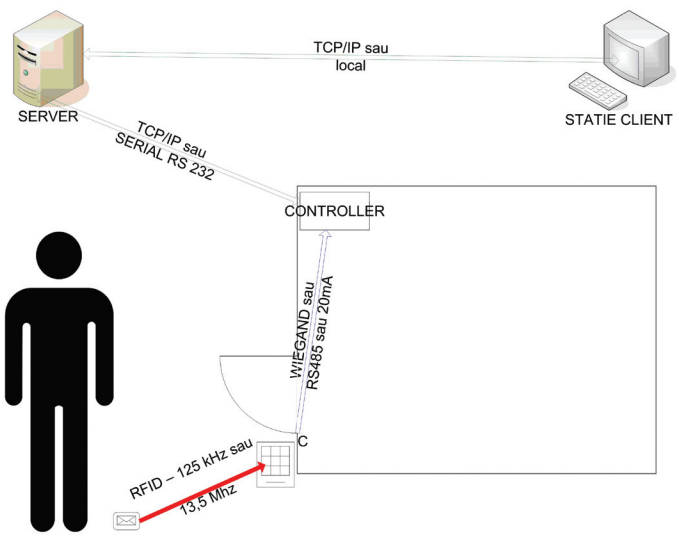
SOLUŢII DE SECURIZARE A CARDURILOR DE CONTROL ACCES

Ing. Vlad Crăciunescu - Director Vânzări SIEL INVEST SRL

Sistemele de control acces sunt folosite pentru a permite accesul persoanelor în spaţiile protejate conform unor reguli stabilite iniţial. Pentru identificarea persoanelor se folosesc mai multe tehnologii, dintre care de departe cea mai întâlnită, şi la care facem referire în cele ce urmează, este cea cu cartele de proximitate RFID.

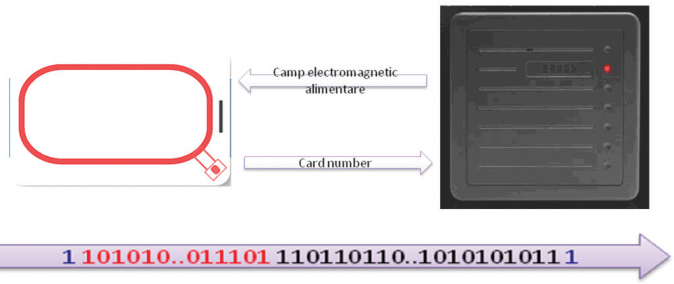
În cazul utilizării cartelelor de proximitate, pe cartelă este stocat un număr care identifică respectiva persoană în sistem. Toate deciziile se iau apoi pornind de la acel număr. Când ne gândim la securitatea sistemului de acces, ignorând forţarea fizică a accesului (care intră în sfera sistemelor de efracţie mai mult) , ne gândim la securitatea stocării acestui număr pe card când nu este folosit şi securitatea comunicării acestui număr de pe card, prin cititor şi controller până la baza de date centrală, aşa cum este arătat şi în diagrama de mai jos.



Se poate uşor vedea că cea mai expusă comunicaţie este cea între cartela şi cititor. Aceasta are loc în spaţiu neprotejat, nu necesită contactul fizic şi este iniţiată de cititor nefiind nevoie de intervenţia/aprobarea posesorului. Orice atacator poate să "asculte" comunicaţia între card şi cititor şi să o înregistreze sau pur şi simplu să îşi creeze un alt card care să transmită aceleaşi informaţii.

Cea mai utilizată tehnologie RFID în acest moment este proximitatea clasică ce funcţionează pe frecvenţa de 125 kHz . Deşi există mai multe variante de implementare, specifice fiecărui producator în principiu modul de funcţionare al acestor cititoare/cartele poate fi descris de schema ce urmează.

Iniţial numărul care identifică fiecare cartelă era limitat la gama de nr exprimabile prin 24 biti în format binar (26 biti din care 2 de paritate). Asta coresFigure_1



pundea unui site code în gama 0-255 (care identifică instalaţia/clientul) şi un card number în gama 0-65536 care identifica utilizatorul individual. Acest format a fost denumit Wiegand 26 biti (W26) si este formatul "standard" pentru sisteme de control acces. În acest moment , când în circulaţie sunt multe milioane de astfel de cartele, practic acest format nu asigură nici un fel de grad de siguranţă. Evident numerele se repeta şi, mai mult decât atât, nu există un control al celor care emit aceste carduri.

Atunci când aceste temeri au început să devină justificate, s-au dezvoltat mai multe soluţii care să crească nivelul de siguranţă :

- o primă soluţie a fost crearea altor formate care să codifice nr. cardului în binar. Una din variantele foarte folosite şi în curent este formatul pe 37 biţi , cu sau fără site code, care este creat şi administrat exclusiv de HID, unul din cei mai mari jucători de pe piaţă;
- o altă soluţie a fost adăugarea unui cod care diferenţiază instalatorii/beneficiarii şi care trebuie să fie acelaşi pe card şi pe cititor pentru ca comunicaţia să aibă loc. O variantă a acestei soluţii includea şi o amestecare a card number-ului într-un şir de nr. binare şi extragerea lui de acolo pe baza codului;
- cea mai frecventă soluţie adoptată de marii furnizori a fost pur şi simplu codificarea pe un nr cât mai mare de biti a card number-ului şi garantarea către beneficiar şi către instalatori că numerele emise către ei nu vor fi emise şi către alţii.

Toate aceste soluţii au crescut puţin securitatea dar prezintă în continuare un mare risc ce poate fi exploatat : comunicaţia poate fi în continuare "ascultată" de către cineva, înregistrată şi retransmisă. Cititorul nu are cum să discrimineze între un card valid şi orice alt dispozitiv care emite către el respectiva informaţie.

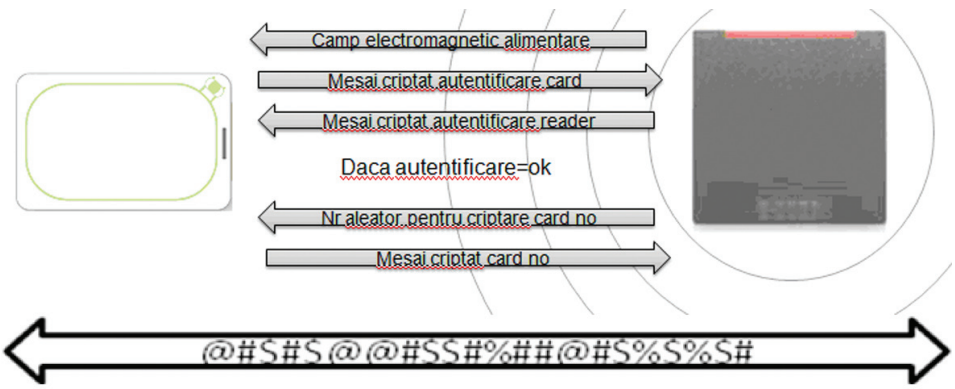
Soluţia inteligentă pentru aceste probleme de securitate nu a întârziat să apară. Ea se concretizează în apariţia de la mai mulţi furnizori a unor aşa numite contactless smart card. În fapt acestea sunt nişte carduri de proximitate inteligente care funcţionează în banda de frecvenţă de 13,56 Mhz. Comparate cu cardurile de proximitate "clasică" aceste carduri au mult mai multe funcţii :

- în primul rând au o memorie care poate varia

între 2k şi 32 k sau alte variante de la diverşi furnizori;

- în acea memorie pot fi stocate , în afară de card-number-ul pentru acces, alte date cum ar fi : PIN-ul, profile BIO dar şi informaţii pentru alte aplicaţii ca de exemplu cashless payment, abonamente etc;
- pe aceste carduri se poate şi scrie informaţie (în câmpurile disponibile) de către "cititor" permiţând aplicaţii diverse;
- toate comunicaţiile între cititor şi card sunt criptate cu un certificat digital.

Aceasta ultimă diferenţă este cea mai importantă în cadrul problemei în discuţie: în practică, între cititor şi card are loc un proces de autentificare reciprocă înainte ca orice informaţii să fie transmise. În plus, odată autenficate cele două componente, se stabileşte o "cheie ", unică pentru acea sesiune de comunicaţie, cu care se criptează toate informaţiile ce sunt transmise de pe card pe cititor şi invers. În acest mod se asigură un grad mult mai mare de securitate pentru întregul sistem decât în cazul cardurilor de proximitate clasică. Practic, chiar dacă cineva ar reuşi să comunice cu cardul sau să "asculte" comunicaţia acestuia cu cititorul, informaţiile ar fi criptate şi în plus cheia de criptare se bazează pe nişte nr aleatoare generate de card şi cititor şi care nu se repetă la următoarea comunicaţie.



Şi în această tehnologie există mai multe metode de implementare care realizează echilibrul între dificultatea de gestionare şi gradul de securitate :

- cea mai simplă formă de utilizare a cardurilor contactless smart card este aceea de a folosi CSN, card serial number. Acesta este un nr alocat de producător fiecarui card . El este presupus a fi unic, dar nu a fost creat pentru a fi folosit ca atare şi nu asigură nici un fel de securitate suplimentară faţă de cardurile de proximitate cu nr unic garantat de furnizor. Acest număr se trimite necriptat şi are doar rol în mecanismul anticolisiune.
- varianta standard de folosire implică folosirea aceluiaşi certificat digital pe toate cititoarele şi cardurile. Asta înseamnă că orice cititor va comunica cu orice card, dar informaţia va fi în continuare criptată. În acest caz se asigură un grad minim de securitate în sensul că, între cititor şi card comunicaţia nu poate fi "ascultată". Totuşi, dacă cineva cumpăra un cititor, poate să citească acel card şi să primească pe ieşirea Wiegand numărul cardului ceea ce este în continuare un risc inacceptabil.
- varianta "High Security" , pentru care au şi fost create aceste carduri, este accea în care pe card şi pe cititor se încarcă un certificat digital personalizat. În acest mod numai cititoarele şi numai cardurile cu acel certificat vor comunica. Dacă este un alt certificat pe card, de exemplu cel standard, cititorul nu va citi nimic de pe acel card. În acest caz, securitatea sistemului de control acces depinde de securitatea acelui certificat. Dacă el este stocat securizat, nimeni din exterior nu va putea să comunice cu acele carduri şi cititoare fără foarte mult efort informatic. Certificatul în discuţie poate să asigure seturi de cititoare/carduri personalizate pentru un distribuitor, pentru fiecare instalator sau pentru fiecare beneficiar. Posesorul acelui certificat este singurul care poate face carduri sau cititoare care să comunice cu celelalte. De reţinut că în acest caz se folosesc aceleaşi carduri şi cititoare ca în varianta standard, dar pe ele se instalează un nou certificat digital specific acelei instalări.

Algoritmii de criptare folosiţi în aceste comunicaţii sunt cei larg utilizaţi în mediul IT (DES, 3DES şi AES) şi asigură un grad de securitate satisfacator pentru situaţia actuală. În plus pe card şi pe cititor se află câte un generator de numere aleatoare care asigură ca la fiecare comunicaţie se foloseşte o altă cheie (diversificată din certificat, numerele aleatoare şi alte informaţii) care nu se va repeta. În plus, funcţie de gradul de securitate dorit, beneficiarul/instalatorul poate alege să schimbe certificatul de pe carduri şi cititoare în mod regulat, eliminând astfel şi riscul folosirii de carduri piedute sau alte breşe.

Dacă ar fi să comparăm sistemele de acces bazate pe carduri de proximitate cu un sistem de identificare cu parole, între doi oameni, atunci proximitatea clasică ar însemna strigarea parolei de la un capat la altul al unui coridor iar varianta cu contactless smart card ar presupune comunicarea parolei la ureche, cu toate literele rearanjate într-un mod cunoscut numai de cei doi şi care se schimbă de fiecare dată.

Având în vedere că costurile componentelor pentru un sistem de control acces bazat pe carduri contactless smartcard nu sunt mult mai mari decât costurile componentelor prox (în unele cazuri sunt chiar mai mici), considerăm că este oportună tranziţia la acest sistem, care asigură un grad de securitate mult mai mare şi în plus un număr de alte aplicaţii care pot folosi acelaşi card.