1400 - Using GPS Spoofing to control time

Friday at 14:00 in 101 Track
45 minutes | Tool
David "Karit" Robinson*Security Consultant, ZX Security*

GPS is central to a lot of the systems we deal with on a day-to-day basis. Be it Uber, Tinder, or aviation systems, all of them rely on GPS signals to receive their location and/or time.

GPS Spoofing is now a valid attack vector and can be done with minimal effort and cost. This raises some concerns when GPS is depended upon by safety of life applications. This presentation will look at the process for GPS and NMEA (the serial format that GPS receivers output) spoofing, how to detect the spoofing attacks and ways to manipulate the time on GPS synced NTP servers. We will also explore the implications when the accuracy of the time on your server can no longer be guaranteed.
David "Karit" Robinson
Dave/Karit has worked in the IT industry for over 10 years. In this time he has developed a skillset that encompasses various disciplines in the information security domain. Dave is currently part of team at ZX Security in Wellington and works as a penetration tester. Since joining ZX Security Dave has presented at Kiwicon, BSides Canberra and Unrestcon and also at numerous local meetups; along with running training at Kiwicon and Syscan. He has a keen interest in lock-picking and all things wireless.

@nzkarit

#defcon25/by_track/101/Friday #defcon25/By_Day/_Friday