### Copy of identity (Rasmus)

Hvordan kan man kopiere/stjæle en ”telefons” identitet?

* Ved at kopiere EMEI og IMSI nummeret og sætte disse på en anden telefon

Hvorfor?

* For at skjule sin egen identitet
  + Terrorisme og anden organiseret kriminalitet
* I GSM netværk, skabes ens identitet ud fra to numre: IMEI (selve telefonen) og IMSI (sim kortet)
  + IMEI nummeret er ikke bundet til den enkelte bruger, men blot telefonen
  + IMSI nummeret er derimod bundet til brugeren, da nummeret sidder i simkortet, som følger brugeren af et telefonabonnement.
* DroidDream er en trojansk hest til Android, der er I stand til at finde oplysninger som EMEI og IMSI nummeret, og derefter sende det til kriminelle, der derved kan lægge disse oplysninger ind på henholdsvis en telefon og et simkort. Den angrebne telefon er hermed klonet, og man ville altså kunne ringe på offerets regning - tilmed med offerets telefonnummer. Dette kan eksempelvis bruges af terrorister til at skjule deres egen identitet.
  + Lignende trojan:
    - Android.Pjapps
    - Hong Tou Tou (a.k.a. ADRD)[[1]](#footnote-1)
  + Hvordan inficeres telefonen?
    - Gennem kinesiske android market kopier, hvor mange populære apps (især spil) er blevet ompakkede og inficerede med vira.
  + Der er flere forskellige måder at anskaffe sig IMSI nummeret, det kan bl.a. kopieres direkte fra simkortet, hvilket dog kræver specielt udstyr og fysisk adgang til simkortet, til gengæld tager det kun få sekunder.
    - I Android, kan enhver app dog få adgang til både IMEI og IMSI nummeret via funktionerne getDeviceId() og getSubscriberId() i biblioteket TelephonyManager.[[2]](#footnote-2)
  + En mere sofistikeret metode til at anskaffe sig oplysninger om brugeren, er at bygge sin egen GSM sendemast. Delene kan købes relativt billigt i ganske almindelige elektronikbutikker. Man kan på den måde opsnappe oplysninger om alle brugere tilknyttet denne sendemast.

1. The SAICB Report (NEWSLETTER-JULY-2011.pdf) [↑](#footnote-ref-1)
2. http://developer.android.com/reference/android/telephony/TelephonyManager.html [↑](#footnote-ref-2)