شرکت سیلیکون تصمیم ایرانیان

(مستقر در پارک علم و فن آوری گیلان)

به نام خداوند جان و خرد
کز این برتر اندیشه برنگذرد

سیستم متمرکز احراز هویت با توکن (OTP) آرش

مقدمه

پس از سه دهه که از عمر موثر اینترنت در دنیا میگذرد، استفاده از خدمات الکترونیکی سازمانها و وب گردی به قصد یافتن مطالب و کالاهای مورد نیاز، اتفاق خوش آیندی است که برای همه ما به صورت روزمره اتفاق می افتد. ولی به طبع پیشرفتهایی که در فن آوری و ارائه خدمات الکترونیکی حاصل میگردد، جرایم و تهدیدهای سایبری در حال رشد و پیشرفت هستند. لذا، آنچه بعضا به عنوان یک تجربه تلخ مشترک شهروندان الکترونیک ساکن دهکده جهانی شناخته میشود، تحمیل روز افزون تعداد بیشماری رمز عبور ثابت و یا انواع سخت افزار توکن با استانداردهای قدیمی به کاربران است که به نظر میرسد با نزدیک شدن به دورانی که آرام آرام وارد فضای نوین پردازش ابری میشویم، نیاز به پیاده سازی یک سیستم متمرکز احراز هویت ایمن، بیش از بیش نمایان میگردد.

رمز یک بار مصرف (OTP) چیست؟

یکی از روش های جلوگیری از حدس زدن کلمات عبور ضعیف و نامناسب، استفاده از رمزهای یک بار مصرف (One Time Password) می باشد. آنچه که از کلمه رمز در ذهن اغلب افراد تداعی می شود، کلمه ی رمز ایستا می باشد که مقداری است ثابت و می بایست به خاطره سپرده شود. در مقابل رمز ثابت ، رمز یک بار مصرف یا OTP قراردارد که به معنای کلمه رمزی است که فقط و فقط یکبار می تواند مورد استفاده قرار گیرد. برای تولید کلمات عبور یک بار مصرف از ابزاری به نام توکن OTP، استفاده می گردد. رمز یکبار مصرف برای ایمن سازی دسترسی کاربران به سیستم های الکترونیکی است، که در آن از قابلیت های رمز نگاری (متقارن) برای تولید رمز تصادفی یک بار مصرف استفاده می شود.

گزارش مشکل در صنعت فن آوری اطلاعات

همانطور که گفته شد، یک ایراد اساسی که کاربران در دنیای امروز با آن دست به گریبان هستند، لزوم ثبت نام و دریافت رمز عبور از تمامی وب سایتهای مخاطب خود هستند. مدیریت و نگهداری این حجم بالای رمزهای عبور ثابت و تک عاملی ، به نحوی که فاش نشوند و غیر تکراری هم باشند، و دارای طول و پراکندگی کافی نیز باشند، به اندازه کافی باعث آزار کاربران میشود که نیاز به دو یا چند عاملی شدن مراحل احراز هویت با دستگاه های OTP نیز بر این بار اضافی به شرح زیر افزوده است:

1- هزینه ای که در اثر اجبار به خرید این سخت افزارها به کاربران تحمیل میگردد
2- هر دستگاه تنها توانایی مخاطب قرار دادن یک سازمان را دارد. بنابراین، هر کاربر در صورت هر نوع جابجایی مجبور خواهد بود تمامی دستگاه های OTP خود را به همراه داشته باشد. نگهداری و حفاظت از این حجم تجهیزات در مقابل دزدیده شدن، به تنهایی باعث استرسی، اتلاف وقت و کاهش بهره وری است.

توکن آرش چیست؟

توکن آرش به عنوان نخستین سخت افزار تولید کننده رمز عبور یکبار مصرف OTP در خاورمیانه، و تنها سیستم متمرکز احراز هویت مبتنی بر رمز نگاری (نامتقارن) در جهان است به نحوی که در سمت کاربر هیچ نیازی به ایجاد کانال انتقال ایمن SSL یا VPN جهت انتقال مقادیر رمز تولید شده و نصب رابط یا پورت سخت افزاری و نرم افزاری خاصی همچون: USB ، NFC ، کارت خوان، نرم افزار درایور و غیره نمیباشد.

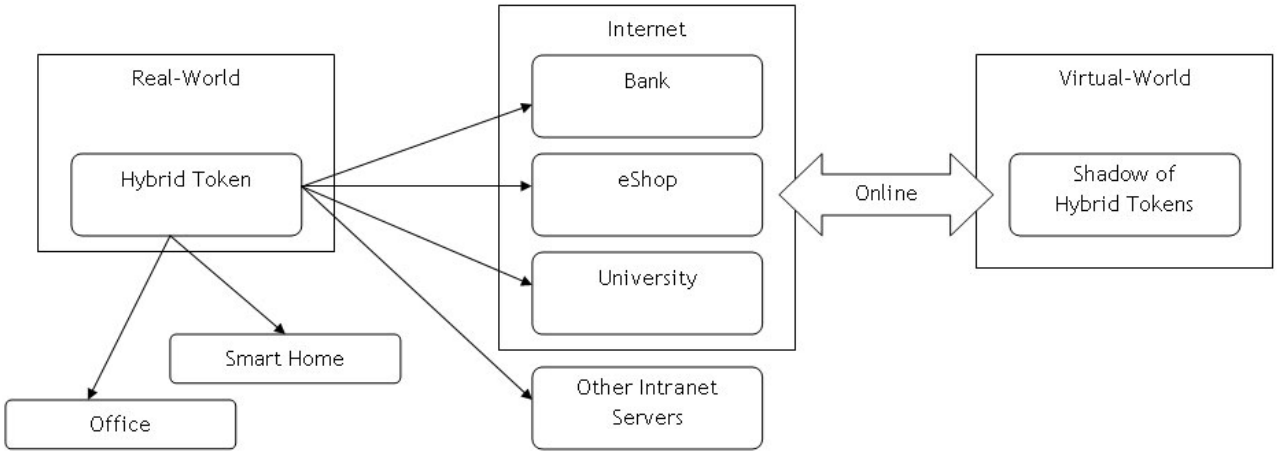
لازم به ذکر است که مالکیت فکری توکن آرش به شماره اختراع 82305 در ایران به ثبت رسیده و در کنار نامهای بزرگی به شرح زیر قرار دارد:

- PAT. NO.: 5,768,373 - **Assignee: Symantec Corporation (Cupertino, CA)** - Title: Method for providing a secure non-reusable one-time password
- PAT. NO.: 7,058,180 - **Assignee: Swisscom Mobile AG (Bern, CH) -** Title: Single sign-on process
- PAT. NO.: 7,548,620 - **Assignee: VeriSign, Inc. (Mountain View, CA)** - Title: Token provisioning
- PAT. NO.: 7,930,554 - **Assignee: Vasco Data Security,Inc. (Oak Brook Terrace, IL) -** Title: Remote authentication and transaction signatures
- PAT. NO.: 8,015,599 - **Assignee: Symantec Corporation (Mountain View, CA) -** Title: Token provisioning
- PAT. NO.: 8,281,375 - **Assignee: eBay Inc. (San Jose, CA) -** Title: One time password authentication of websites
- PAT. NO.: 8,468,351 - **Assignee: Codesealer APS (Valby, DK)** - Title: Digital data authentication
- PAT. NO.: 8,543,829 - **Assignee: eBay Inc. (San Jose, CA)** - Title: Token device re-synchronization through a network solution
- PAT. NO.: 8,600,056 - **Assignee: Apple Inc. (Cupertino, CA) -** Title: Method and system for controlling the locking/unlocking of the network access functions of a multifunction terminal
- PAT. NO.: 8,667,285 - **Assignee: Vasco Data Security, Inc. (Oakbrook Terrance, IL) -** Title: Remote authentication and transaction signatures

راه حلی که توکن آرش ارائه میدهد

همانطور که گفته شد، ایجاد یک سیستم متمرکز احراز هویت مبتنی بر رمز نگاری (نامتقارن) راه حلی است که اختراع پیشرفته توکن آرش آنرا ارائه میدهد. با تمرکز سیستم احراز هویت در یک محل که سرور سایه Shadow نامیده میشود، سرویس دهنده های مختلف این توانایی را خواهند داشت که با اتصال به این سیستم متمرکز، اقدام به شناسایی کاربران نمایند. همچنین جدای از اینترنت، کاربران در این سیستم میتوانند دستگاه های توکن آرش خود را جهت هماهنگی با سرویس دهنده های شبکه های محلی از قبیل محل کار یا خانه های هوشمند ، پیکر بندی کنند. این بدان معناست که توکن آرش به سادگی میتواند با نادیده گرفتن قابلیت های فراوان خود در

اینترنت، تنها برای یک مرکز در اینترنت یا شبکه محلی اینترانت به صورت منحصر بفرد پیکربندی شود. بـه همـین دلیل توکن آرش دارای صفت هایبرید (دارای کاربری دوگانه) میباشد.



بنابراین، در صورت بکار گیری این دستگاه در یک سازمان همچون بانک، این قابلیت را به مشتریان میدهد تا تنها با استفاده از یک دستگاه توکن آرش، بتوانند از تمامی سرویسهای الکترونیکـی بـه صـورت همزمـان اسـتفاده نماینـد. همچنین، از آنجایی که توکن آرش بر مبنای الگوریتمای قدرتمند (نا متقارن) اقدام به تولید رمز عبور یکبار مـصرف مینماید، استفاده از کانال رمز شده SSL یا VPN (به منظور جلوگیری از حملات دیکشنری) برای انتقـال مقـدار رمز تولید شده مربوطه الزامی نیست. بنابراین، سیستمهایی همچون تلفن بانک یا موبایل بانک کـه از ابتـدایی تـرین شکل انتقال داده (متن رمز نشده) استفاده میکنند نیز تحت پوشش این دستگاه قرار میگیرند. مزایای یـک سیـستم احراز هویت متمرکز برای سرپرست شبکه و مدیران فن آوری اطلاعات سازمانها کاملا واضح و گسترده است.

توکن آرش، نقاط ضعف توکنهای OTP موجود را ارتقاء میدهد:

- RFC 4226: page 2 - At the same time, the current approach that requires an end user to carry an expensive, single-function device that is only used to authenticate to the network is clearly not the right answer.
- RFC 4226: page 3 - One-Time Passwords are often preferred to stronger forms of authentication such as Public-Key Infrastructure (PKI) or biometrics because an air-gap device does not require the installation of any client desktop software on the user machine, therefore allowing them to roam across multiple machines including home computers, kiosks, and personal digital assistants.
- RFC 6287: page 17 - IC6 - All the communications SHOULD take place over a secure channel, e.g., SSL/TLS, IPsec connections.
- RFC 6287: page 18 - **Conclusion:** This document introduced several variants of HOTP for challenge-response-based authentication and short signature-like computations.

توضیح: دستگاه های تولید رمز عبور یکبار مصرف موسوم به One Time Password عموما از استاندارد متن باز OATH استفاده میکنند که نقاط ضعف امنیتی آنها به جهت کسب سهم بیشتر بازار به مشتری اعلام نمیشود در حالی که در متن صریح RFC های مربوط به دانش فنی این قبیل دستگاه ها، اعلام میگردد که این روشهای فعلی راه حل مناسبی برای رفع نیاز احراز هویت کاربران در دنیای انفورماتیک نیستند و صرفا جهت اطلاع و یک نقطه آغاز میتوانند مورد استفاده قرار گیرند:

- شرکتهای تولید کننده دستگاه های تولید رمز عبور یکبار مصرف ، برداشت سطحی و مشتری پسند همچون قابلیت امضای دیجیتال، از متن صریح RFC-6287 مربوط به فن آوری تولید چنین دستگاه هایی را ارائه میدهند که به هیچ عنوان صحت ندارد.
- متن صریح RFC-4226 و RFC-2104 اعلام میدارد که اهمیت و محبوبیت دستگاه های OTP به دلیل عدم نیاز آنها به نصب هر نوع واسط نرم افزاری یا سخت افزاری در سمت کاربر است و علی رغم ضعف امنیتی این روش نسبت به روشهای احراز هویت بیومتریک و زیر ساخت کلید عمومی، همچنان مورد اقبال بازار است.

سایر مزایای توکن آرش:

- استفاده از الگوریتم رمزنگاری نامتقارن طول پیام را چند برابر میکند که همین امر باعث عملکرد به مراتب بهتر دستگاه توکن هایبرید در محافظت از قابل پیش بینی شدن رفتار تابع تولید پیام در مقابل مهاجم میگردد.
- به این دلیل که تمامی توابع و ساختارهای سخت افزاری و نرم افزاری توکن آرش در محل شرکت سیلیکون طراحی و ساخته شده است، این اطمینان برای سازمانها وجود دارد که به هیچ عنوان این سیستم به هیچ نوع Back Door آلوده نیست. چیزی که در مورد سایر توکن های موجود در کشور صدق نمیکند.
- به دلیل استفاده از ابتدایی ترین المانهای الکترونیکی، تقریبا هیچ نوع تحریمی بر این دستگاه اثر ندارد.
- دستگاه توکن آرش، پدیده ای نو در مقوله Internet of Things با رویکرد پردازش ابری است.
- توکن آرش از یک منطق منحصر بفرد در تولید پویای تابع HASH به صورت منتشر نشده استفاده میکند.

توکن آرش چه خدماتی را ارائه میدهد:

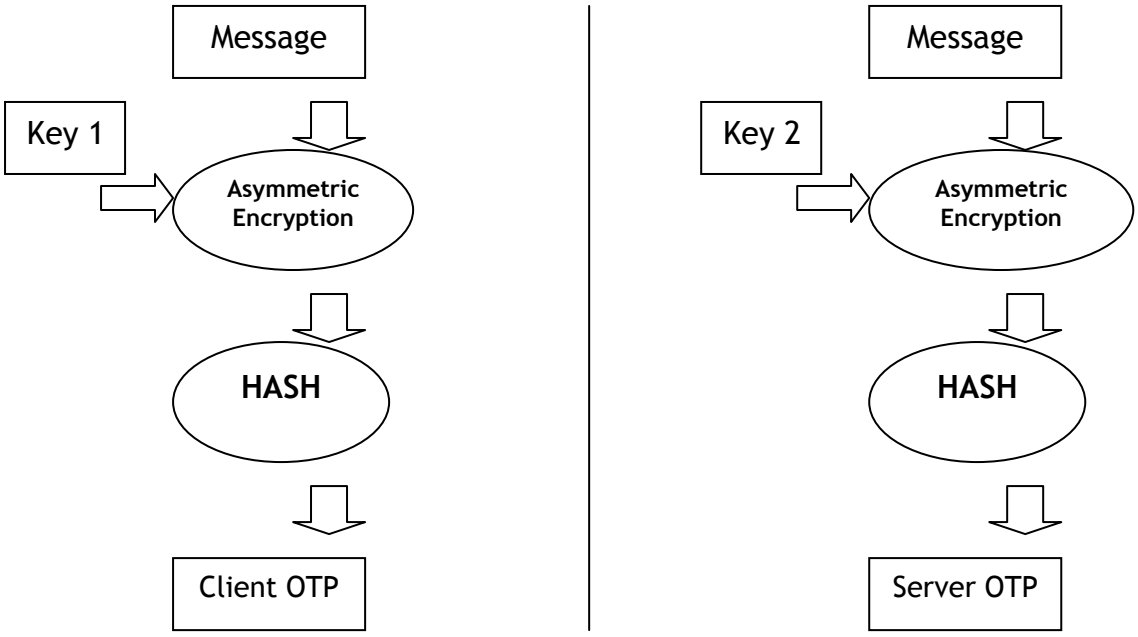
- تولید رمز عبور یکبار مصرف OTP
- امضاء الکترونیکی انواع تراکنشهای مالی و اداری
- سیستم متمرکز احراز هویت

توکن آرش چه خدماتی را ارائه نمیدهد:

- زیر ساخت کلید عمومی
- آنتی ویروس یا ضد بد افزار
- دیوار آتشین
- کنترل محتوی ترافیک
- کانال امن تبادل داده

برتری توکن آرش نسبت به سایر رقبا در استفاده از رمزنگاری نامتقارن نهفته است:

نکته عمده در ارتباط با باقی ماندن نقاط ضعف در فن آوری توکن OTP، در اجبار طراحان در استفاده از الگوریتمهای رمز نگاری متقارن و الزام به عبور دادن پیام رمز شده از یک تابع HASH است ، به نحوی که در سمت سرویس دهنده و سرویس گیرنده یک روال مشابهه با الگوریتم و مقادیر مشابه دنبال میگردد و در صورتی که پاسخ متناظر و مشابه در هر دو سمت تولید گردد، احراز هویت به سبک رمز عبور یکبار مصرف OTP با موفقیت انجام میگردد. در حالی که مطابق شکل زیر، قدرتمند کردن OTP ها با الگوریتمهای رمزنگاری نامتقارن به دلیل ماهیت الگوریتمی OTP Token ها در دستگاه های (غیر متصل) که امکان تبادل کلید عمومی ندارند، یک امر غیر ممکن است:



بررسی عملکرد الگوریتمی توکن هایبرید آرش

الگوریتم ها به تنهایی فن آوری محسوب میگردند – در ارجاع به مقدمه کتاب پیشرفته Introduction to Algorithms – ISBN: 0-07-013151-1 از انتشارات Mc Graw Hill نگارندگان در بدوی ترین تعریف قابل ارائه از الگوریتم، اشاره به این مهم دارند که الگوریتمها به تنهایی یک فن آوری محسوب میشوند ، هم رده سخت افزارها، واسط های کاربری گرافیکی، سیستمهای شی گرا و شبکه ها:

It also makes a case that algorithms are a technology, just as are fast hardware, graphical user interfaces, object-oriented systems, and networks.

اما تعریف عمومی از الگوریتم به شرح زیر ارائه شده است: الگوریتم به مراحل محاسباتی ترتیبی گفته میشود که ورودی ها را به خروجی ها تغییر شکل میدهند:

An algorithm is thus a sequence of computational steps that transform the input to the output.

همچنین نظرکتاب فوق در مورد نحوه تعیین صحت یک الگوریتم ، به این شرح است: بـه الگـوریتمی صـحیح گفتـه میشود که برای هر ورودی نمونه ای که به آن وارد شود، ختم به یک پاسخ صحیح گردد:

An algorithm is said to be correct if, for every input instance, it halts with the correct output.

همچنین بر همین منوال در تعریف الگوریتمهای نا صحیح آمده است کـه: الگوریتمهـای نـا صـحیح بـرای برخـی از ورودی های نمونه قادر به اتمام محاسبات نمیگردند و یا به پاسخهای غیر منتظره ختم میگردند:

An incorrect algorithm might not halt at all on some input instances, or it might halt with an answer other than the desired one.

لازم به یاد آوری است که اصولا ماهیت مقوله امنیت در رایانه ها ، در ایجاد قابلیت غیر قابل پیش بینی بودن نتـایج برای مهاجم است. یعنی در روشهای نرم افزاری که به ایمن سازی در فضای سایبری ختم میگردد، اتفاقـا بـر عکـس الگوریتمهای محاسباتی و عملیاتی که نتایج قابل پیشبینی با نتایج حاصل از الگوریتم مقایسه شده و صحت عملکـرد الگوریتم را نتیجه میدهد، دستیابی به الگوریتمهای نا صحیح معیار برتری و ارزشمند بودن یـک الگـوریتم در مقولـه امنیت است. خصوصا که در موضوع و ادعای ثبت اختراع با دستگاهی سر و کار داشته باشیم که ادعا میکند میتوانـد رمز یکبار مصرف تولید کند. یعنی هرگز خروجی قابل پیشبینی ارائه نمیدهد.

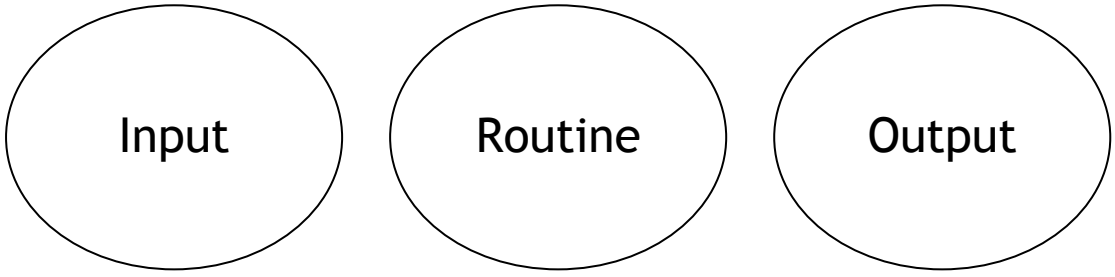
از همین رو کتاب در ادامه اعلام میکند: بر خلاف آنچه برخی انتظار دارنـد، الگوریتمهـای غلـط میتواننـد در برخـی موارد سودمند باشند، در صورتی که میزان خطا قابل کنترل باشد. ما در فصل 31 یک نمونه از این نوع الگوریتمها را وقتی به مطالعه الگوریتمهایی برای یافتن اعداد اول بزرگ بپردازیم، مشاهده خواهیم کرد. هر چنـد کـه معمـولا، مـا باید نگران الگوریتمهای درست باشیم:

Contrary to what one might expect, incorrect algorithms can sometimes be useful, if their error rate can be controlled. We shall see an example of this in Chapter 31 when we study algorithms for finding large prime numbers. Ordinary, however, we shall be concerned only with correct algorithms.

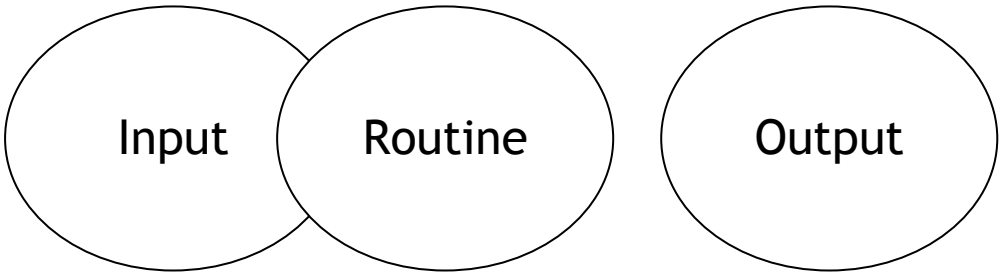
قابل توجه اینکه، مثال ذکر شده در فصل 31 کتاب ، مربوط بـه صـفحه 881 در شـرح الگـوریتم رمزنگـاری کلیـد عمومی RSA میباشد.

خواص الگوریتمی فن آوری موجود در دستگاه توکن هایبرید

در این باره، نمودار ون بهترین شکل توصیفی را ارائه میدهد. در الگوریتمهای صحیح، عملکرد الگوریتمی همیشه به صورت اجزای مجزای ورودی ، روتین های اجرایی و خروجی هستند که هیچ نقطه اشتراکی هم با هم ندارند:

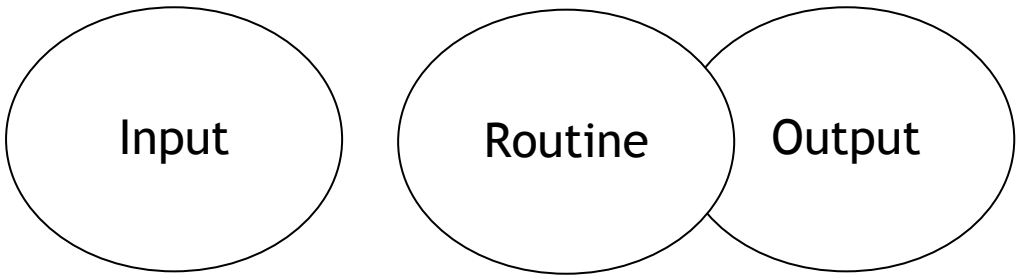


جهت روشنتر شدن مطلب، به طور مثال، الگوریتمهای رمزنگاری متقارن Symmetric به صورت عمومی از ساختار الگوریتمهای صحیح استفاده میکنند و در اثر اعمال هر نوع ورودی، وظایف خود را به طور مثال در قالب تکرار یک XOR ساده به انجام رسانده و خروجی را گزارش میدهد. ولی در الگوریتمهای رمزنگاری نا متقارن همانند RSA ، به دلیل شرایطی که روتین های محاسباتی بر ورودی ها و شرایط پیش از اجرای روتین های داخلی اعمال میکنند، نمودار ون آنها به شکل زیر تغییر مینماید:

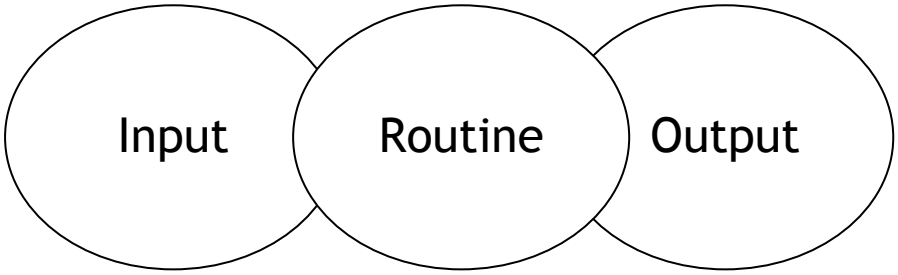


چنین الگوریتمهای از یک طرف برای محاسبه خروجی به سادگی محاسبات را به اتمام میرسانند و در صورتی که قصد داشته باشید از خروجی به ماهیت ورودی دست پیدا کنید، با یک مسئله سخت روبرو میشوید، بنابراین برای دست پیدا کردن به مقدار ورودی که مطابق تعریف **برگشت پذیر** است ، میبایستی از طریق یک روتین دیگر (کلید دوم) اقدام به محاسبه نمایید.

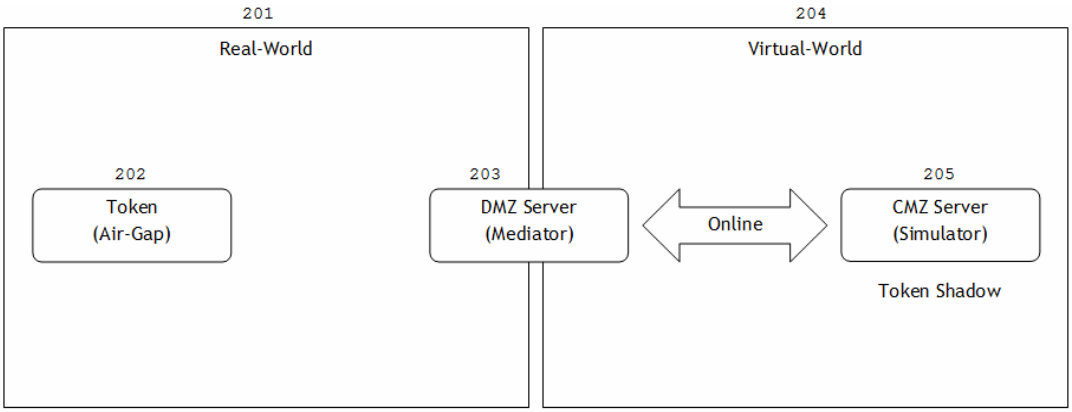
و همچنین در الگوریتمهایی که به جهت تولید یک مقدار HASH یک طرفه به عنوان خروجی طراحی شده اند، شرایطی بر خروجی حاکم میگردد که محاسبه مقدار ورودی از مقدار خروجی کاملا غیر قابل برگشت میباشد. لذا نوع رفتار الگوریتم در نمودار ون به شرح زیر تغییر ماهیت میدهد:



بنابراین، برای احراز عملکرد روتین های تعبیه شده، نیازمند **پردازش موازی** روتین در برابر یک مقدار ورودی یکسان هستید. به استناد RFC های ضمیمه ادعای شماره 3، شرایطی مشابهی نمودار ون فوق، به دلیل استفاده همزمان از رمزنگاری متقارن و توابع HASH در دستگاه های فعلی OTP موجود در سطح جهان حاکم است. ولی در مورد الگوریتمهای غلط مورد استفاده در دستگاه توکن هایبرید که باعث ارزشمندی آن شده است، نمودار ون به شرح زیر تغییر میباید:

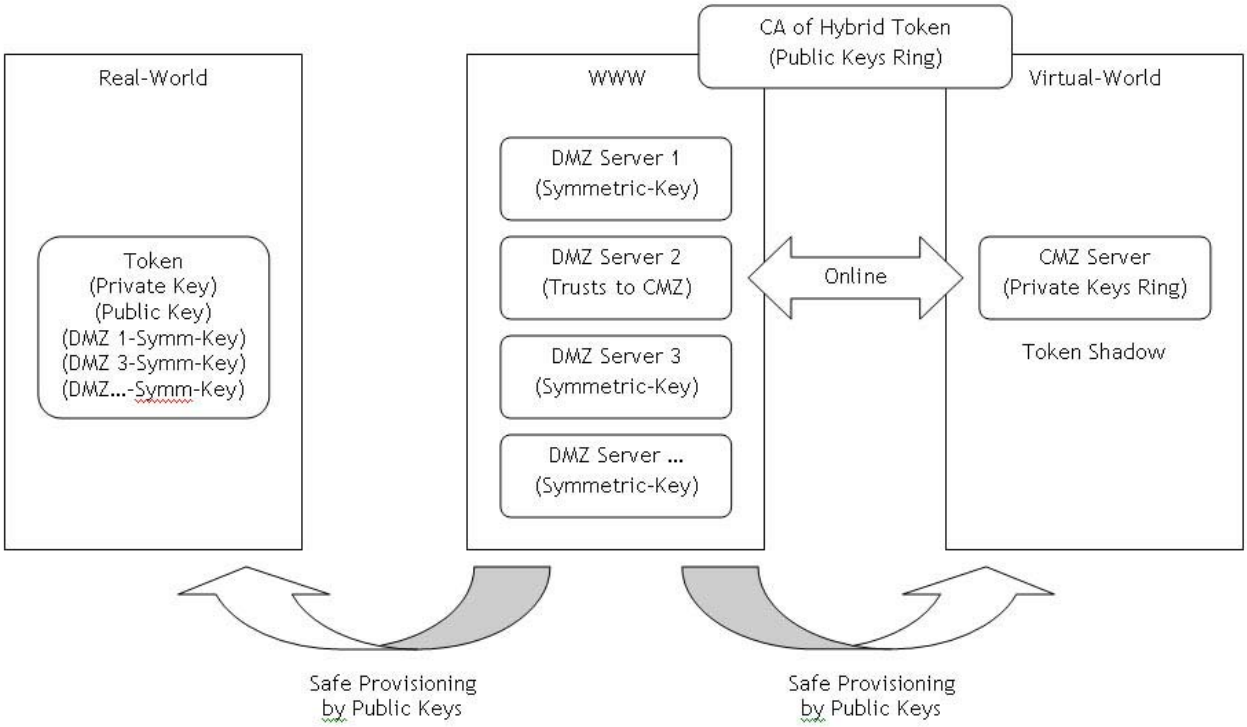


و به این ترتیب، آنچنان سطح آشفتگی ، اعمال قانون و نظارت از طریق روتین های داخلی الگوریتم به دو مجموعه ورودیها و خروجیها تحمیل میگردد که شایسته استفاده در زیر ساختهای امنیت سایبری میگردد. استفاده همزمان از الگوریتمهای رمزنگاری نا متقارن **شرایط ویژه ای را بر Input های خود تحمیل میکند**، غیر از اینکه جهت تولید پاسخ نهایی با عبور دادن مقادیر از یک تابع عملگر HASH یک طرفه، **شرایط پردازش موازی را نیز بر Output سیستم حاکم مینماید**. که باعث یکتا شدن این اختراع شده است. در حقیقت حفظ پیوستگی در تمامی مراحل اجرای یک الگوریتم غلط، یکی از مواردی است که دقیقا در اجرای سیستم متمرکز تولید رمز عبور یکبار مصرف توسط دستگاه توکن آرش به شرح زیر رعایت میگردد:



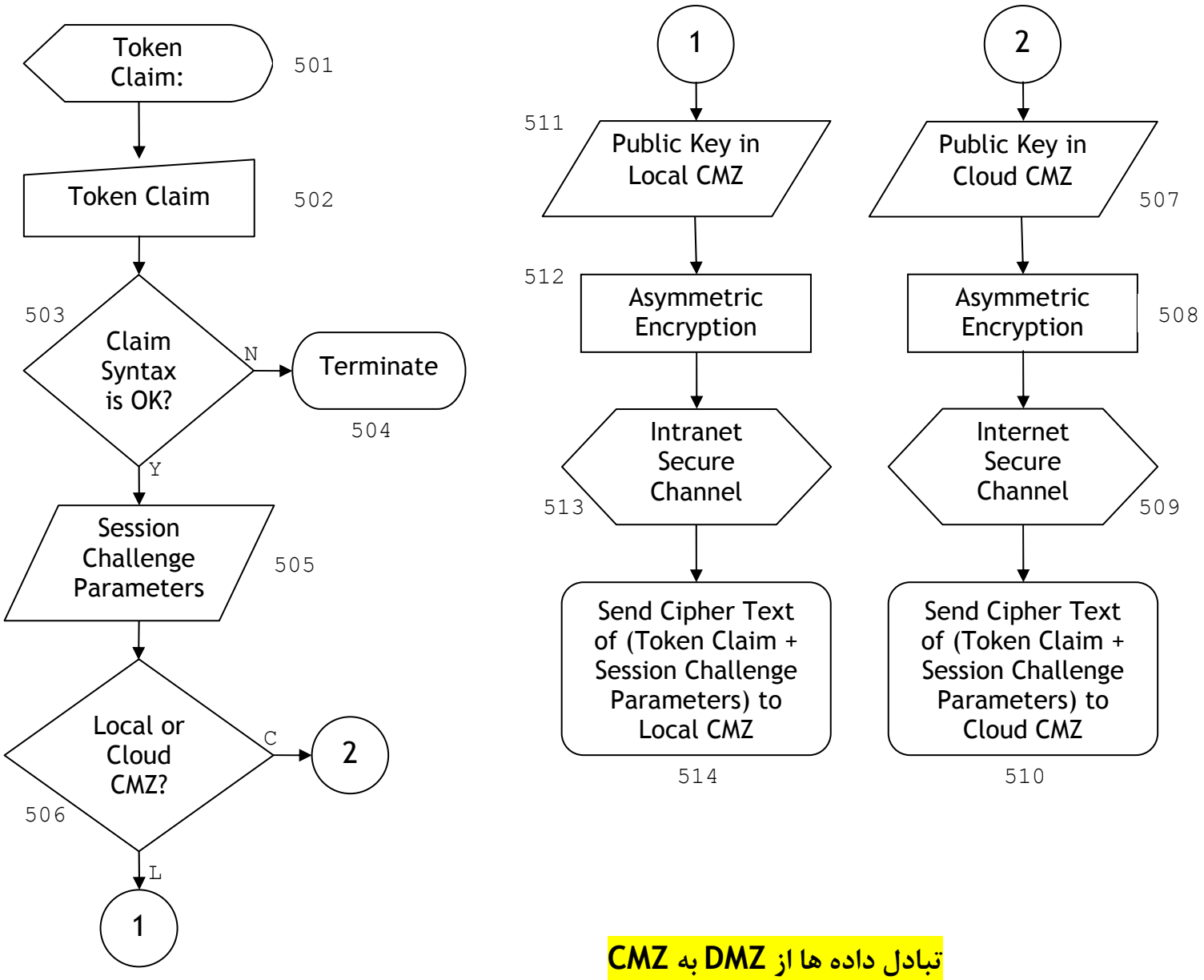
در این حالت در صورتی که از رمزنگاری متقارن برای تمرکز در CMZ جهت شبیه سازی توکن استفاده شود، نظر به اینکه کلید مورد استفاده قرار گرفته، نمیتواند در محل DMZ قابل دسترسی باشد، لذا هیچ کنترلی نیز بر روال احراز هویت نداشته و در عمل خارج از محدوده الگوریتم غلط قرار میگیرد. این امر باعث عدم اعتماد لایه DMZ در ایجاد یک شبکه امن و یکپارچه خواهد شد. ولی از سوی دیگر، استفاده از الگوریتم نامتقارن در این فرآیند متمرکز

سازی، این قابلیت را به لایه DMZ میدهد که با دسترسی به کلید عمومی، در فرآیند انتقال پیام از محل DMZ به CMZ شرکت داشته و این عمل باعث خدشه دار شدن پیوستگی در الگوریتم غلط نگردد.

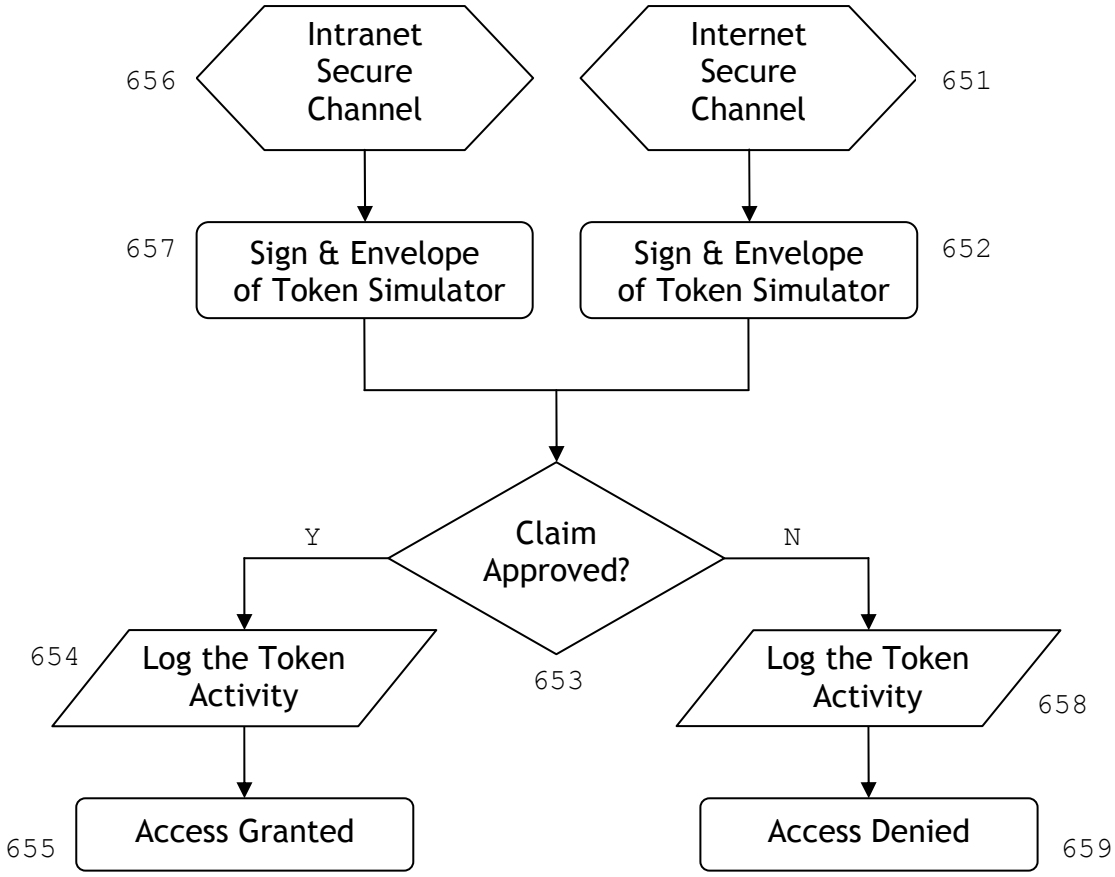


همچنین، استفاده از تابع رمز نگاری نامتقارن این اطمینان را به توابع موجود در DMZ میدهد که پیام تولید شده در DMZ دقیقا توسط توکن شبیه سازی شده متناظر دریافت میگردد. نظر به اینکه ماهیت CMZ در ایجاد پیام هیچ مشارکتی نمیتواند داشته باشد، در مواردی لازم است که لایه DMZ پیش فرضهایی را (حتی در حد تعریف یک کلید متقارن اضافی میان DMZ و Token اصلی جهت تولید پیام) و یا برخی پیش فرضها در توکن شبیه سازی شده تغییر داده و یا به روز رسانی کند. در چنین شرایطی مقادیر مذکور به سادگی میتوانند توسط کلید عمومی رمز شده و در اختیار دو توکن اصلی و شبیه سازی شده قرار گیرند و این اطمینان را برای DMZ حاصل کنند که تابع تولید پیام در توکن مورد نظر، مخاطب اختصاصی DMZ بوده است. اتخاذ چنین رویکرد نامتقارنی، قابلیت تحمل خرابی در ارتباط بین DMZ و CMZ مرکزی را بر روی شبکه اینترنت، با توجه به منحرف کردن مسیر احراز هویت به اینترانت داخلی در سطح DMZ بالا میبرد. چنین رفتاری در شبکه متمرکز مبتنی بر رمزنگاری متقارن فعلی قابل تصور نیست.

توضیح 1: توکن شبیه ساز در CMZ یک تولید کننده رمز عبور یکبار مصرف نیست و تنها به صورت تایید کننده صحت یک رمز یکبار مصرف عمل کرده و کشف و استخراج کلید خصوصی از ان عملا غیر ممکن است. دستگاه توکن اصلی، تنها دستگاه تولید کننده رمز عبور یکبار مصرف است.
توضیح 2: توکن آرش را میتوان در چند برنامه و شبکه به صورت همزمان مورد استفاده قرار داد.



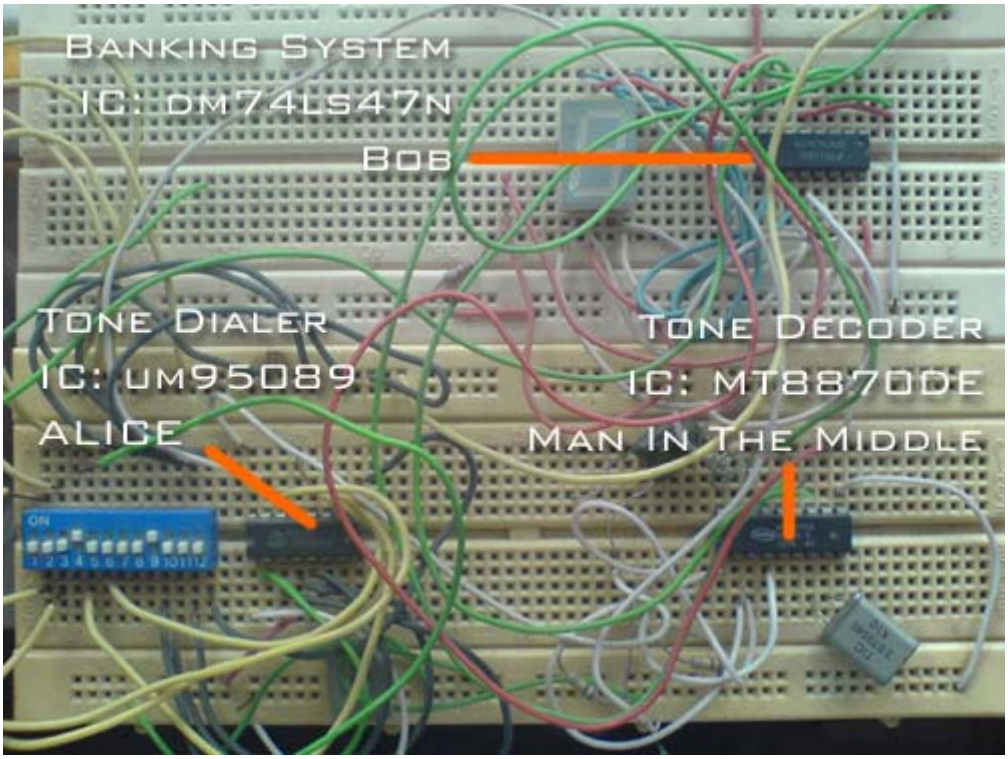
تبادل داده ها از DMZ به CMZ



تبادل داده ها از CMZ به DMZ

خنثی کردن حملات Man In The Middle

توکن هایبرید به دلیل استفاده از الگوریتم رمزنگاری نا متقارن عملا مجهز به نوعی SSL درونسازی شده است در حالی که FRC-6287 تبادل رمز یکبار مصرف را تنها از طریق یک کانال امن مجاز میداند. در ادامه، روش حمله شبیه سازی شده غیر فعال Passive Attack به سیستمهای تلفن بانک سراسر کشور قابل توجه است. این برد الکترونیکی در آزمایشگاه روبوتیک و هوش مصنوعی در محل شرکت سیلیکون موجود است. تجهیز این دستگاه به میکرو کنترلر و فرستنده، آنرا قادر به انجام حملات مهلکی به کاربران شبکه بانکی میکند:



همچنین میبایستی در نظر داشت که امروزه حملات مرد میانی به پیام در حال تبادل منحصر نمیشوند و دامنه آنها به انواع Key Logger ها در درون رایانه یا تلفن همراه مشتری و یا رصد ورود رمز در عابر بانکها در خیابان – قبل از وارد شدن داده پیام به کانال ارتباطی امن- نیز گسترش یافته است. لایه ایمن SSL به هیچ عنوان قادر به حذف چنین حملاتی از قبیل Fabrication و بعضا Modification نمیباشد. بنابر این توکن هایبرید، علاوه بر احراز هویتAuthentication ، به دلیل قابلیت دریافت پارامترهای اضافی در رشته مربوط به پیام، میتواند عملا در بحث حق دسترسی Authorization نیز وارد شده و بخشهایی از دستورات – مثلا – اطلاعات کارت بانکی مقصد و مبلغ مرتبط با یک پرداخت الکترونیکی را در درون تابع تولید پیام خود وارد کند و به این ترتیب، در صورت ایجاد هر گونه تغییر در متن دستور توسط مهاجم، کل عملیات لغو شود.

جدول مقایسه ای توکن آرش با انواع توکن های موجود در بازار

Token Type	Single Button	Numeric Keypad	Smart Card	USB Device	Arash Token (Numeric Keypad)
One Time Password	X	X	X	X	X
Transaction Integrity		X	X	X	X
Non-Repudiation			X	X	X*
Signature Like		X			X*
Crypto Algorithm	Symmetric	Symmetric	Asymmetric	Asymmetric	Asymmetric
Secure Channel Included			X	X	X
Air-Gap	X	X			X
Centralized Authenticator		X	X	X	X
DMZ Envelope			X	X	X
DMZ Special Envelope					X
Net Failure Protection					X
Multi Functional in Internet			X	X	X
Multi Functional in Intranet					X
Pin Protection		X	X	X	X
Anti Padding Attack	X	X			X
Anti Clone					X

*Non-Repudiation: when CMZ follows related standards.
*Signature Like: when CMZ does not follow related standards.
*Secure Channel Included: generated OTPs could transmit in plain text because of using strong asymmetric encrypt algorithms.
*Air-Gap: needs no extra reader device or connector at client side.
*Centralized Authenticator: a group of DMZ servers could use one authenticator behind them.
*DMZ Envelope: could provide encryption among multi DMZs and a single token.
*DMZ Special Envelope: could provide special extra encryption and proceed to provision among multi DMZs to a single multi-functional token.
*Net Failure Protection: when centralized authenticator and DMZ fail to connect, DMZ alone could still continue authentication process.
*Multi Functional in Intranet: simultaneously works both in internet and several intranets like smart home, office, etc.
*Pin Protection: when you turn on the device, asks for a PIN to login.

سر خط آخرین گزارشات و تهدیدهای امنیت سایبری (July, 2014) که با توکن هایبرید آرش خنثی میشوند:

- اعلام نا کار آمدی الگوریتم HASH موسوم به SHA-1 که زیر ساخت توکنهای موجود در بازار میباشد:
SHA-1 to SHA-2: The future of SSL and enterprise application security
http://www.linkedin.com/today/post/article/20140704134155-17333004-sha-1-to-sha-2-the-future-of-ssl-and-enterprise-application-security

- حملات پدینگ به توکن های USB:
Efficient Padding Oracle Attacks on Cryptographic Hardware
https://eprint.iacr.org/2012/417.pdf

- درسهایی که از نفوذ به eBay گرفته میشود:
What Enterprises Can Learn From eBay Data Breach
http://www.toptechnews.com/article/index.php?story_id=132004JXHTW0

- چالشهای سیستمهای POS:
Point-Of-Sale System Security Challenges
https://www.clickssl.com/blog/point-of-sale-system-security-challenges

- حفره امنیتی در سیستم مالی:
Banks: Credit Card Breach at P.F. Chang's
http://krebsonsecurity.com/2014/06/banks-credit-card-breach-at-p-f-changs/

- اعلام نا کار آمدی سیستم عامل اندروید در نگه داری رمزهای عبور درون سازی شده:
Serious Android Crypto Key Theft Vuln Affects 86% Of Devices
http://arstechnica.com/security/2014/06/serious-android-crypto-key-theft-vulnerability-affects-86-of-devices/

- تحت کنترل قرار گرفتن دستگاه های اندروید توسط بد افزار های مخفی در گوگل پلی:
Google Play Store Update Allows Apps to Silently Gain Control
http://thehackernews.com/2014/06/google-play-store-update-allows-apps-to.html