



Kronikkforfatterne viser blant annet til dette åpen kildekode-prosjektet som et interessant tiltak mot mobilavlytting. (Bilde: Android IMSI Catcher Detector)

IMSI-catchere er kommet for å bli

KRONIKK: Dette bør du vite for å unngå avlytting.



AV: HARALD BROMBACH | DEBATT | PUBLISERT: 29. DES. 2014 - 13:57

Av Øyvind Stensby og Aleksander Gorkowienko, PA Consulting Group

Aftenposten har avdekket bruk av «IMSI-catchere», som trolig er satt opp for å gi ukjente aktører sensitiv informasjon.

Hovedproblemet er at slike enheter enkelt kan bygges basert på vanlige mobil-komponenter eller annet lavkost radioutstyr, og at dette utstyret blir billigere for hver måned. Med andre ord, hvem som helst med teknisk innsikt og onde hensikter kan være i stand til å fange opp hva du og jeg sier. Videre finnes det en mengde oppskrifter på nettet som detaljert beskriver hvordan man kan bygge passive GSM-baserte avlytningsenheter.

Konsekvensen er at det ikke lenger nødvendigvis er agenter som bedriver klassisk sikkerhetsspijasje eller industrispijasje som står bak slik avlytning.

Nyhetsbrev fra digi.no

Hold deg oppdatert med de viktigste sakene fra digi.no rett i innboksen



Innlegget er skrevet av Øyvind Stensby og Aleksander Gorkowienko, begge fra PA Consulting Group.

Det kan like gjerne være presse, ulike former for «haktivister» eller andre som står bak. Trusselbilde er sammensatt og det eneste som er helt sikkert er at noen hele tiden kan få tak i ukryptert informasjon i mobilnettet. Det er et tankekors at informasjonssikkerhet i stor grad blir en salderingspost i IT-prosjekter, og at det i stor grad er en «det går stort sett bra»-holdning til informasjonssikkerhet.

Er det mulig å sikre seg mot slik overvåking?

Selvsagt finnes det tiltak som reduserer muligheten til overvåking. Det første er å se på hvordan IMSI sendes i nettet. [TMSI](#) bør i større grad benyttes. Dette hindrer at abonnenten blir identifisert. Videre kan det installeres programvare som alarmerer brukeren når det ikke foreligger kryptering. På samme måte som det finnes oppskrifter for folk med onde hensikter på nettet, finnes det også oppskrifter for hvordan man kan sikre seg på nettet.

Det er et interessant åpen kildekode-prosjekt kalt [Android IMSI Catcher Detector](#), som har til hensikt å avdekke og unngå falske base stasjoner (IMSI-fangere), og andre basestasjoner med dårlig eller ingen kryptering. Prosjektet har til hensikt å advare brukere om at kryptering er skrudd av i tillegg til flere andre beskyttelsesmekanismer. Kanskje er det slike tiltak som kan bli videreutviklet for å sikre telefonene til samfunnets nøkkelpersonell? Inntil dette er i drift bør det innføres sikkerhet i prosessene rundt bruk av mobilkommunikasjon. Regjeringen bør vurdere hyppig bytte av SIM-kort og telefon, og telefonen må selvfølgelig slås av og legges utenfor lyttbar avstand til møterom der viktige beslutninger tas.

Vi kan bare håpe at kommunikasjonsløsningene for pasientdata og andre kommende samfunnskritiske prosjekter tar høyde for den nye trusselen. Bruk av IMSI-catchere og andre «Man In The Middle»-angrep på kommunikasjon er kommet for å bli, og bedrifter og myndigheter må ta hensyn til dette når nye prosjekter planlegges.

Inntil videre får vi holde oss til den gamle, men utrolig effektive regelen fra Forsvaret når det gjelder behandling av fortrolig informasjon: «Mottoet er lett; hold tett».

Delta i debatten

Informasjon om debattinnlegg og kronikker i digi.no

Alle innlegg må sendes til redaksjon@digi.no. Husk å legge ved et portrettbilde. Vi forbeholder oss retten til å redigere innsendt materiale.

 Debatt

Nyhetsbrev fra digi.no

Hold deg oppdatert med de viktigste sakene fra digi.no rett i innboksen

Comments for this thread are now closed

0 Comments **digi.no**

Login ▾

Recommend Tweet Share

Sort by Best ▾

This discussion has been closed.

Subscribe Add Disqus to your site Add Disqus Disqus' Privacy Policy Privacy Policy Privacy Policy

Motta daglige nyhetsbrev fra digi.no?

Din e-postadresse

Ja, meld meg på

----- EKSKLUSIVT INNHOLD FOR DIGITALE ABONNENTER -----

Nyhetsbrev fra digi.no

Hold deg oppdatert med de viktigste sakene fra digi.no rett i innboksen

E-postadresse

Ja takk

Lukk