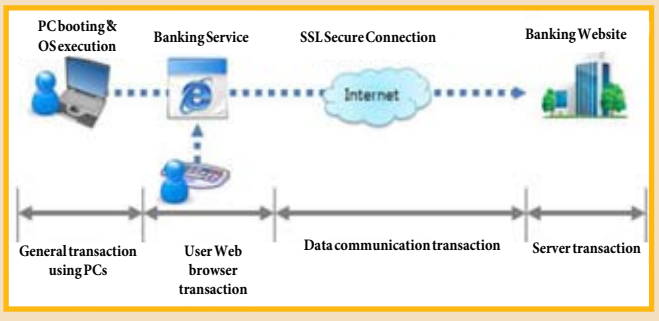
تهدیدها و ضد تهدیدها در بانکداری آنلاین

جواد مروی‌مقدم
مدیر سخت‌افزار و امنیت شبکه بانک حکمت ایرانیان

این مقاله شـــرح جامعی از انواع تهدیدهایی را ارائه می‌دهد که در فرایند یک دادوســـتد الکترونیکی از طریق رایانه پیـــش روی ما قرار دارند و بـــه ابزارها و فناوری‌هایی می‌پردازد که برای از کار انداختن تهدیدات به‌کار می‌آیند. بانکداری الکترونیکی مجموعه فرایندهایی است که طی آن، مشتری بانکی از طریق مرورگر وب نصب شده روی رایانه، وارد وبگاه بانک شده، مبادلات گوناگونی مثل انتقال وجه، دریافت موجودی و... انجام می‌دهد. بانکداری الکترونیکی در چهار مرحلهٔ اصلی توضیح داده می‌شود. (شکل شماره ۱)

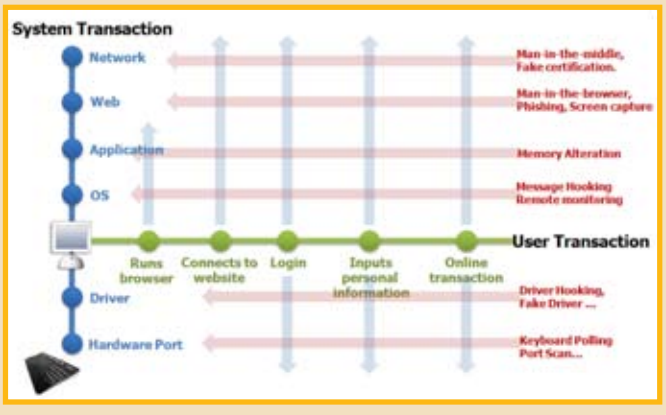


شکل شماره ۱- مراحل تراکنش‌های بانکداری الکترونیکی

۱. کاربر رایانه را روشن و سیستم عامل را بارگذاری می‌کند.
۲. پس از اینکه مرورگر وب باز شـــد، کاربر وارد وبگاه بانک شده و رمز را با استفاده از صفحه کلید وارد می‌کند.
۳. داده‌های ورودی توســـط SSL (Secure Socket layer) رمزنگاری و به سرور بانک منتقل می‌شود.
٤. سرور بانک، ضمن رمزگشایی اطلاعات وارده، اعتبار کاربر را بررسی و در صورت صحت اطلاعات وارد شده، استعلام حساب، انتقال وجه و... را بررسی می‌کند.

تهدیدهای چند جانبه

محیط رایانه در حالت عادی (به دلیل ناامن بودن وب و نصب یا اســـتفاده از انواع برنامه‌های بازبینی نشده) در معرض تهدیدهای بسیار گوناگونی قرار دارد. اگر کاربری یک معامله بانکداری الکترونیکـــی را در محیطی انجام دهد که در معرض تهدیدهای گوناگون قرار دارد، هیچ ضمانتـــی برای صحت این معامله وجود نخواهد داشت. در محیط اینترنت ابزارها و نرم‌افزارهای هک کنندهٔ جدید، که در رایانهٔ کاربر نصب و اجرا می‌شوند، به وفور پیدا می‌شود. در حالی که کاربر با آسودگی در وب می‌چرخد و ای‌میل‌ها را باز می‌کند، این ابزارهای هک می‌توانند به آســـانی کلمهٔ عبور فرد، شماره حساب و اطلاعات شـــخصی کاربر را ذخیره کنند. علاوه بر این، هکرها هم‌چنین قادرنـــد صفحه وبگاه اصلی بانک را با یک



شکل شماره ۲- در هر مرحله از تراکنش ممکن است با تهدیدهایی روبه‌رو باشیم

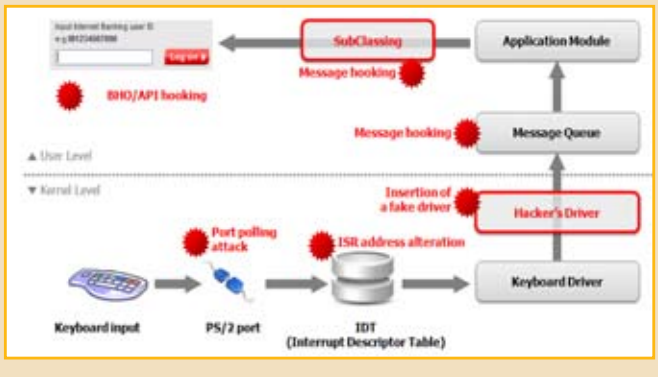
صفحه جعلی، که کاملاً شبیه صفحه اصلی است، جایگزین کنند. این صفحه‌های جعلی را هکرها برای دزدیدن اطلاعات حساب کاربر طراحی می‌کنند. در چنین وضعیتی اطلاعات ورودی کاربر به بانک منتقل نمی‌شود؛ چرا که هکرها این اطلاعات را برای انتقال وجه به‌صورت غیرقانونی، به سرور هک کننده جهت‌دهی می‌کنند. بنابراین هکرها و ابزارهای هک کننده می‌توانند با استفاده از حفره‌های بسیار زیادی طی فرایند بانکداری الکترونیکی به ما حمله کنند. (شکل شماره ۲)

اینترنت و نسل جدید مخرب‌ها

هرچند برنامه‌های آنتی‌ویروس و ضد بدافزار برای حفاظت در برابر تهدیدها بر روی رایانه نصب می‌شوند، اما این برنامه‌ها قادر به مقابله با افزایش نسل‌های جدید کدهای مخرب که در شکل شماره ۳ نشان داده شده، نیستند. زیرا فناوری ضد بدافزار طوری طراحی شده که فقط تهدیدات آشنا و شناخته شده را می‌تواند شناسایی کند. برای مثال، یکی از ابزارهای هک کنندهٔ بانکداری الکترونیکی، Zenus نام دارد و شامل این فناوری است که نرم‌افزارهای ضد بدافزار را شناسایی و از آن‌ها دوری می‌کنند و به‌طور مداوم نسل‌های جدید یا انواع Zenusها را در سراسر وبگاه‌ها منتشر می‌کنند.

تهدید به اطلاعات شخصی وارد شده

کاربر به سرویس بانکداری الکترونیکی وارد می‌شود و نام کاربری و کلمهٔ عبور خود را وارد می‌کند. وقتی کاربر صفحه کلید را فشار می‌دهد، سیگنال‌های ورودی از طریق پورت متصل به صفحه کلید به تعدادی از وسایل دیگر منتقل می‌شود. به عبارت دیگر، پروسهٔ ورود به وبگاه بانکداری الکترونیکی، شامل اطلاعات شخصی واردشده از طریق ضربات صفحه کلید می‌شود، اطلاعات ورودی را روی صفحه نشان می‌دهد و با کلیک کردن بر روی دکمه log in یا submit آن‌ها را انتقال می‌دهد. شکل شماره ۳ حمله‌های احتمالی‌ای را نشان می‌دهد که ابزارهای هک کننده طی این پروسه انجام می‌دهند.

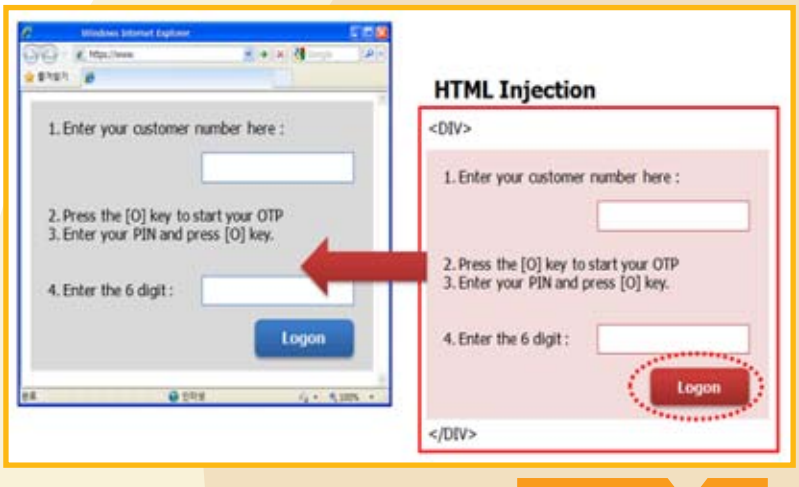


شکل شماره ۳- تراکنش ورودی صفحه کلید و تهدیدهای وابسته به آن

تکنیک هک کردن key logging که قبلاً به سطح کاربر محدود شده بود، از سال ۲۰۰۶ به بعد به همهٔ مراحل کل پروسه و از جمله سطوح بنیادین آن نیز گسترش یافته است. اخیراً روش‌های polling و hooking در حملات در سطح پورت مکرراً مورد استفاده قرار می‌گیرند. شکل شماره ٤ دیاگرام type of keyboard/ps۲ را نشان می‌دهد، باید توجه داشت که حتی صفحه کلید USB یا صفحه کلید Bluetooth هم نسبت به این حملات آسیب‌پذیرند. اطلاعات حساب مسروقه در هر مرحله از کل پروسهٔ بانکداری الکترونیکی از طریق FTP همراه با تصویر صفحه که ضبط شده به سرور هکر منتقل می‌شود.

تهدید به مرورگر وب

حمله‌های MITB (Man in the browser) کاربر انتهایی را به سایت‌های جعلی با نیت سرقت اطلاعات وی، هدایت می‌کنند. اکثر بانک‌ها کلمه عبور یک‌بار مصرف OTP (One Time Password) را برای حفاظت کلمهٔ عبوری که کاربر روی صفحه کلید وارد می‌کند، ارائه می‌دهند. این فناوری حملات را disable می‌کند؛ به این صورت که هر بار کاربر log in می‌شود OTP، یک کلمهٔ عبور جدید می‌سازد و به کاربر ارائه می‌کند. به‌طوری‌که هکر نمی‌تواند کلمه عبور ضبط شده توسط ابزار هک کنندهٔ Key logging را به کار گیرد؛ هر چند هکر می‌تواند عملکرد OTP را با یک حملهٔ ساده از کار بیندازد. با استفاده از ابزار هک کننده که ابتدا در رایانهٔ کاربر نصب می‌شود، هکر می‌تواند یک وبگاه بانکداری الکترونیکی جعلی را که با تغییر Host Fileهای کاربر ساخته است، به جای وبگاه اصلی بانک نشان دهد. هم‌چنین می‌تواند در جلسات بانکداری الکترونیکی کاربر نفوذ کرده با پوشش وبگاه کاربر از طریق تزریق کدهای HTML به یک وبگاه جعلی هدایت و با اطلاعات حساب کاربر پر کند.



شکل شماره ۴- وبگاه جعلی
از طریق تزریق کدهای HTML

در پایان، کاربر اطلاعات حساب یا اطلاعات مالی خود را بر روی وبگاه جعلی وارد می‌کند، اطلاعات به حساب جعلی و سپس به وبگاه بانک منتقل می‌شود. وقتی انتقال وجه غیرمجاز بر اساس درخواست هکر کامل شد، هکر حتی صفحه‌ای را نشان می‌دهد که بیان می‌کند که عملیات کاربر به‌طور موفقیت‌آمیز انجام شده است و کاربر قادر به درک ناصحیح بودن عملیات نخواهد بود.

حملات MITB انواع بسیاری دارد و هکر حتی می‌تواند مشتریان یک بانک خاص را هدف خود قرار دهد. حملات MITB می‌تواند با نگه‌داری یک جلسه نشست بانکی با استفاده از اطلاعات حساب و کلمه عبور که شامل OTPهایی که از رایانهٔ کاربر به سرقت رفته صورت پذیرد. هکرها می‌توانند به کاربر بانک،

ابزارهای هک تهدیدهای گوناگون

هکرها علاوه بر ذخیره کلمهٔ عبور و اطلاعات شخصی کاربر، قادرند یک صفحه جعلی، کاملاً شبیه صفحه اصلی را به جای صفحه وبگاه اصلی بانک بنشانند. در چنین وضعیتی اطلاعات ورودی کاربر به بانک منتقل نمی‌شود؛ چرا که هکرها این اطلاعات را برای انتقال وجه به‌صورت غیرقانونی، به سرور هک کننده جهت‌دهی می‌کنند

یک صفحه با پیغام خطا و آخرین OTP که در صفحهٔ بانکداری الکترونیکی وارد کرده، نشان دهند و بدین ترتیب هکر می‌تواند عملیات انتقال غیرقانونی را تکمیل کند. این تروجان‌های چند جانبهٔ بانکداری الکترونیکی می‌توانند ضررهای مالی زیادی را به کاربران بانک تحمیل کنند؛ گاهی این ضررها به اندازه‌ای سنگین‌اند که سبب ورشکستگی مؤسسه‌های هدف می‌شوند.

تهدیدات مربوط به ارتباط SSL

همراه با پیشرفت در اینترنت بی‌سیم، امروزه با استفاده از اینترنت در کافی شاپ‌ها یا فروشگاه‌ها، خرید آنلاین در شبکه میسر می‌شود. البته، تقریباً تمام وبگاه‌های بانکداری الکترونیکی از ارتباطات SSL (SSL Man-in-the-middle) رمزنگاری شده (۱۲۸ بیت یا بیش‌تر) برای تأمین امنیت مرورگران وب استفاده می‌کنند و آن‌ها را در برابر حملات MITM توسط Sniffing ایمن می‌سازند. اگر چه مشکل می‌توان قاطع و صریح گفت که ارتباط SSL می‌تواند امنیت را در محیط اینترنت (Wireless (Wi-Fi تضمین کند.

شکل شماره ۵- جلسهٔ ارتباطی امن از طریق SSL

یک حملهٔ SSL MITM از طریق Wi-Fi می‌تواند به‌صورت زیر پیشرفت کند:

۱.کاربر انتهایی از طریق Wi-Fi به بانکداری الکترونیکی وارد می‌شود؛

۲.هکر به همان شبکه Wi-Fi متصل شده و حملهٔ SSL MITM را از طریق کلاه‌برداری(ARP (Address Resolution Protocol و DNS (Domain name system) آغاز می‌کند؛

۳.هکر یک وبگاه جعلی بانکداری الکترونیکی و یک گواهی جعلی به کاربر ارائه می‌دهد؛

٤.مرورگر وب به یک نشست متصل شده با این سؤال روبه‌رو می‌شود که آیا گواهی ایمن و غیرجعلی است یا خیر؟ اگر پاسخ منفی باشد، پیام اخطار در

شکل شماره ۶: پیغام امنیتی برای مرورگر وب

شکل شماره ٦ نشان داده می‌شود. هر چند به‌دلیل اینکه اکثر کاربران دانش کافی در مورد این نوع هک کردن ندارند، گزینه «yes» را برحسب عادت بدون فکر انتخاب می‌کنند. به عبارت دیگر، مجرمان از لحاظ اجتماعی پیغام‌ها را طوری طراحی می‌کنند که کاربر یک گواهی غیر طبیعی را که به‌طور رمزی ایجاد شده قبول کند؛

۵.اگر ارتباط SSL توسط عملیات رمزنگاری ۱۲۸ Bit انجام شود، هکر بستهٔ SSL را با یک ابزار شنود هک می‌کند، مانند Etherous؛

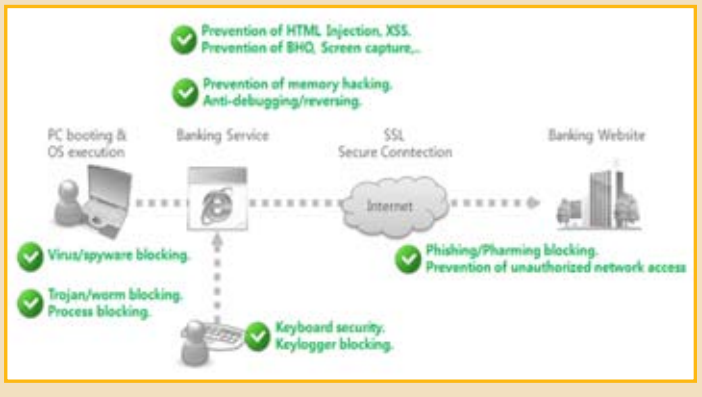
٦.هکر از یک گواهی جعلی و یک نسخهٔ SSL برای رمزگشایی کدهای سرقت شده استفاده کرده و اطلاعات مالی و حساب کاربر را به‌دست می‌آورد.

۷.هکر اکنون به یک وبگاه بانکداری الکترونیکی معتبر وصل شده و انتقال غیرقانونی وجه را انجام می‌دهد.

شکل شماره ۷- SSL Man-in-the-middle

اقدامات متقابل

بانکداری الکترونیکی از طریق یک سری معاملات در محیط‌های متنوع بین کاربر انتهایی و سامانه انجام می‌شود و این معاملات همیشه نسبت به حملات چند جانبه از سوی هکرها آسیب‌پذیر هستند. در تحلیل نهایی، یک راه حل فنی خاص نمی‌تواند اقدامات متقابلی را فراهم کند که تمام حملات هکرها را از کار بیندازد. ما باید کاربران نهایی بانکداری الکترونیکی را با راه حل امنیتی چند جانبه محافظت کنیم. راه حلی که تمام مسیرهای هک کردن را فهمیده و تمام فناوری‌هایی که امنیت را برای اطلاعات ورودی کاربر، بر روی مرورگر وب و برای شبکهٔ مورد استفاده فراهم می‌آورند، ارائه کنند. (شکل شماره ۸)

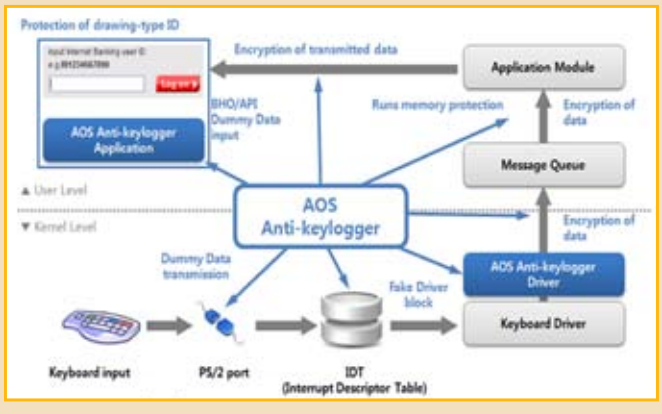


شکل شماره ۸: فناوری‌های امنیتی برای حفاظت از تراکنش‌های بانکداری الکترونیکی در مراحل گوناگون

فناوری Anti-Keylogging

برای حفاظت اطلاعات ورودی از طریق صفحه کلید، هر بخش از کل سامانه باید حفاظت شوند. همان‌طور که در شکل شماره ۹ نشان داده شده است، شروع از صفحه کلید کاربر بوده است که در حافظهٔ مرورگر وب ضبط شده و در نهایت

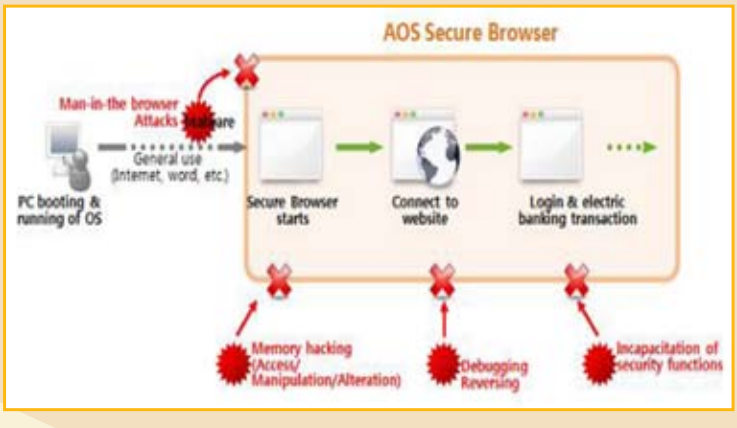
در صفحه، نمایش داده می‌شود. برای امنیت صفحه کلید، راه حل پیشنهادی باید قادر باشد هر چیزی را شناسایی کند؛ نه تنها در سطح هستهٔ اصلی (Kernel) بلکه در Key logging کاربر نیز باید این توانایی وجود داشته باشد. در سطح هسته‌ای (Kernel)، امکان حفاظت از اطلاعات ورودی صفحه کلید تنها وقتی میسر است که این داده‌های ورودی از پورت به IDT (Integrated Digital Technologies) و از پورت به راه‌انداز (Driver) به‌صورت رمزنگاری شده باشند. در سطح کاربر سد کردن غیرمجاز (hooking) باید در هر مرحله از فرایند شناسایی شده و حافظه (Memory) باید محافظت شود. به اضافه، یک فناوری پیچیده و ماهرانه باید به کار رود تا وقتی که هکر بخواهد اطلاعات صفحه کلید کاربر را از طریق BHO یا رابط برنامهٔ کاربردی (API) ضبط کند، یک سری اطلاعات ساختگی و زائد را نشان دهد، که این اطلاعات بی‌معنی خواهند بود. (شکل شماره ۹)



شکل شماره ۹- محافظت از داده‌های ورودی که از طریق صفحه کلید وارد می‌شود در برابر key-loggerها

فناوری امنیت در مرورگر وب

مرورگر وب که مورد هدف اکثر حمله‌ها است، محدودیت‌های ساختاری بسیاری را دربرمی‌گیرد. همانند یک پردازشگر اشتراکی، مرورگر وب در محافظت از حافظه‌اش و در کنترل کردن ماژول‌های آتی که از خارج اعمال می‌شوند محدودیت دارد. نقاط کور در امنیت مرورگر وب برای عموم با هک کردن به‌صورت مهندسی معکوس (reverse engineering hackers) باز شده و حمله Zero-day ممکن می‌شود. هم‌چنین نقص‌های ساختاری در برابر حملات MITB در مرورگر وب وجود دارد؛ مثل تحریف شدن با صفحهٔ وب توسط پروسه‌های BHO و پردازشگر خارجی. (شکل شماره ۱۰)



شکل شماره ۱۰- مرورگر امن در برابر انواع حمله‌ها مانند MITB و...

جهت امنیت بانکداری الکترونیکی، ما نیاز به یک فناوری مرورگر داریم که بتواند این ضعف‌ها را حل کند. با این فناوری، مرورگر باید قادر باشد از خودش در برابر اشکال‌زدایی و مهندسی معکوس توسط هکرها محافظت کرده و هر تلاشی برای دسترسی و دخالت در حافظه خود را مسدود کند. به‌علاوه، فناوری جدید مرورگر وب باید قادر به مسدود کردن حمله‌های Component object Model (COM hooking) و XSS و هم‌چنین محافظت در برابر ضبط کردن کلمهٔ عبور باشد. در پایان، فناوری جدید مرورگر وب باید بتواند راه را بر حمله‌های Pharming و Phishing ببندد، حمله‌هایی که توسط فایل‌های هاست دروغین و یا DNS به انجام می‌رسند.

فناوری امنیت شبکه و جلوگیری از هک شدن

ما نیاز به یک فناوری امنیتی داریم که تهدیدهای بانکداری الکترونیکی را، توسط مسدود کردن متجاوزان غیرقانونی و هکرهای خارجی متوقف کند. این راه حل امنیتی باید متجاوزان را نه تنها در سطح کاربر بلکه در سطوح هسته مسدود کند و کرم‌ها و تروجان‌هایی را که از طریق امضا شناخته می‌شوند و به‌طور مداوم به‌روزرسانی می‌شوند، مسدود یا حذف کند. برای اینکه از عهدهٔ تهدیدهایی که هنوز ناشناس هستند برآییم، باید محیط بانکداری الکترونیکی را به‌خوبی شناخته و ارتباطات غیرقانونی شبکه را از طریق یک برنامه‌ریزی ویژه مسدود کنیم. تیم امنیتی سرویس بانکداری الکترونیکی باید همیشه آماده باشد تا از هک سازمان‌دهی شده و پیچیده جلوگیری کند که این امر با استفاده از فناوری‌های امنیتی وارد کردن کلمات کلیدی، فناوری مرورگر وب و امنیت شبکه و انسداد ابزارهای هک کننده میسر است. یک راه حل امنیتی بانکداری الکترونیک از سه فناوری اصلی تشکیل می‌شود:

۱. Anti key logger که در آن از یک صفحه کلید امنیتی جهت ورود اطلاعات استفاده می‌شود؛

۲. Secure browser یک مرورگر وب اختصاصی که کلیهٔ نکات امنیتی در آن رعایت شده است؛

۳. یک Firewall اختصاصی جهت مسدودکردن ابزارهای هک کنندهٔ مورد استفاده در شبکه و برقراری امنیت شبکه.

فناوری جدید امنیت مرورگر

ما نیاز به یک فناوری امنیتی داریم که با مسدود کردن متجاوزان غیرقانونی و هکرهای خارجی تهدیدها را متوقف کند. این راه حل امنیتی باید متجاوزان را نه تنها در سطح کاربر بلکه در سطوح هسته مسدود کند و کرم‌ها و تروجان‌هایی را که از طریق امضا شناخته می‌شوند و به‌طور مداوم به‌روزرسانی می‌شوند، مسدود یا حذف کند

منابع:

* www.global.ahnlab.cm/online banking:threats and countern countermeasures
* www.en.wikipedia.org
* www.krebsonsecurity.com