دوشنبه 03 مهر 1391 - 07:02

نيمه تاريك فناوري

از دستگاه خودپرداز (ATM) كه براي پرداخت و دريافت پول است تا سيستم مسيرياب جهاني(GPS)، فناوري يك نيمه تاريك هم دارد. اشكال مختلف از اين نيمه‌هاي تاريك فناوري مي‌تواند عواقب ترسناكي داشته باشد.

جام جم آنلاين: از دستگاه خودپرداز (ATM) كه براي پرداخت و دريافت پول است تا سيستم مسيرياب جهاني(GPS)، فناوري يك نيمه تاريك هم دارد. اشكال مختلف از اين نيمه‌هاي تاريك فناوري مي‌تواند عواقب ترسناكي داشته باشد.
ما عادت كرده‌ايم هميشه نگران حمله ويروس‌ها يا هكرها به رايانه‌مان باشيم، اما امروزه نگراني اصلي تبديل شدن تلويزيون‌ها، خودروها، تلفن‌ها و لوازم خانگي به وسايل آسيب‌پذير است كه اين آسيب‌پذيري به واسطه استفاده ما از فناوري‌هايي مانند Wi-Fi، بلوتوث، RFID و GPS براي متصل‌كردن آنها به هم است.

اگرچه اين افزايش ارتباطات براي ايجاد راحتي و سهولت ارتباط سودمند است، اما اين افزايش موجب پديدارشدن وجه خطرناك اين فناوري‌ها شد. در حقيقت، استفاده از اين فناوري‌ها موجب شد تا چيزهاي بيشتري از دنياي واقعي در معرض هك‌شدن قرار بگيرد.

هكرها مي‌توانند قفل يك ماشين را باز و موتورش را روشن كنند يا بدون اين‌كه به كيف پولتان دست بزنند از كارت اعتباري‌تان سرقت كنند آن هم فقط با راه رفتن پشت سرتان. آنها مي‌توانند با آدم‌ربايان براي پيداكردن مكان‌يابي يك فرد همكاري كنند يا اطلاعات خصوصيتان را به دست آورند.

در اينجا به طور خلاصه به فناوري‌هايي كه مي‌تواند توسط افراد بد و مجرمان براي ضربه‌زدن به شما و هرچه در اطرافتان است مورد استفاده قرار بگيرند، اشاره مي‌كنيم.

خودپرداز بانك

اولين فناوري‌اي كه مي‌تواند نيمه تاريك داشته باشد دستگاه خودپرداز يا همان عابر بانك است كه روزانه از آن استفاده مي‌كنيد. براي نشان دادن نيمه تاريك اين فناوري ابتدا بايد بدانيم خودپرداز چگونه كار مي‌كند.

دستگاه خودپرداز مانند يك رايانه آنلاين است. وقتي شما كارت‌تان را وارد مي‌كنيد كارتخوان (Card Reader) محتويات آن را كه روي نوار مغناطيسي كارت ضبط شده مي‌خواند و به سرور مركزي مي‌فرستد.

بعد از آن از شما مي‌خواهد رمز كارت (PIN code) را وارد كنيد و بعد از بررسي و تائيد آن عمليات مورد نظرتان مثلا پرداخت پول را انجام مي‌دهد.

اطلاعات موجود در نوار مغناطيسي كارت اعتباري شما بدون پين كد كارت بي‌استفاده است و حتي پيچيده‌ترين و پيشرفته‌ترين خودپردازها هم نمي‌توانند پين كد را بازيابي كنند. اين پين كد در واقع نقطه ضعفي است كه مجرمان از آن سوءاستفاده مي‌كنند تا نيمه تاريك اين فناوري را بسازند.

مجرمان از پوشش پلاستيكي شفاف و پيشرفته‌اي استفاده مي‌كنند و آن را روي كليدهاي دستگاه خودپرداز قرار مي‌دهند تا رمز كارت يا همان پين كد قرباني را ضبط كند. با داشتن پين كد، سرقت كار آساني خواهد بود. مشكل اينجاست كه كشف خودپرداز و ضبط‌كننده پين كد قبل از سرقت از حساب بانكي كاربر، كار بسيار سختي خواهد بود.

جنگ پيامكي

عبارت جنگ پيامكي (war texting) در واقع به فرآيند ربودن سخت‌افزارهاي متصل به سيستم سراسري GSM (سيستم سراسري ارتباطات سيار ـ Global System for Mobile Communications) شبكه‌هاي تلفن همراه اشاره دارد.

دوربين‌هاي حفاظتي، سيستم‌هاي خودكار منازل و حتي خودروها وابسته به سيستم GSM براي به‌روزرساني ميان‌افزارهاي (تركيبي از نرم‌افزار و سخت‌افزار ـ firmware) خود هستند. اگرچه GSM براحتي اين سيستم‌ها را به‌روزرساني مي‌كند، اما آنها را نيز در برابر حملات خارجي آسيب‌پذير مي‌سازد.

سال گذشته در كنفرانس امنيتي بلك هت (Black Hat security conference) در لاس وگاس، مشاوران امنيتي iSec، دان بيلي (Don Bailey) و متيو سولنيك (Matthew Solnik) تهديد جنگ پيامكي را اثبات كردند. آنها قفل در يك خودروي سوبارو را باز و موتور آن را روشن كردند، البته همه اين كارها از راه دور بوده است.

بيلي مي‌گويد كشف چگونگي قطع ارتباط پيامي بي‌سيم بين خودرو و شبكه براي او و سولنيك حدود دو ساعت طول كشيده است و بعد از آن اين ارتباط پيامي را دوباره بين خودرو و لپ‌تاپ‌شان برقرار ساختند.

با اين حساب، داشتن خودروهاي گران‌قيمت با سيستم‌هاي هوشمند امنيتي به جاي ايجاد امنيت، تهديدي براي امنيت خواهند بود!

شناسايي با فركانس راديويي (RFID)

تراشه RFID يك دستگاه بسيار كوچك حاوي اطلاعات بوده كه به آن چسبانده شده است كه مي‌تواند يك كارت ID محتوي اطلاعات پزشكي شخصي، سوئيچ يك خودرو، قفل الكتريكي يك در و يك كارت اعتباري باشد.

هدف اوليه ساخت يك تراشه RFID جاسازي اطلاعات ديجيتال در يك وسيله غيرديجيتال بود تا به اين وسيله امكان ايجاد ارتباط و پيگيري يك شيء را آسان‌تر كند.
يكي از مزيت‌هاي تراشه‌ها اين است كه تقريبا تراشه‌هاي RFID حتي به باتري هم نياز ندارند و به صورت الكترومغناطيسي از دريافت‌كننده نزديكشان تغذيه مي‌شوند اما مشكل اينجاست كه هر وسيله‌اي كه داراي يك تراشه RFID است پتانسيل هك شدن را دارد (با تراشه‌هايي كم قيمتي حدود 0.07 دلار مي‌توان اين كار را انجام داد.)

اين در حالي است كه اين تراشه‌ها هر روز روي وسايل بيشتري نصب مي‌شوند.

اوايل امسال در كنفرانس ShmooCon hacker-centric security، پژوهشگر امنيتي كريستين پاگت (Kirstin Paget) نشان داد چقدر راحت مي‌توان يك تراشه RFID مجهز به كارت اعتباري را هك كرد. براي اين كار به 350 دلار تجهيزات نياز است.

پاگت توانست به صورت بي‌سيم اطلاعات كارت اعتباري‌اش را كه در RFID موجود بود كپي و يك كارت جديد براي خود توليد كند سپس براحتي از طريق يك كارتخوان اسكور(Square card reader) از آن استفاده كند. در حقيقت، پاگت نشان داد هك‌كردن يك تراشه RFID به صورت خجالت‌آوري ساده است.

راحتي هك كردن اين فناوري، زنگ خطر براي كساني است كه از اين فناوري براي اطلاعات شخصي‌شان، قفل درها و ديگر موارد امنيت استفاده مي‌كنند.

سيستم مسيريابي جهاني (GPS)

سيستم مسيريابي جهاني (GPS) كه تلفن‌هاي هوشمند و بيشتر تلفن‌هاي همراه مجهز به آن هستند نيز از فناوري‌هايي است كه نيمه تاريك دارد.

توليدكنندگان برنامه‌ها از اين فناوري از طرق مختلف نه فقط براي پيداكردن مختصات طول و عرض جغرافيايي بلكه براي به دست آوردن اطلاعات شخصي افراد استفاده مي‌كنند.

براي مثال، برنامه‌هايي مانند FourSquare از GPS براي پيگيري عادات اجتماعي و عادات خريد و خرج كاربران خود استفاده مي‌كند.

شايد نگران‌كننده‌ترين جنبه اين فناوري اين است كه تحت قوانين موجود، دسترسي به اطلاعات شخصي افراد كه توسط برنامه‌هايي مانند FourSquare ايجاد مي‌شود براي كاربران اين برنامه‌ها قانوني است. ميزان خصوصي بودن اطلاعات جمع‌آوري شده چيزي است كه موجب افزايش نگراني‌ها درباره اين فناوري مي‌شود.

اين كه مجرمان بتوانند جاي افراد مختلف و اطلاعات شخصي‌شان را براحتي به دست آورند موضوعي نيست كه براحتي بتوان از آن گذشت.

كلام آخر

بسياري از اختراعات و فناوري‌هاي ساخته شده توسط انسان مانند شمشير دو لبه است كه مي‌توان از آنها هم در جهت خير و هم در جهت شر استفاده كرد. فناوري‌هايي كه در اينجا به صورت اجمالي به آنها اشاره شد نيز جزو همين دسته‌اند.

نيمه تاريك اين فناوري‌ها نبايد باعث شود افراد خود را از فوايد و مواهبي كه آن فناوري‌ها در اختيارشان مي‌گذارند، محروم كنند؛ بلكه افراد بايد تلاش كنند آنها را بخوبي بشناسند و خود را در برابر خطرات احتمالي‌شان ايمن سازند. (جام جم - ضميمه كليك)

مطهره وجيهي