Probing Mobile Operator Networks

Collin Mulliner
collin[at]mulliner.org

July 25th 2012

This document is the accompanying white paper for the presentation *Probing Mobile Operator Networks* at Black Hat USA 2012 in Las Vegas, NV, USA.

Today all devices need to be connected to a network somehow in order to communicate back home. This is either to get data back to the home network or to remotely control the device from the home network. Often devices are in the field, outside of the property of the device owner, and thus do not have a fixed network connection. To connect these devices to the home network they get equipped with wireless modems so they can be connected to the cellular network. Connecting devices to the cellular network is very convenient since mobile operators have made sure to service most populated areas around the world.

So now many device are Internet connected using cellular networks. This opens a number of questions, these are:

- What kind of devices are on mobile networks today?
- Which kind of device is popular?
- Are these devices reachable, from the cell network, the Internet?
- What are the security implications of these device?

The idea behind this research is to answer these questions and in addition determine how to answer these questions. The answers will tell us how cellular networks are used today for other tasks then mobile telephony and short messages. Yes, you read that correctly the presented results will not focus on mobile phones or smart phones but on industrial control or enterprise grade devices that are connected to the public Internet via the cellular network. So far we found applications such as vehicle tracking, portable bar code scanners, GPS devices, PLCs, and devices used for smart metering. As the use of old 2G cellular networks currently is on the rise for these kind of applications this provides an interesting forecast into the future of connected industrial and enterprise applications and their possible security impact.

For the actual details such as measurement methodology, obstacles, raw numbers, and graphs we kindly point the reader to the slides of the talk. The slide deck is very detailed and is suited for reading.

The slides are available on the Black Hat USA 2012 CD or at: http://mulliner.org/security/pmon/