Mission Secure, Inc.

Attack on Traffic Systems

From start to finish how a cyber attack would be performed on traffic system, we will go over first day >> exploitation of the device >> the real-world aftermath.

These attack examples have happened in the past.

We will take an in-depth look into the process of the chain of events that lead to the exploit.
Did not happen. But if it did.
24 CVE. From 10 Different Companies.

1. Microsoft - 5
2. Qualcomm - 2
3. Samsung - 5
4. Verizon - 4
5. AT&T - 1
6. HTC - 2
7. Trimble – 2
8. GM -1
9. FCA - 1
10. Google - 1
A work van in broken into while on a service call. At the intersection for NW River drive and NW 28th st there are several devices taken from a van.

1. An expensive GPS survey unit
2. A tablet PC
3. Two configured yet uninstalled S-408
What is an S-408? It is a fictitious device for that is the example for this presentation. This device and its configurations are now out of the intended owners controls.
While the GPS unit was sold locally on craigslist and the tablet to pawnshop the S-408 with no local market for the device was placed on an online auction which just ended at 9:30. The device is now on its way to new home outside of the United States.

The device was in a list from a script written by a Blackhat Hacker. The Script runs on all the worlds auctions sites searching for certain devices that are used in the USA, and restricted for export and are for sale to a private party.
After being mailed to England the package was forwarded to PO box and taken into North Korea. At this point the device was inspected after the box was opened.

The devices manual was downloaded online and translated for the next steps. The next steps will be performed by a team of attackers.
The S-408 is cleaned and hooked into using the chip trace and markings on the board. Once hooked into the boards JTAG ports the firmware is dumped off the device while it is booting.

The S-408 is also plugged into the network where all of the communications are observed. Once the expected communication is established a program called a fuzzer is used to enumerate errors and limitation of the device.
After 206 hours of the fuzzing script running the team of hackers look at the crash log of programs and services on the device. The “Core Dump” is extracted using the chip traces to the flash memory on the device.

The core dump shows 17 crashed processes. The software was not made to handle the constructed queries that were outside the bounds of normal traffic. The single process that detects baud changes between traffic systems did not check size before excepting communication from the other device.
The program has found a buffer overflow issue which will lead to unintended code. Once the “entry point” for the exploit is found.

The attacker looks at the amount of “space” of his payload. The payload is code that is constructed into a message after an error to make the computer think it was doing the commands when the crash occurred.
Once payload is decided the firmware pulled from the device is analyzed and common issues with other like Operating systems can be used. The attack of the system now affects all S-400 series running 6.5.0 to 7.1.3

The attackers use a Reverse shell exploit payload that was released in a previous exploit in 2016 for S-404 which is an older version of the system. This exploit simply turns Call home to the device on the select portion of the network.
How is the payload tested? What is the impact on the device?
How is the device exploited in the wild? Example: The system credentials are pulled from device and used as a platform to attack other devices and breach further.
Last stages of the attack. The affect of the other systems on the network.
How final attack impacts the system. Real world results.
We’re Hiring!

www.missionsecure.com