RFID og SIKKERHED

En undersøgelse af sikkerheds aspekterne vedrørende RFID systemer.

18. April 2006

Martin Dam Pedersen

Institut for Matematik og Datalogi
Syddansk universitet

Indholdsfortegnelse

Hvad er RFID

RFID er en forkortelse for Radio-Frequency IDentification. De fleste forbinder RFID med de små chips(Tags) med unikke serienumre man påsætter alle mulige genstande sådan at disse kan identificeres. Man skal dog her huske på at disse chips ikke er nok i sig selv, men at man skal have et helt system bestående af RFID-tags, RFID-læsere og et backend system.

Da tagget kun indeholder et unikt serie nummer ligger data om et produkt derfor i backend systemets database. Det kunne for eksempel være oplysninger som varens navn, producenten, produktions tidspunkt m.m.

Forskellen på dette system og det gamle stregkode system er betydelige. For det første kan enhver vare få sit eget unikke serienummer, hvor man før kun kunne kategorisere en vare. Dette betyder at den enkelte vare i princippet kan følges fra fødsel til død. Desuden er aflæsningen af RFID tags betydeligt lettere end aflæsning af stregkoder. Hvor man før skulle have visuel kontakt med den vare man scanner er det nu nok at være indenfor en bestemt afstand af varen. Desuden kan en hel palle med f.eks. 100 forskellige varer scannes øjeblikkeligt uden nogen form for forsinkelse.

Hvor RFID kan bruges

RFID systemet kan bruges i en række forskellige sammenhænge og ikke kun til identifikation af varer. Som eksempler kan nævnes:

• Sporing af husdyr	• Lager styring
• Betalings systemer	• Detail handlen
• Tyveri beskyttelse	• Implantater
• Forfalsknings beskyttelse	• Biblioteker
• Adgangs kontrol	• Etc.....

Kun fantasien sætter grænser for hvor disse systemer kan bruges.

Sikkerhed og RFID

Som ovenstående liste viser kan RFID bruges i mange forskellige applikationer. Desuden er kravet til sikkerheden varierende afhængig af applikationen. Et af de meget diskuterede emner indenfor RFID er kravet om privatlivets fred. Hvis man forestiller sig en person med en masse forskellige tags på sig så kan enhver med en RFID læser læse disse, og derfra udlede en masse personlige oplysninger om personen. Illustrationen nedenfor beskriver dette scenario.

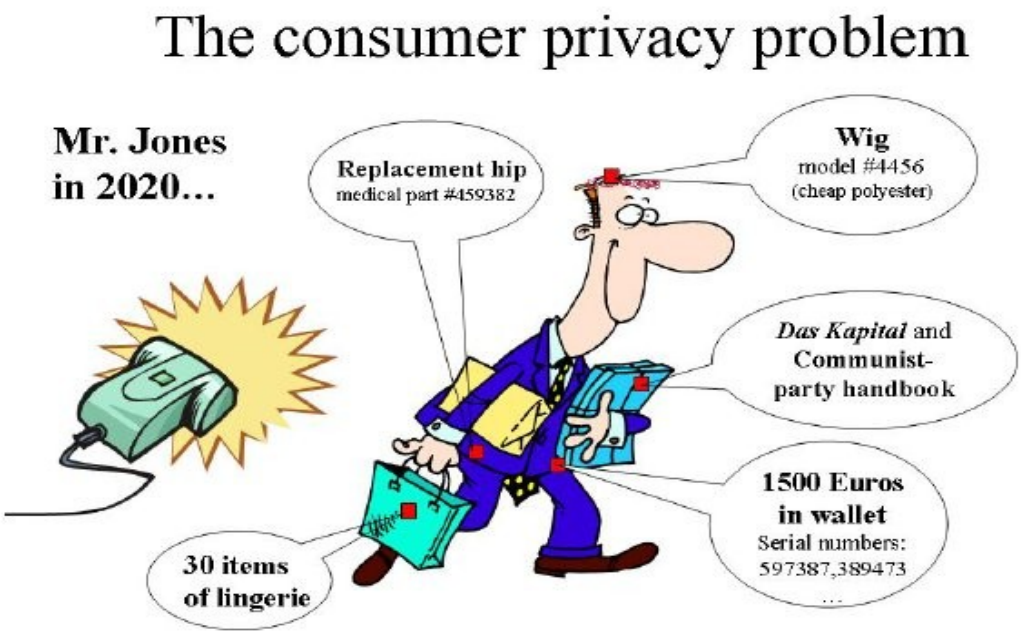


Illustration 1:Eksempler der viser hvorledes privatlivet er truet [RSALAB]

Der er adskillige andre trusler i forbindelse med RFID, nedenfor opremses nogle af dem:

• Eavesdropping • Cloning • Spoofing	• Tracking • DOS

Jeg vil nedenfor komme ind på nogle få af de problemer der kan forekomme i forbindelse med brugen af RFID i forskellige applikationer. Først vil jeg kort beskrive de to grundlæggende tag typer og derefter beskrive problemer ved brugen af disse til forskellige formål.

RFID-Tag typer

Grundlæggende findes de meget simple typer der ikke kan meget andet end at sende et serienummer, og de mere avancerede der kan lave kryptografiske operationer.

De simple typer tags der f.eks. benyttes på varer og lagre er også kendt som EPC-tags(Electronic Product Code tags). EPC er en standard defineret af EPCGlobal[1]. Desuden kan man på nogle tag skrive data en eller flere gange.

De mere avancerede typer er typisk lukkede systemer, hvor man holder kortene tæt til kroppen. Bl.a. kan nævnes Texas Instruments "Digital Signature Transponder", som dog har vis sig usikker idet forskere fra RSAlabs har fundet en måde at snyde systemet på. Dette er primært lykkedes på grund af et for dårligt implementeret symmetric key system, hvor man kun brugte en 40 bit nøgle. Dette medførte at det var muligt at knække systemet ved et bruteforce attack[2] .

RFID som adgangskontrol

Hvis man benytter RFID tags som adgangskontrol til bygninger eller biler er der flere ting som er vigtige at overveje grundigt. For det første skal man sikre sig at ingen kan klone ens tag, og derved skaffe sig adgang til bygningen eller bilen. Dernæst er der overvejelser i forbindelse med sporing af en persons bevægelser. Hvis tag'et svarer med det samme serienummer hver gang det bliver aktiveret, kan det lade sig gøre at spore den person der benytter det pågældende tag.

Med hensyn til at sikre sig mod kloning er der flere forskellige sikkerheds strategier man kan tage. Da der i forbindelse med tags til adgangskontrol er tale om et tag pr. person der skal have adgang, er det ikke økonomien der afgør om man benytter et tag til 50 øre eller et til 5 kroner , det giver derfor mening at benytte de dyre tags som også giver mulighed for kryptografi. Ved at benytte en symmetric key tag kan man gennemføre en simpel challenge-response protocol på flg. vis:

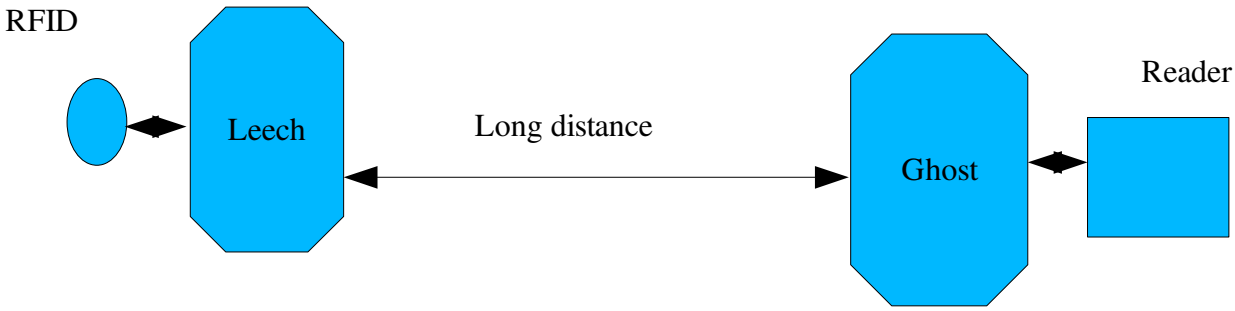
- Tag identificerer sig selv ved at sende T
- Læser genererer en nonce N og sender den til tag
- Tag beregner og svarer med $C = E_k(N)$
- Læser checker at C virkelig er lig med $E_k(N)$.

Da RFID-læseren ved hvilken key der er tilknyttet tag med serienummer T, kan den nemt tjekke om det er det rigtige tag der har svaret. Dette er en sikker metode for RFID-læseren at identificere og autentificere det tag der bliver talt med. Med denne form for tags er det altså ikke umiddelbart muligt at klone et tag, derimod er der stadig problemer med sporing af personer idet tag'et altid sender T. Dette kan dog løses på mange forskellige måder, hvor en af dem kunne være at tag'et fik ny T tildelt hver gang den har talt med en gyldig RFID-læser.

1 EPCGlobal is the organisation entrusted by industry to establish and support the EPCglobal Network™

2 http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/pdfs/DSTbreak.pdf

Ovenstående er dog stadig sårbar overfor et man-in-the-middle-attack.



Tegning 1:Man in the middle attack

Ved bygnings adgangskontrol kan et sådan angreb foregå ved at en bandit(Leecher) placerer sig tæt på et offer med et RFID-adgangsbadge, dette kunne f.eks. være i toget. Leecheren er i besiddelse af en RFID-læser som er forbundet med en ghost-rfid. Denne ghost-rfid befinder sig ved indgangsdøren til bygningen. Ghost og Leech er i forbindelse med hinanden v.h.a. f.eks. en mobiltelefon. Når Leech taler med tag'et sender den blot svaret videre til Ghost der gensender til den rigtige RFID-læser. På samme måde sender Ghost den anden vej. På denne måde tror RFID-læseren altså at tag'et reelt befinder sig indenfor den rigtige afstand, og vil derfor åbne døren. Offeret har ingen anelse om at han netop har givet adgang til sin kontor bygning. Der er forskellige måder at takle problemet på, jeg vil dog ikke komme nærmere ind på dem her.

RFID i dagligvarebutikkerne

Vi kender alle fremtids visionen om hvordan vi handler ind om 10 år. Man putter ganske enkelt varerne i indkøbsvognen, og når man forlader butikken siger det blip og en scanner har registreret hvad man har købt og hvem der skal betale. Med RFID-tags på alle varer og et RFID-Kreditkort er dette faktisk allerede muligt.

Inden vi ser disse butikker er der dog nogle sikkerhedsmæssige ting der skal på plads. Desuden må man også spørge sig selv om hvad prisen på et tag skal være, før det kan betale sig at udstyre f.eks. en 2 kroners vare med en RFID-tag. med den nuværende pris på ca. 50 øre er der jo nok et stykke vej endnu. Dette skal dog ikke forhindre os i at se på de sikkerhedsmæssige aspekter i denne forbindelse.

Først og fremmest er der problemet med at andre folk med en scanner har mulighed for at se hvad vi har i indkøbsposen. Denne trussel kan dog undgås på flere forskellige måder, hvor en af de enkleste er at tag'et ganske enkelt bliver ødelagt(slået ihjel) idet vi forlader butikken. Problemet med dette er at tag'et jo så heller ikke virker når vi kommer hjem og placerer mælken i vores RFID-køleskab, og det var jo ikke meningen. Vi ønsker altså at benytte tag'et i butikken, og når vi kommer hjem, men ikke når vi går på gaden med bæreposen. Løsningen til dette er en ”spærre tag” som spærrer for læsningen af tags i nærheden, denne tag placeres i bæreposen og gør altså at varerne i posen ikke kan scannes.

For de ovenstående forslag er det nemt at se at de kan benyttes af forbrydere til at stjæle varer i butikker. Forbryderen kan jo bare placere en ”spærre tag” i nærheden af de varer han ikke ønsker at betale for. Måden hvorpå dette kan undgås er ved hjælp af PIN-koder. For at et tag kan spærres af

”spærre tag'et”, skal det først sættes i ”spærret tilstand”, og for at kunne gøre dette skal man kende en PIN-kode. Denne PIN-kode kender butikken naturligvis, men ingen andre.

Et andet problem i forbindelse med RFID-tags på alle varer i butikken, er muligheden for konkurrenter der kan følge med i omsætningen i butikken. De kan ganske enkelt gå igennem butikken med en RFID-læser og lave en optælling af hvilke varer der er i butikken, og på den måde finde ud af hvad der bliver omsat.

Fremtiden for RFID

Der er ingen tvivl om at vi fremover vil se RFID teknologien blive brugt i flere og flere applikationer. Dette medfører en øget risiko for DOS angreb på systemerne, dette kan ske ved at personer med skumle bagtanker jammer radio signalerne med en kraftig sender.

Det kan for nogle personer være svært at se truslen i at enhver kan se hvad du har i bæreposen, for hvad kan man dog bruge denne viden til?. Men hvis disse data kan knyttes til data fra f.eks. et kreditkort i pungen, så er de færreste vel i tvivl om at det måske er lidt farligt.

Når vi taler om sporing af folks bevægelser vil mange også mene at det ikke værre end den måde vi allerede i dag kan spore folk ved hjælp af deres mobiltelefoner. Men den store forskel her er at det er muligt at slukke en mobiltelefon, dette er ikke muligt med en RFID-tag. Og endnu værre er det hvis du f.eks. bærer tag'et uden at vide det.

Jeg har i ovenstående kun beskrevet nogle få af de sikkerhedsproblemer der er med RFID-tags, og der vil helt sikkert dukke flere op når RFID bliver mere udbredt. Det er derfor vigtigt at man er opmærksom på problemerne omkring RFID-systemer.

Bilag

Litteraturfortegnelse

- Ari Juels, RSA Laboratories: ”RFID Security and Privacy: A Research Survey”
- RSAlabs page on rfid: http://www.rsasecurity.com/rsalabs/node.asp?id=2115
- Wikipedia: http://en.wikipedia.org/wiki/Rfid
- Stephen August Weis: “Security and Privacy in Radio-Frequency Identification Devices”
- http://www.rfidjournal.com/
- http://www.epcglobalinc.org
- http://tekno.dk/subpage.php3?article=1212&language=dk&category=7&toppic=kategori7