INSTITUTIONEN FÖR DATAVETENSKAP | LUNDS TEKNISKA HÖGSKOLA | PRESENTATIONSDAG 2015-08-28

EXAMENSARBETE The security of communication protocols used for Internet of Things
STUDENT Farhad Johari
HANDLEDARE Jesper Holmén Notander (LTH), Jens Christensen (Cybercom Sweden)
EXAMINATOR Flavius Gruian

Hur säkert är ”smarta hem”?

POPULÄRVETENSKAPLIG SAMMANFATTNING **Farhad Johari**

I takt med att “smarta hem” har blivit ett allt mer populärt koncept har säkerheten blivit en väldigt viktig fråga. Under detta examensarbete undersöks det hur felaktigt användande av en integrationslösning för smart hem kan göra hemmet känsligt för attacker.

Under de senaste åren har paradigmet Internet of Things varit ett mycket omtalat ämne i den teknologiska världen. Paradigmet har introducerats i industrier som exempelvis transport, sjukvård och hemnätverk. Smarta hem, som bygger på hemnätverk, är något som blivit mycket populärt och skälet till detta är att tillgängligheten av utrustning och det ökade intresset av att göra egna smarta lösningar i hemmet. Vid uppsättning av ett smart hem kan flera olika lösningar implementeras och det som skiljer lösningarna ifrån varandra är den struktur och process som används vid trådlös kommunikation. Med den växande trenden har säkerheten i smarta hem ifrågasatts då en bristfällig teknik kan möjliggöra intrång från obehöriga. Den trådlösa kommunikationen kan inte riktas till en enskild mottagare utan finns tillgänglig för alla inom räckhåll från den sändande enheten. Detta examensarbete har som målsättning att undersöka säkerheten i ett par olika lösningar och försöka besvara några av de säkerhetsfrågor som finns. Vidare fastställs vilken lösning som är bäst anpassad för smarta hem från en säkerhetssynvinkel.

Under arbetet har kommunikations protokollen som utnyttjats av ZigBee och Z-Wave analyserats på djupet ur en säkerhetssynvinkel. Potentiella brister i säkerheten betraktas och riskerna som dessa kan utgöra presenteras. Vidare sätts ett scenario upp för en Replay attack där en utomstående part fångar och skickar ut paket, och ett scenario för en Eavesdropping attack där fångad kommunikation försöker att tolkas. Resultaten av dessa scenario analyseras teoretiskt. Båda integrationslösningar jämförs med varandra och bevisar på olika sätt att de teoretiskt har tagit åtgärder för att förebygga dessa attacker.

Baserat på Z-Waves strikta protokoll och deras popularitet på marknaden väljes den för en praktisk undersökning. Ett smart hem konstrueras med den utvalda teknologin och de två scenarion som beskrivits utförs i praktiken. Resultatet av de praktiska attackerna visar att det teoretiska resultatet inte sammanfaller med det praktiska resultatet. Skillnaden beror på att den produkt som undersökts i det praktiska experimentet använde sig av ett statiskt värde istället för ett genererat slumpvärde. Detta leder till att det inte blir någon variation i kommunikations paketen vilket leder till att paket som innehåller samma kommando blir identiska. Slutsatsen som dras är att varje produkt som används i ett smart hem bör kontrolleras så att de följer riktlinjerna för hur protokollet ska användas. Om man inte har kunskap eller utrustning för att själv testa produkter kan man använda befintliga säkerhetskontroller som företag i samarbete med tillverkaren av integrationslösningen tagit fram, Z-Wave Alliance i Z-Waves fall.