop server, whether they contain any information or not, so then the traffic pattern makes it look like there is traffic going through the server from multiple locations at all times.

Using three servers to disguise the messages even more

But just sending out regular spoof messages is not enough to confuse the bad guys. If an attacker managed to infiltrate the dead-drop server, the criminal would instantly be able to see which users were actually communicating and where the messages were being sent by looking to see which users were accessing which memory addresses.

So to make it even harder for attackers to infiltrate Vuvuzela, the system uses not one but three different servers. All the messages, both real and fake, are sent through the system wrapped in three layers of encryption.

The first server peels off the first layer of encryption on a message and then passes the message onto the second server, but the first server also deliberately mixes up the order of the messages so they get to the second server in a different order, and the second server does the same, so only the third server can see which are the real messages which need to go to the memory address so a user pick it up.

MIT says that statistically, as long as one of the three servers is not compromised the system still works to protect the messages.

"Tor operates under the assumption that there's not a global adversary that's paying attention to every single link in the world," said Nickolai Zeldovich, an associate professor of computer science and engineering, and co-leader of the Parallel and Distributed Operating Systems group at CSAIL.

"Maybe these days this is not as good of an assumption. Tor also assumes that no single bad guy controls a large number of nodes in their system. We're also now thinking, maybe there are people who can compromise half of your servers."

Also See:

1. Mark Zuckerberg Quits His Job At Facebook, All Due To A Facebook Bug

2. Google patches critical media processing and rooting vulnerabilities in Android
3. Hacker-Friendly Search Engine that Lists Every Internet-Connected Device
4. Here's How Google Can "Remotely Bypass" Pattern Lock Of Android Device
5. Steam is 'hijacked' 77,000 times a month
6. Snowden Unveils NSA "God Mode" Malware That Lives On Your Motherboard And Can Not Be Traced
7. 6.1 Million smart devices at risk from 3 year old flaw
8. Critical Vulnerabilities Discovered in 3G/4G Modems Includes "Remote Code Execution,Cross-Site Request Forgery And Cross-Site Scripting"