Analys av säkerhetsläget för *Internet Of Things* (IoT)

Bakgrund
IoT-marknaden har börjat lyfta och konsumenter kan köpa uppkopplade versioner av de flesta hushållsprodukter på marknaden såsom kylskåp, mikrovågsugnar och tv-apparater. Dessvärre kan dessa användas i storskaliga DDoS-, övervaknings- och andra attacker där ägarna till dem är omedvetna om att de är en del det botnät som utför attacken. Exempel finns där IoT-enheter använts för att utföra DDoS-attacker som gjorde att Twitter, SoundCloud, Spotify, Shopify samt vissa svenska myndighetssajter blev oåtkomliga.

Syfte
Exjobbet syftar till att undersöka säkerhetsläget på IoT-marknaden och att analysera hur det kommer sig att en stor andel av produkterna är sårbara.

- **Undersöka och kartlägga dagens tekniker för implementation av IoT**
  Vilka programmeringsspråk används för IoT? Vilka ramverk finns? Vilka typer av hårdvara körs produkterna på? Finns några existerande säkerhetslösningar för IoT? Hur vanligt förekommande är kryptering för kommunikation mellan enheter? …

- **Undersöka regler och lagar kring säkerhet för IoT**
  Finns det några krav på företagen i dagsläget? Kommer IoT-marknaden påverkas av GDPR?

- **Analysera kända attacker och undersök mönster kring säkerhetsbrister**
  Vilka typer av säkerhetsbrister är mest vanligen förekomna? Finns det några mönster? Finns det kopplingar till den teknik som används (punkt 1)? Hur svårt hade det varit att skydda enheterna mot dessa sårbarheter?

- **Visa praktiskt hur kända säkerhetsbrister kan användas för att bygga botnät**
  Visa hur ett botnät kan byggas av IoT-enheter genom att använda kända säkerhetsbrister

Din utbildning och erfarenhet
Detta arbete lämpar sig väl för en student i Datateknik, Informationsteknik, Elektroteknik, Teknisk fysik med inriktning datalogi eller motsvarande. Då exjobbet har en tydlig säkerhetsinriktning är kurser inom datasäkerhet ett krav. Ett intresse för *Internet Of Things* är meriterande.

pontus.thulin@omegapoint.se

omega point.