禪

[redacted]

[redacted]

[redacted]

[redacted]

مطلب پیشنهادی

مغز انسان همچنان قدرتمند و گرهگشا است

استفاده از پالسهای مغزی به جای رمزعبور و حسگرهای بیومتریک

فرض کنید با اطمینان از دستگاهی استفاده میکنید که تنها بر پایه مکانیزم احراز هویت اثر انگشت مورد استفاده قرار میگیرد؛ اما اگر اثرانگشت شما به سرقت رفت و از این اثر انگشت برای بازگشایی انواع مختلفی از حسابها استفاده شد، باز هم میتوانید اثرانگشت خود را عوض کنید؟ آیا آنتیویروسهایی که این روزها بازار پر رونقی دارند را میتوانیم در برابر انواع مختلفی از تهدیدات مورد استفاده قرار داده، بهطوریکه از ما در برابر تهدیدات سنگین محافظت به عمل آورند؟ آیا نرمافزارهای امنیتی ما توانایی مقابله با حملات سنگین DoS را دارند؟ اینها سؤالاتی است که در این مقاله قصد داریم با ذکر دلیل به آنها پاسخ و به شما نشان دهیم، آینده دنیای امنیت، چیزی فراتر از ابزارهایی است که این روزها با آنها آشنا هستیم .

فناوریهای خلاقانهای که امروزه به تاریخ پیوستهاند

آیا از شکاف حفاظتی تعبیه شده روی فلاپیدیسکها، برای پیشگیری از آلوده شدن آنها به ویروسهای بوتسکتور و مخرب استفاده میکردید؟ آیا مودم دیالآپ خود را در طول شب خاموش میکردید، تا هکرها در طول شب اقدام به شمارهگیری آن نکنند؟ آیا از بارگذاری درایور فایل ansi.sys که میتوانست توسط فایلهای مخرب مورد استفاده قرار گرفته و با تغییر جای کلیدها فرمت کردن هارددیسک را امکانپذیر سازد، ممانعت به عمل میآورید؟ آیا فایلهای Autoexec.bat و Config.sys را مورد بازبینی قرار میدادید تا مطمئن شوید هیچ موجودیت تخریبی درون آنها قرار نداشته باشد؟ همانگونه که این فناوریها و راهکارها در گذر زمان، ناپدید شدند و جای خود را به فناوریهای دیگر دادند، هکرها نیز سیر تکامل و پیشرفت را پشت سر نهادند. گاهی اوقات ما مدافعان امنیتی روی روش خوبی متمرکز میشویم که هکرها در حال مهاجرت به آن هستند.

مطلب پیشنهادی

تقابل سیستمهای سنتی و مدرن

رمزعبور امنتر است یا اثر انگشت؟

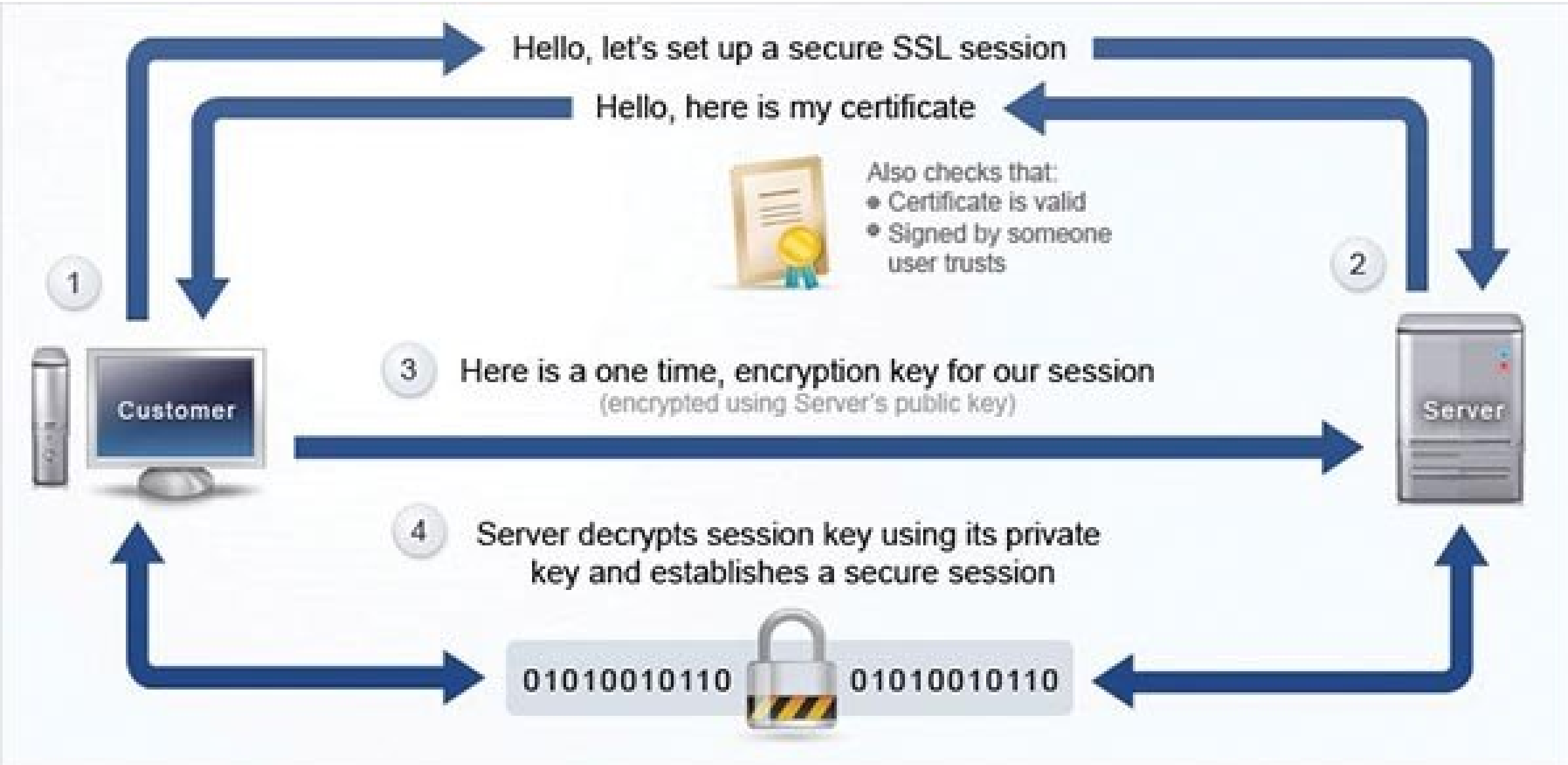
گاهی اوقات ویژگیهای خاص دفاعی حذف میشوند؛ به دلیل اینکه متخصصان تشخیص دادهاند، ویژگی دفاعی آنگونه که باید توانایی محافظت از ما را ندارد، یا ممکن است نقاط ضعف پیشبینی نشدهای، در یک ویژگی امنیتی وجود داشته باشد . اگر شما هم مثل من مدت زمان طولانی در دنیای امنیت کامپیوتری مشغول فعالیت بودهاید، فناوریهای امنیتی بسیاری را مشاهده کردهاید . این همان نقطهای است که شما توانایی پیشبینی آنچه باعث بهبود شده و آنچه دیر یا زود منقرض خواهد شد را درک خواهید کرد؛ هر چند اکنون به نظر میرسد یک تعادل نسبی مابین حملات و فناوریهای دفاعی وجود دارد و روشهایی مانند سیستم احراز هویت و دیوارهای آتش پیشرفته، ممکن است از ما در برابر حملات محافظت کنند؛ اما این فناوریها در نهایت شکست خورده و از بین خواهند رفت . الگویی که امروزه از فناوریهای دفاعی به چشم میآید، بهنظر میرسد به جای آنکه زمینهساز آسایش و راحتی ما باشند، بیشتر کتابهای تاریخ را نشانه رفتهاند .

1: [illegible]

[illegible]

Biometrics
Physiological
Behavioral
face
fingerprint
hand
iris
DNA
keystroke
signature
voice

[illegible]



فیزیکی پیدا کنید؛ در حالیکه ورود بیومتریک به سرعت تبدیل به یک ویژگی امنیتی مرسوم شده است؛ اما دلایل زیادی وجود دارد که آنها نمیتوانند و نخواهند توانست بیهمتا باشند . کافی است تنها یکبار مردم احساس کنند سیستمهای بیومتریک نمیتوانند از عهده آنچه وانمود میکنند برآیند؛ در آن هنگام است که این سیستمها محبوبیت خود را از دست خواهند داد و ناپدید خواهند شد . در آن زمان مردم نیازمند سیستم احراز هویت دومی، خواهند بود که با قابلیت اطمینان بالا بتواند آنها را شناسایی کنند .

فناوریهای محکوم به فنا، شماره 2: SSL

پروتکل امنیتی لایه انتقال (سرنام Secure Socket Layer) اولین بار در سال 1995 توسط نتاسکیپ معرفی شد. (شکل 2) برای نزدیک به دو دهه این فناوری خدمات قابل توجهی به ما عرضه کرد؛ اما ممکن است از این موضوع اطلاع نداشته باشید به لطف حمله Poodle این سیستم شکسته شد و حتی امکان ترمیم آن نیز وجود ندارد . (Poodle سرنام Padding Oracle Downgraded Legacy Encryption است. در حمله پودل که روی پروتکل SSL نسخه 3 انجام میگیرد، نسخهای که 18 سال قدمت دارد، هکرها توانایی گوش کردن به ترافیک رمزنگاری نشده ارتباطات قربانی را دارند . برای آنکه اطلاع پیدا کنید آیا در برابر این حمله ایمن هستید یا خیر، به سایت https://www.poodletest.com مراجعه کنید؛ (اگر سیستم شما در برابر این آسیبپذیری ایمن باشد، پیغام Not vulnerable را مشاهده خواهید کرد، در صورتیکه مرورگر شما آسیبپذیر باشد، تصویر یک سگ پشمالو را مشاهده خواهید کرد .)

Hello, let's set up a secure SSL session
Hello, here is my certificate
Also checks that:
• Certificate is valid
• Signed by someone user trusts
1
2
Customer
Server
3
Here is a one time, encryption key for our session
(encrypted using Server's public key)
4
Server decrypts session key using its private key and establishes a secure session
01010010110
01010010110

لایه انتقال ایمن TLS (سرنام Transport Layer Security) وضع بهتری نسبت به SSL دارد . از تمام فناوریهای محکوم به فنایی که درباره آنها صحبت خواهیم کرد، جایگزینی SSL از همه محتملتر است و نباید بهطور گسترده مورد استفاده قرار گیرد، اما سؤال این است؛ در حالیکه صدها هزار سایت اینترنتی به SSL اعتماد کردهاند یا اجازه استفاده از آن را میدهند، این فناوری چه ایرادی دارد؟ در جواب باید گفت، آسیبپذیریهای موجود در این پروتکل نه تنها شنود ارتباطات کاربران را امکانپذیر میسازند؛ بلکه مرورگرها را مجبور میسازند تا از نسخه 3 پروتکل SSL استفاده کنند . در جدیدترین نسخه عرضه شده از مرورگرها، اگر همه گزینههای مربوط به SSL را غیرفعال کنید، مرورگرها بهطور پیشفرض، سایتهایی که با این پروتکل وابسته بوده و به درستی کار نمیکنند را فهرست میکنند . مرورگرها همچنین سایتهایی که به مرورگر یا برنامه کاربردی اجازه میدهند سطح SSL را به نسخه 3 تنزل دهند را نیز فهرست میکنند؛ حتی اگر صحبت از هیچ سایت یا مرورگری در میان نباشد، هنوز هم میلیونها سرور از پروتکل SSL قدیمی استفاده میکنند؛ اما در نقطه مقابل OpenSSH قرار دارد که این روزها بهنظر میرسد در جایگاه بهتری قرار دارد و در مقابل حملات هکری پایدارتر است . هر چند نیمی از حملات انجام گرفته روی OpenSSH هیچ ارتباطی با SSL ندارند، اما امروزه بیش از نیمی از حسابها، به دلیل آسیبپذیریهای SSL در معرض خطر قرار دارند . میلیونها سایت SSH/OpenSSH هنوز از SSL، استفاده میکنند؛ در حالیکه نباید اینکار را انجام دهند . بدتر آنکه امروزه اصطلاحی در میان حرفهایهای دنیای فناوری باب شده است که خود تبدیل به یک معضل جدی شده است. هر شخصی در صنعت امنیت کامپیوتری گواهی دیجیتالی TLS را گواهی SSL مینامد؛ در حالیکه این گواهیها اصلا از SSL استفاده نمیکنند . این درست مثل این است که ما یک دستگاه کپی را به دلیل اینکه هیچ نام تجاری ندارد، یک

[illegible] (Xerox) [illegible] SSL [illegible] .TLS [illegible] SSL [illegible] TLS [illegible] SSL [illegible].

[illegible] 3: [illegible]

[illegible] RSA، Diffie، Hellman [illegible] ...، [illegible] 3 [illegible].

[illegible] RSA، DiifeHellman [illegible] ECC [illegible] Isogeny [illegible].

:[illegible]
[illegible]

دسته بندی:

امنیت

تاریخ انتشار :

10:22 - 25/10/1394

برچسب:

بیومتریک - ssl - رمزنگاری - تشخیص چهره - اسکنر اثر انگشت

▯▯▯▯▯ منبع: https://www.shabakeh-mag.com/security/2706