Bilaga 1.

Vinnarna i 5G Cyber Security Hackathon samt utmaningar presenterade av Ericsson, Nokia och Uleåborgs universitet

Ericsson Black Box Challenge:

Världens behov av konnektivitet förändras. Den globala mobildatatrafiken förväntas öka femfaldigt före slutet av 2024 och samtidigt förväntas 22 miljarder IoT-apparater bli anslutna till nätet. Föregående generationer av mobilnät koncentrerade sig på konsumentkommunikation och personlig kommunikation men nu kommer 5G att betjäna konsumenter och företag och ta sakernas internet till nästa nivå där konnektivitet av första klass är en grundförutsättning.

Ericsson har under flera år skapat ny grundtestning och försök med 5G. Vi tror verkligen på livslångt lärande och kontinuerlig förbättring. Även om säkerhet är inbyggd i våra produkter söker vi alltid saker som kan utvecklas.

Genom att ta denna utmaning till 5G Hackathon vill vi erbjuda dig en unik möjlighet att testa utvecklingsstadiet för nästa generations telekomutrustning som möjliggör till exempel smart tillverkning, distanshälsovård och mycket mer. Om du vill säkra framtiden är denna utmaning för dig!

Tekniska detaljer:

Denna utmaning ger dig en unik möjlighet att komma åt Ericssons nuvarande 5G-radioinfrastruktur och se om du kan hacka den. Kan du hitta sårbarheter? Syftet är att testa given infrastruktur genom kreativa lösningar och olika tekniker som innebär fysiskt tillträde till noder, för det är en sak som kommer att vara mer åtkomlig för angriparna än någonsin tidigare. Utmaningarna börjar med en "blackbox approach" som testar dina kunskaper och går sedan stegvis mot "whitebox testscenarier". Ericsson har experter vid denna utmaning. Vill du se hur långt du kan gå?

Vinnarna i Ericsson Challenge:

1.TDC SECURITY

2.NCC GROUP

3. SIG KILL

Nokia Home Network Challenge:

Nokias nya FastMile gateway är självständiga hemapparater med trådlös koppling till ditt 4G- eller 5G-nät samtidigt som de skapar en bättre och snabbare Wi-Fi-erfarenhet hemma. Nokia tar den senaste prototypen av nästa generation för testning innan den publiceras. Nokias Fastmile har flera gränssnitt som kan hackas. Nokia erbjuder tillträde till wifi-, moln-, administrations- och 5G-gränssnitt under tävlingen.

Läs mer om FastMile Gateway på: https://www.nokia.com/networks/solutions/fastmile/

Vinnarna i Nokia Challenge:

1.ABC OF SECURITY

2.TELIA CYGATE

3.SIG KILL

University of Oulu iHealth Challenge:

I sjukhusmiljö tillämpas nya teknologier snabbt för att låta läkare och sjukskötare göra sitt arbete på ett allt säkrare och effektivare sätt. För att säkerställa tillförlitlig konnektivitet, kort fördröjning och trygg användning förväntas 5G-nät bli använda för kritiska funktioner, till exempel i sjukhus.

Förlorad konnektivitet på operationsbordet? Förlorad kontroll över en apparat under operation? Nya teknologier presenterar nya outforskade hot mot nätsäkerhet. Uleåborgs universitet vill hitta cybersäkerhetsexperter som ska skydda den digitala framtiden i sjukhus. Systemets säkerhetsegenskaper kan förbättras om man hittar svaga punkter genom att hacka in i 5G-apparater, basstationer, servrar eller applikationer i en säker miljö.

Din uppgift är att hacka framtidens sjukhussimulation på vårt universitetscampus. Sjukhusmiljön är byggd med ett verkligt ändpunkt till ändpunkt 5G-nät som är integrerat med 4G. Miljön är alltså en så kallad 'non-standalone' arkitektur som 5G Testnätet erbjuder. Ett verkligt nät med tillträde till 5G och verkliga terminaler med hotspot-tillträde som möjliggör datatransmission via existerande teknologi med sensorering, VR och AR för hackning.

För hackning får du välja vilken kritisk funktionalitet som helst i vårt framtida sjukhus:

1. 5G-nätet via otillförlitlig perifer utrustning
2. kapa en 5G-terminal
3. störa 5G-radio eller angripa nätet från basstationen
4. tillhandahållande av tjänster i edge computing-miljön
5. någonting som vi inte ens kunde tänka på

Vinnarna i Oulu University Challenge:

1. DEEP CUTS

2. TCY

3:e plats fick ett hedersomnämnande