

به نام خدا

## **امنیت کارتهای اعتباری وایرلس (RFID)**

شاید در دنیای امروز کمتر کسی برای وارد نمودن مشخصات خود، ورود و خروج و اعتبار سنجی از کارتهای اعتباری استفاده ننماید و تقریباً جزئی فنا نا پذیر در زندگی بشر امروز شده است و همه از بزرگ و کوچک استفاده ان را بلدند .

از جمله این کارتها که روزمره از ان استفاده می کنیم کارت بدون تماس شرکت واحد می باشد، البته این طرح در شهرای کوچک مورد استفاده قرار ننگرفته است اما به زودی در همه جا اجرا خواهد شد

تاثیر ناپذیری  
موبایل روی کارت



روش کارت زدن  
موازی دستگاه



قابل استفاده از  
داخل کیف پول



## کارت بلیط اعتباری الکترونیکی اتوبوس



هنگام خرید و شارژ  
قبض دریافت نمایید



نگهداری کارت با  
سایر کارت ها



کارت نباید تا شود



عدم قرار گیری در  
حرارت شدید



کارت زدن نادرست



شاید باورش سخت باشد که این کارتها با این همه ادعای ارائه دهندگانشان مبنی بر امنیت و... بسیار ناامن در برابر هجوم هکرها می باشند

برای روشن شدن قضیه بهتر است کمی در باره عملکرد این کارتها بیشتر بدانیم

### روش کار کارتهای غیر تماسی RFID

RFID مخفف "شناسائی با استفاده از فرکانس رادیویی" می باشد. این تکنولوژی متشکل از آی سی های کوچک الکترونیکی و یک آنتن می باشد که ایسی مذکور قابلیت نگهداری 2000 بایت اطلاعات دارد. موارد استفاده کارتهای RFID مانند بارکد و یا نوارهای مغناطیسی موجود در پشت کارتهای بانک می باشد. اینگونه کارتها یک شماره شناسائی منحصر به فرد و غیر قابل تکرار را در اختیار شما قرار می دهند. و جهت شناسائی این کد، دقیقاً مانند دستگاه کارت خوان بارکد و یا کارت خوان مغناطیسی باید کارت توسط دستگاه کارت خوان RFID خوانده شود.



یکی از ویژگیهای منحصر بفرد دستگاههای RFID نسبت به سایر دستگاههای ذکر شده این است که نیازی نیست که دستگاه کارت خوان دقیقاً و با طبق قوانینی خواص در کنار کارت قرار گیرد و قادر است کارت را از فواصل متفاوت شناسائی کند (بسته به نوع کارت و دستگاه انتخاب شده). همه ما با مشکلات یک فروشنده فروشگاه که از سیستم بارکد استفاده می کند آشنا هستیم. و همینطور در مورد کارتهای اعتباری و کارتهای بانکی که حتماً باید در یک جهت خاص و با یک شیوه خاص کارت کشیده شود.

در کل سیستمهای RFID قادر به شناسائی کارت از چند سانتیمتری می باشند (حد اکثر 6 متر برای کارتهای فرکانس بالا و برای کارتهای معمولی کمتر از 10 سانتیمتر) به عنوان مثال شما می توانید کلیه کالاهای خریداری شده را در یک کیسه قرار داده و همه را به یکباره بر روی دستگاه کارت خوان قرار دهید. و دستگاه قادر است کلیه کارتهای RFID را شناسائی و قیمت کل را محاسبه نماید.

تکنولوژی RFID از 50 سال پیش بوجود آمده است ولی اخیراً ویژگیهای آن در کنترل انبار و ردیابی و... مورد توجه قرار گرفته است شرکت آلین تکنولوژی اخیراً 500 میلیون تک را به فروش رسانده است یکی از دلایلی که باعث شد RFID دیرتر مورد استفاده عموم قرار گیرد فقدان استاندارد در این زمینه بوده است. شرکت های زیادی تنها جهت ردیابی کالاهای خود در این زمینه سرمایه گذاری کردند. یکی از بزرگترین ویژگیهای RFID زمانی مشخص می شود که ردیابی کالا از یک کارخانه به کارخانه ای دیگر و یا از یک کشور به کشوری دیگر انجام می شود.

حال می دانیم که این کارتها چگونه کار می کنند و این را هم مطلعیم که می شود این کارتها را از راه دور خواند، به نظر شما نمی شود این کارتها را کپی کرد و از اطلاعاتش استفاده کرد؟؟؟

ایا نمی شود از اعتبار کارتی استفاده کرد؟؟؟؟

البته که می شود کفایت هکر دستگاهی را طراحی نماید و کنار شخصی که کارت اعتباری دارد بنشیند یا حتی بگذرد و دستگاه او تمام اطلاعات کارت مورد نظر را به سرقت می برد و هکر میتواند به نفع خود از آن استفاده نماید

لازم به ذکر است که طراحی این دستگاهها کار بسیار آسانی است و دزدین اطلاعات کارت نیز و کپی روی کارت دیگر یا حتی شبیه سازی کارت با میکرو کنترلر ها به راحتی امکان پذیر می باشد چون کارتها هیچ گونه الگوریتم رمز نگاری شده ای ندارند

اگر هم الگوریتم رمز نگاری داشتن هیچ فرقی برای هکر نداشت

این مثال را ما برای کارتهای اعتباری بلیت (کارت بلیت) زدیم و فکر نکنید تنها هک مختص به این کارتها می باشد در بعضی از مکانها که دنبال امنیت می گردند مد شده که از این نمونه کارتها استفاده می کنند برای ورود و خروج پرسنل بی آنکه لحظه ای اندیشیده باشند که آیا نمی شود از این کارتها سوء استفاده کرد ???

کافیست هکر از کنار یکی از پرسنل عبور کند تا اطلاعات آن پرسنل را برای خود داشته باشد و از آن استفاده کند این شامل خودروهایی که دربهای آنها با تگ های اراف ای دی هم باز و قفل می گردد می شود

هکر تنها با دست دادن با شما می تواند اطلاعات سویچ شما را بدزد و در فرصت مناسب به ماشین شما نفوذ کند

شاید اگر بخواهیم در این باره بحث کنیم ساعتها برای نوشتن این مقاله وقت صرف شود اما همین گوشزد کافیست تا بدانیم که راحت تر از اب خوردن میتوان این کارتها را هک کرد و از آن سوء استفاده نمود

امین کیمیایی 1 شهریور ماه 1392

انبردست .ای ار

Anbordast.ir

Iranled.com