Žad Deljkić: Android USB vektor napada

Dnevnik rada

1. tjedan (27.3.-2.4.2014.)

Dosadašnji rad

Do sada sam razvio prototip aplikacije za Android uređaje sa instaliranim Kali NetHunterom koja može preko USB-a detektirati OS te pokrenuti USB HID napad, te sam napisao nacrt rada na engleskom.

Napisao sam plan rada koji je okvirno dogovoren na početnom sastanku u petak 24.3. Trenutno istražujem što je moguće sa USB napadima, načine detektiranja OS-a preko USB-a te moguće zaštite protiv USB napada.

Dok sam istraživao zaštite protiv USB napada općenito, došao sam opet i do Qubes-a, OS-a koji je općenito fokusiran na sigurnost te ju postiže gotovo ekstremnom izolacijom, te sam ga sada i instalirao i trenutno ga isprobavam. Autori su svjesni raznih napada, između ostaloga i USB napada. No ako korisnik koristi USB tipkovnicu i/ili miš, ne postoji nikakva ugrađena zaštita od USB napada. I dalje je vjerojatno moguće nekako ručno zabraniti novim USB uređajima da se spoje (što opet nije idealno rješenje). USB HID napad (isprobao sam simuliranje tipkovnice) funkcionira na Qubes-u, moguće je direktno napasti dom0, najsigurniju domenu, no detektiranje OS-a ne funkcionira, računalo se ne spaja automatski na mrežu sa mobitelom.

Daljnji koraci

Jednom kada je istraživanje gotovo, osmisliti daljni smjer rada - što je točno problem kojim će se rad baviti, te kako ćemo ga rješiti.

Plan je napraviti nešto novo. Jedna opcija je nastaviti s već razvijenom aplikacijom, završiti ju te joj potencijalno proširiti funkcionalnosti. Druga opcija je osmisliti i implementirati novi USB napad koji do sada nije bio istražen, ukoliko pronađemo nešto takvo.