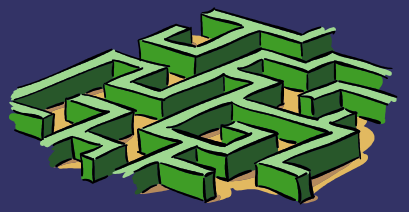
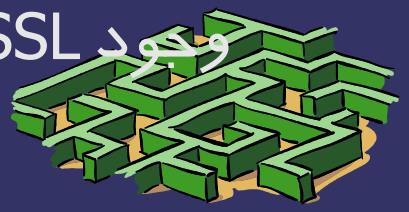
آشنایی با حمله ***MITM*** و راههای مقابله

مهدی عطائیان
http://www.ataeyan.com



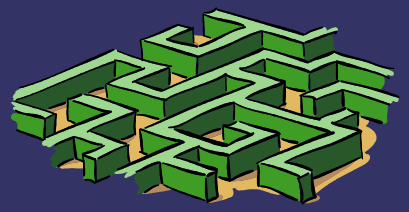
SSL - TLS

- لایهٔ سوکت‌های امن (Secure Sockets Layer) یا اس‌اس‌ال (SSL) پروتکلی است که توسط شرکت Netscape برای ردّ و بدل کردن سندهای خصوصی از طریق اینترنت توسعه یافته است. SSL از یک کلید خصوصی برای به رمز درآوردن اطلاعاتی که بر روی یک ارتباط SSL منتقل می‌شوند استفاده می نماید. طبق آن‌چه در استاندارد آمده است. URLهایی که نیاز به یک ارتباط از نوع SSL دارند با ht-tps به جای http: شروع می‌شوند. SSL یک پروتکل مستقل از لایه برنامه است (Application Independent).بنابراین، پروتکل‌هایی مانند HTTP، FTP و Telnet قابلیت استفاده از آن را دارند. با این وجود SSL برای پروتکل‌های HTTP، FTP و IPSec بهینه شده‌است.

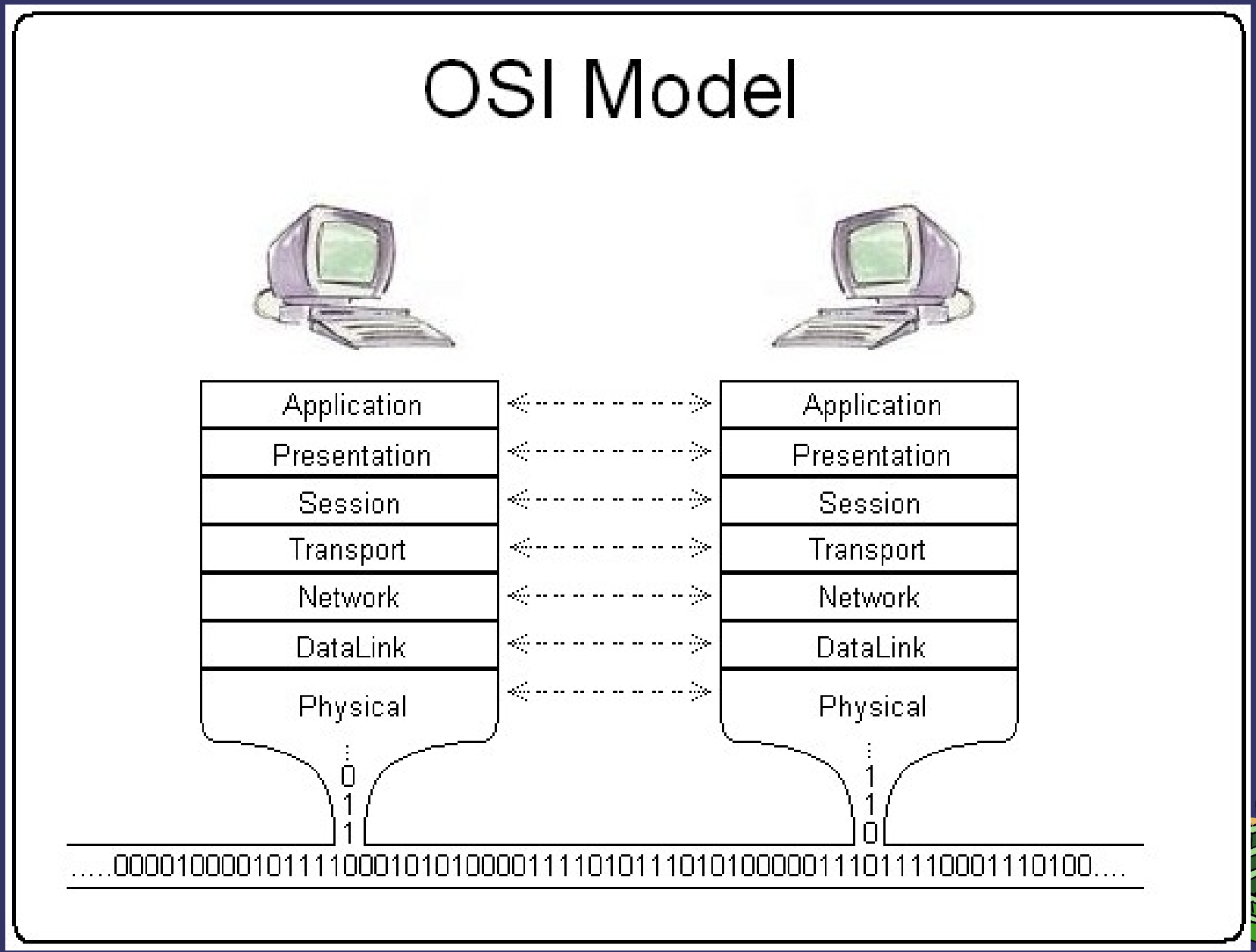


SSL - TLS

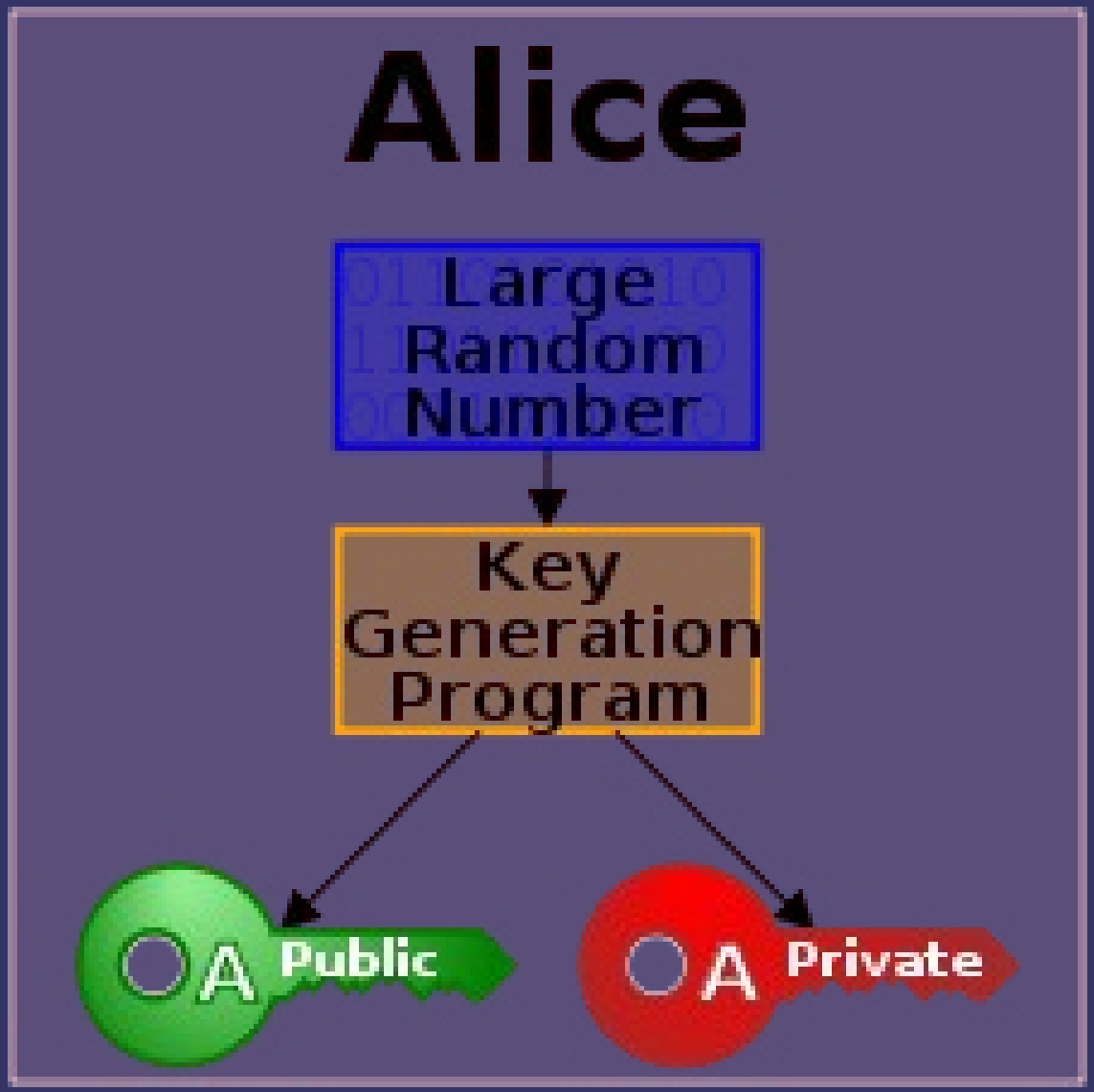
- پروتکل امنیتی لایهٔ انتقال (Transport Layer Security)، بر پایه لایهٔ سوکت‌های امن(Secure Sockets Layer) که یکی از پروتکل‌های رمزنگاری است بنا شده‌است. این پروتکل امنیت انتقال داده‌ها را در اینترنت برای مقاصدی چون کار کردن با پایگاه‌های وب، پست الکترونیکی، نمابرهای اینترنتی و پیام‌های فوری اینترنتی به کار می‌رود. اگرچه TLS و SSL با هم تفاوت‌های اندکی دارند ولی قسمت عمده‌ای از این پروتکل کم و بیش یکسان مانده است.

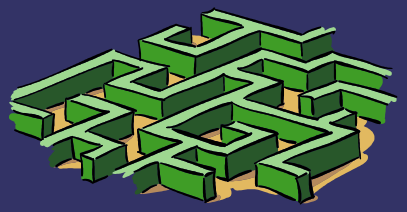


SSL - TLS

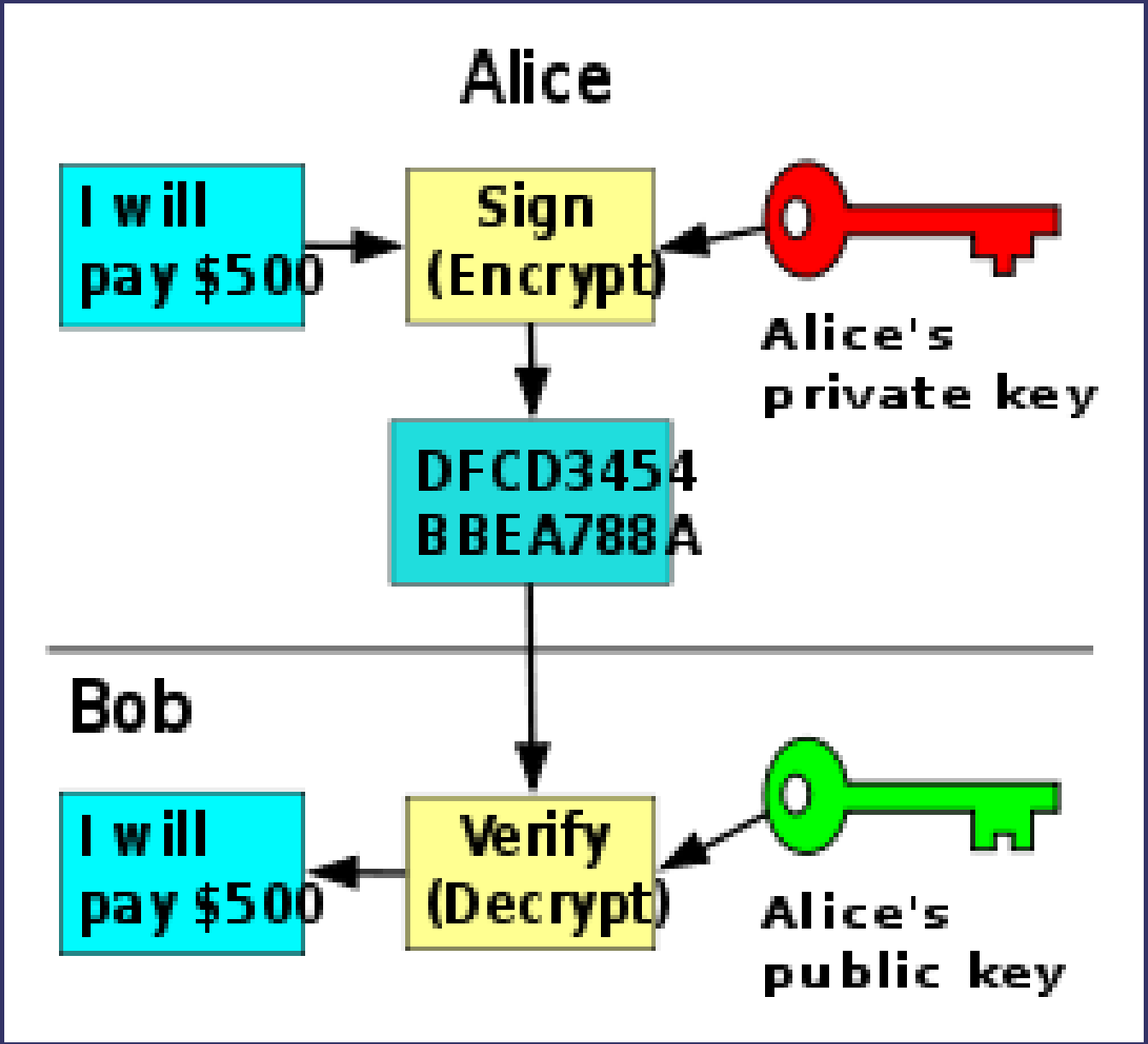

OSI Model
Application
Presentation
Session
Transport
Network
DataLink
Physical
Application
Presentation
Session
Transport
Network
DataLink
Physical
0
1
1
1
1
0
.....00001000010111100010101000011110101110101000001110111100011101000....

الگوریتم رمزنگاری متقارن

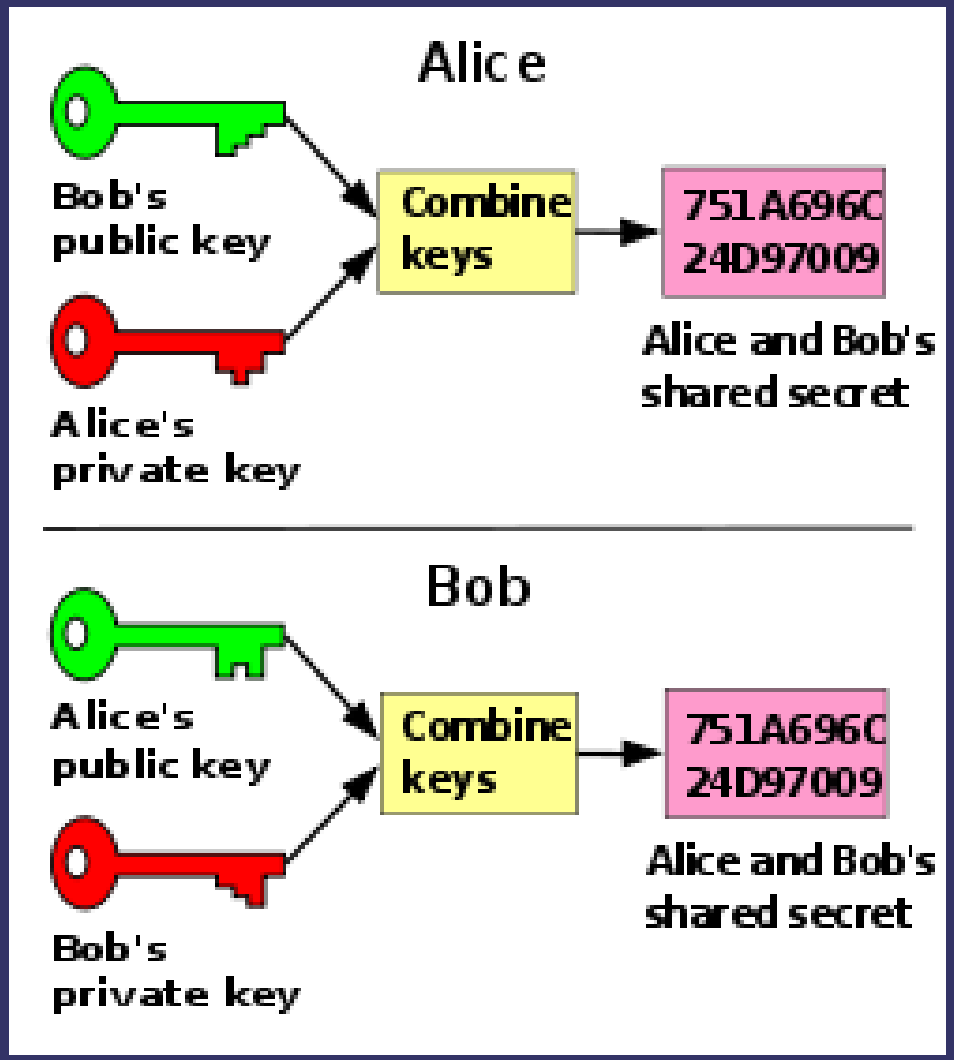


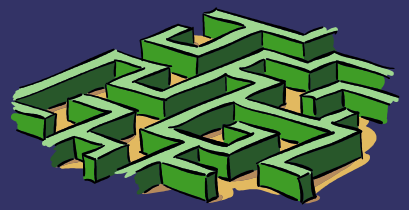


الگوریتم رمزنگاری متقارن



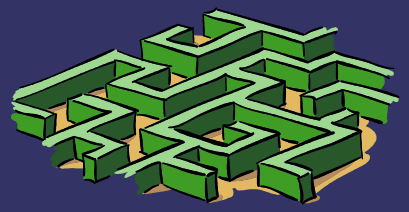
الگوریتم رمزنگاری متقارن



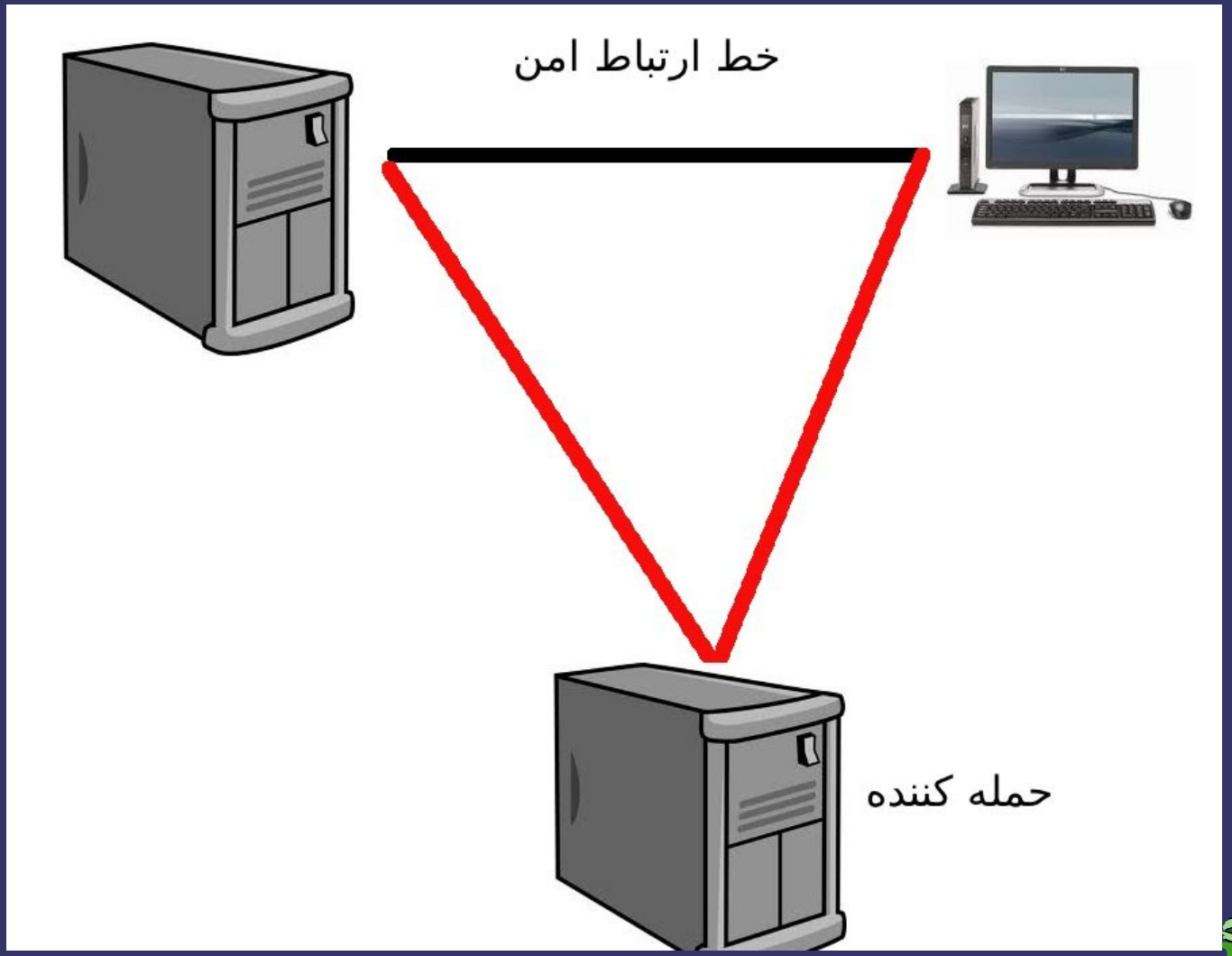


Man-in-the-middle attack

- یک نوع حمله با هدف شنود مکالمات و اطلاعات بین دو نود.
- در این حمله مهاجم بین دو نود قرار میگیرد و مکالمات هر یک از دو طرف را پس از شنود به دیگری می‌دهد.
- در این نوع حمله هر یک از دو نود تصور میکند مستقیما با طرف مقابل مکالمه میکند.
- درصد بالای از حملات MITM در شبکه‌های وای‌فای اتفاق می‌افتد.
- روشهای رمزنگاری پیشرفته می‌تواند مانع حمله MITM شود.

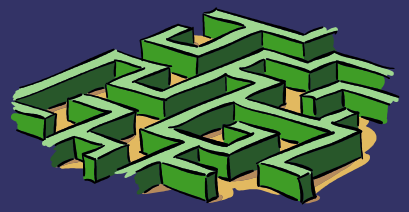


Man-in-the-middle attack



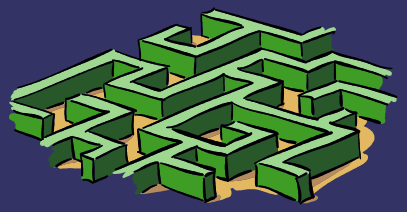
پک مثال از حمله

- ژیلا از پدرام کلید عمومی را میخواهد
- پدرام کلید عمومی را برای ژیلا میفرستد
- مهدی بین راه کلید عمومی پدرام را ذخیره میکند و کلید عمومی خود را برای ژیلا میفرستد.
- ژیلا کلید عمومی را برای پدرام میفرستد
- مهدی بین راه کلید عمومی ژیلا را ذخیره میکند و کلید عمومی خود را برای پدرام میفرستد
-



یک مثال از حمله

- ژیلا پیام «سلام پدرام» که بوسیله کلید خصوصی خود و کلید عمومی مهدی رمز شده را برای پدرام میفرستد.
- مهدی با کلید خصوصی خود و کلید عمومی ژیلا پیام را از رمز خارج میکند و میخواند. و مجددا پیام را با کلید خصوصی خود و کلید عمومی پدرام به مرز میکند و برای پدرام میفرستد و ...
-

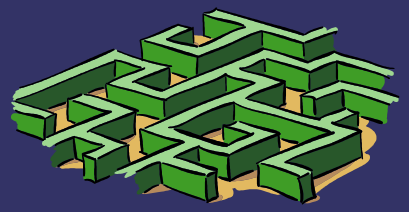


حمله ***mitm*** در عمل

- پراکسی یا خدمات دهنده اینترنت شما که از این پس به نام حمله کننده شناخته می‌شود. یک گواهی امنیتی جعلی گوگل برای خود میسازد.
- حمله کننده با تغییر دی‌ان‌اس یا روشهای دیگر آی‌پی گوگل را به آدرس خودشان تغییر می‌دهند.
- شما پس از ورود به سایت گوگل بر اساس اطلاعات گواهی جعلی گوگل را (حتی با تغییر آی‌پی) به عنوان یک سایت معتبر میشناسید و کلید عمومی جعلی موجود در گواهی امنیتی را به رسمیت می‌شناسید.
- شما اطلاعات و پسورد خود را به سایت میانه (سایت حمله‌کننده میفرستید) و سایت حمله کننده پس از رمزگشایی اطلاعات شما با کلید خصوصی جعلی مجددا اطلاعات را رمز کرده و به سایت گوگل می‌فرستد و ...

CA (Certificate authorities)

- در رمزنگاری بوسیله جفت کلید خطر تغییر کلید عمومی (بوسیله نفر سوم) وجود دارد.
- CAبر اساس اطلاعات طرفین و تاریخ انقضای گواهینامه تعیین هویت می‌کند.
- اطلاعات CA ها در اکثر مرورگرها وجود دارد.



Diginotar

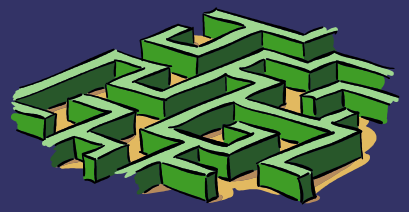
- یک CA هلندی
- در تاریخ ۱۰ام جولای ۲۰۱۱ Diginotar یک گواهی دیجیتال برای سایت گوگل صادر میکند (*.google.com).
- چند آی‌اس‌پی از این گواهی دیجیتال برای حمله MITM استفاده کردند.
- شرکت Vasco ادعا کرده این حمله را در ۱۹ جولای ۲۰۱۱ کشف کرده اما تا زمان حمله این خبر را منتشر نکرده است.
- شرکت چندین گواهی دیگر برای سایتهای Yahoo! و Mozilla و WordPress و Tor Project را لغو کرده است اما هیچ تضمینی برای لغو این گواهی‌ها نمیدهد.

Diginotar

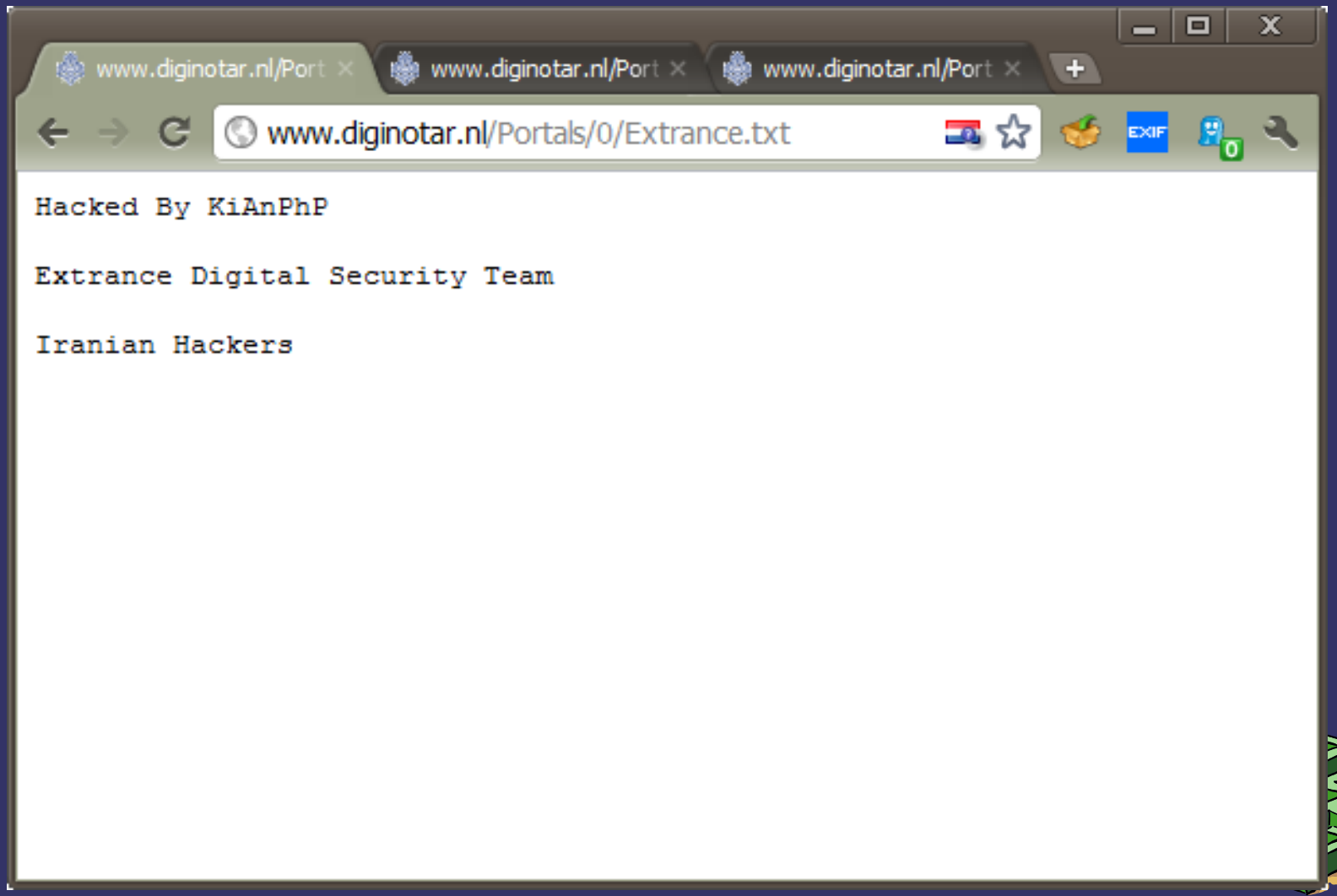
- تحقیق شرکت F-Secure نشان داده سایت Diginotar در سال ۲۰۰۹ بارها بوسیله هکرهای ترکیه و ایران هک شده است. و در زمان نگارش مقاله نیز همچنان نشانه‌هایی از هک در سایت وجود دارد.
- گوگل ۲۴۷ گواهی دیجیتال را در مرورگر کروم بلاک کرد. با اینکه مرورگر کروم قادر به تشخیص گواهی‌های جعلی است اما گوگل diginotar را از لیست CA های مرورگر خوب پاک کرد.
- مایکروسافت diginotar را از لیست CA همه مرورگرهای خود پاک کرد.
- اپرا همیشه لیست CA ها را آنلاین بررسی میکند و بنابراین آسیب‌پذیر نیست.

Diginotar

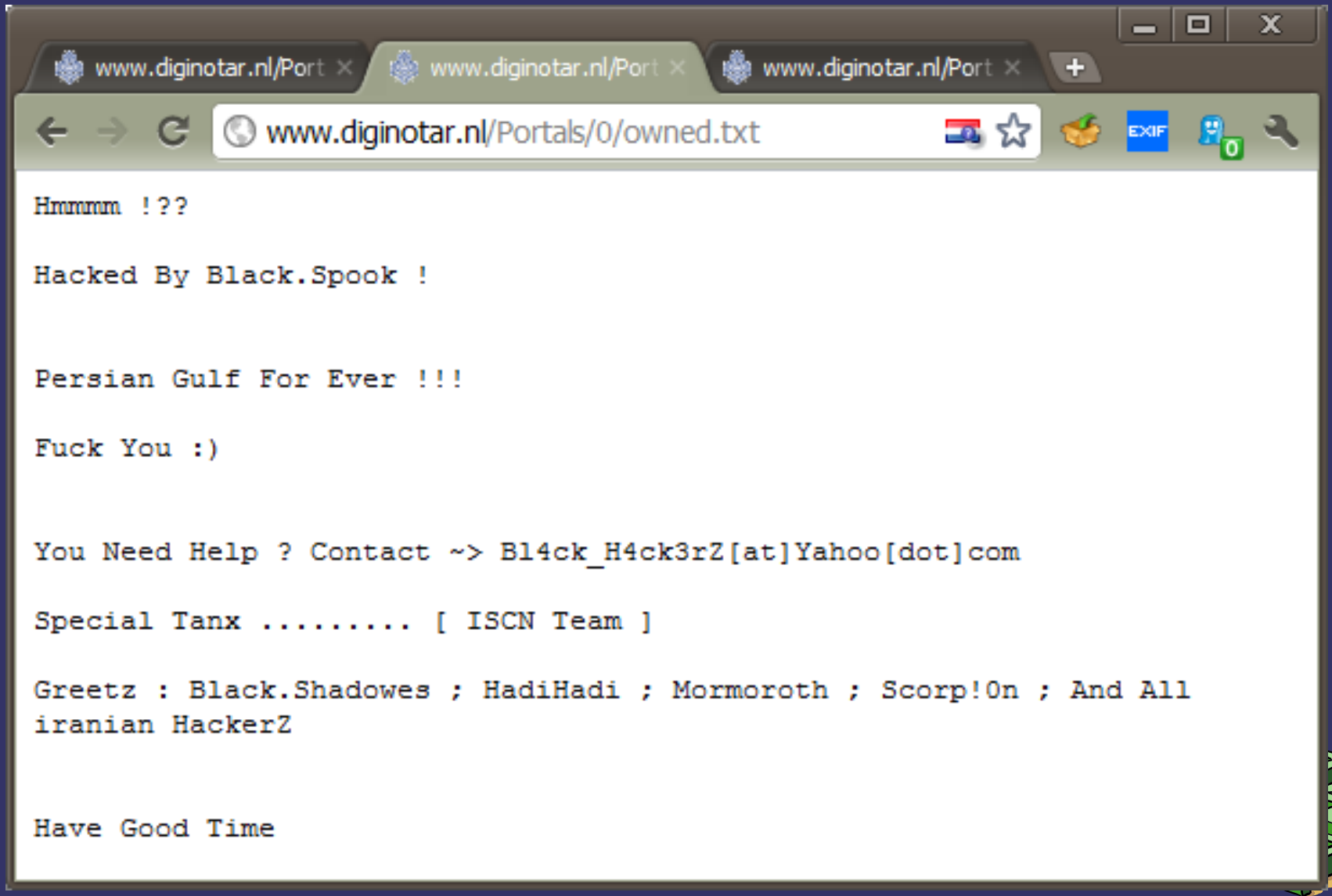
- از آنجا که diginotar مرجع صدور گواهی دیجیتال دولت هلند بوده و پس از حذف این CA عملیات کاری دولت هلند با اشکال مواجه شد بنابراین به درخواست دولت هلند موزیلا مجددا این CA را به مرورگر خود افزود.
- این اتفاق افت شدید ارزش سهام این شرکت را در پی داشت.



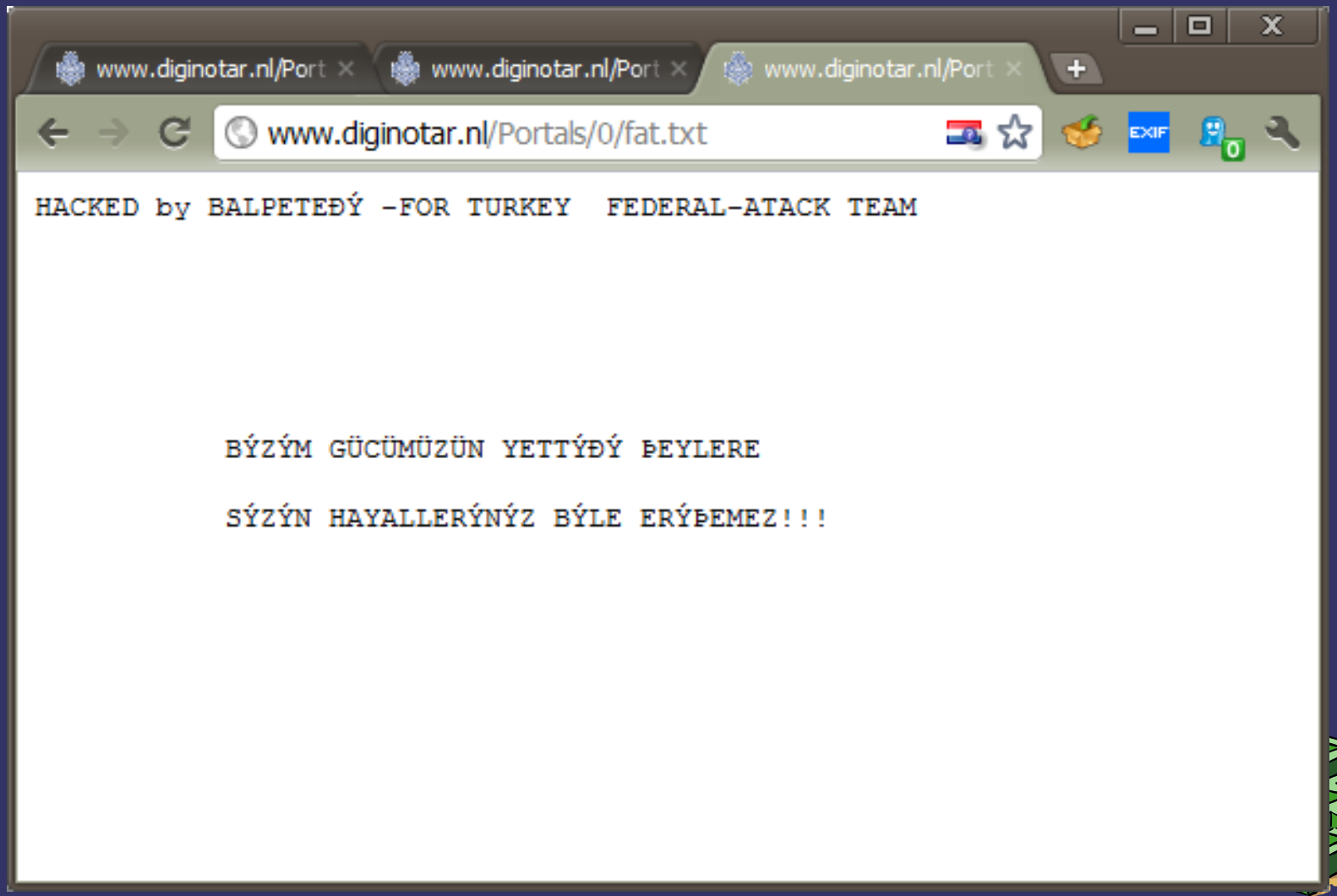
Diginotar


www.diginotar.nl/Port
www.diginotar.nl/Port
www.diginotar.nl/Port
www.diginotar.nl/Portals/0/Extrance.txt
Hacked By KiAnPhP
Extrance Digital Security Team
Iranian Hackers

Diginotar

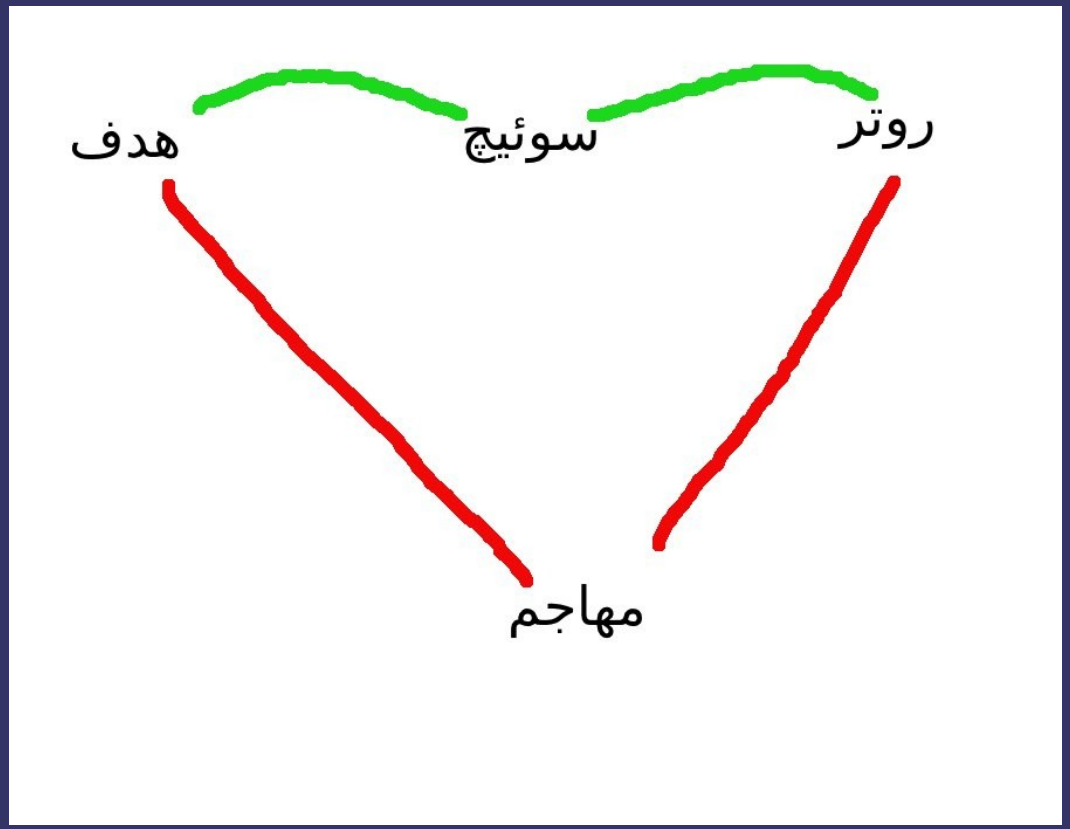

www.diginotar.nl/Port
www.diginotar.nl/Port
www.diginotar.nl/Port
www.diginotar.nl/Portals/0/owned.txt
Hmmmm !??
Hacked By Black.Spook !
Persian Gulf For Ever !!!
Fuck You :)
You Need Help ? Contact ~> Bl4ck_H4ck3rZ[at]Yahoo[dot]com
Special Tanx ..... [ISCN Team]
Greetz : Black.Shadowes ; HadiHadi ; Mormoroth ; Scorp!0n ; And All iranian HackerZ
Have Good Time

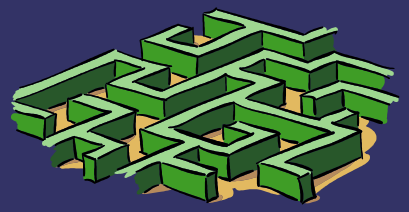
Diginotar


www.diginotar.nl/Port
www.diginotar.nl/Port
www.diginotar.nl/Port
www.diginotar.nl/Portals/0/fat.txt
HACKED by BALPETEĐÝ -FOR TURKEY FEDERAL-ATACK TEAM
BÝZÝM GÜCÜMÜZÜN YETTÝĐÝ ÞEYLERE
SÝZÝN HAYALLERÝNÝZ BÝLE ERÝÞEMEZ!!!

انواع روشهای حمله ***MITM*** روش مسموم کردن حافظه کش ***ARP***

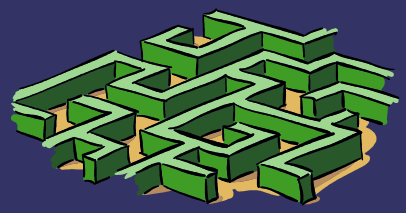
- روش مسموم کردن حافظه کش ARP
- برای پیدا کردن مکان فیزیکی در یک شبکه از ARP استفاده میکنیم.





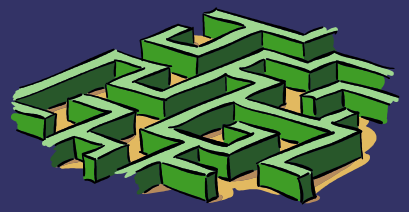
انواع روشهای حمله ***MITM*** روش مسموم کردن حافظه کش ***ARP***

- یک نود درخواست دسترسی به یک نود خاص را می‌دهد
- نود ۱: من نود با آی‌پی ۱.۲.۳.۴ و مک آدرس ۱.۲.۳.۴.۵.۶ یک پیام برای نود با آی‌پی ۵.۶.۷.۸ دارم اما مک نود ۲ را ندارم هر کس اطلاعات این نود را دارد لطفا به من اعلام کند.
- نود ۲: من آی‌پی آدرس ۵.۶.۷.۸ هستم و مک آدرس من ۵.۶.۷.۸.۹. هست.
- روتر شبکه اطلاعات جدول ARP را با اطلاعات جدید آپدیت میکند.
- حمله کننده با فرستادن چند فرستاده بلا عوض ARP خود را به عنوان روتر یا سوئیچ معرفی میکند.



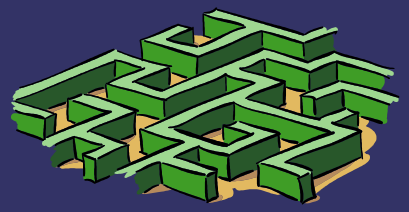
انواع روشهای حمله ***MITM*** حمله با تغییر ***DNS***

- شخص حمله کننده اطلاعات دی‌ان‌اس نادرستی برای قربانی ارسال میکند و قربانی به اشتباه آدرس آی‌پی حمله کننده را باز میکند.
- لطفا از DNSSEC استفاده کنید!
- به هیچ وجه از DNS سرورهای خدمات دهنده استفاده نکند. سرویسهای نام گوگل بهترین راه حل!
- 8.8.4.4 – 8.8.8.8



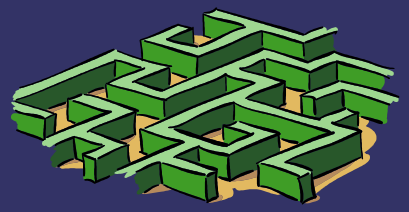
ربودن جلسه (کوکی)

- در این روش بسته‌ها را برای یافتن کوکی شنود میکنیم و سپس با استفاده از کوکی با سرور ارتباط برقرار میکنیم.



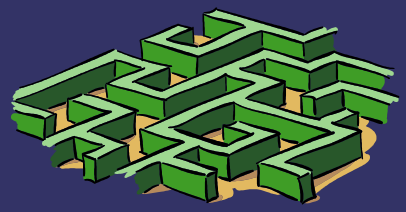
ربودن SSL

- ارتباط‌های امن با کلیک بروی یک لینک ناامن شروع می شود! پی میتوان با تغییر اطلاعات در صفحه ناامن و ارتباط به سایت امن یک حمله MITM ترتیب داد!
- همیشه به آیکون قفل یا آدرس‌بار در مرورگر دقت کنید!



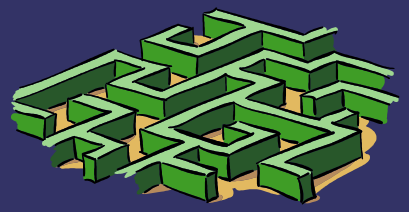
هک CA ها

- حمله‌کننده به یک CA دسترسی پیدا کرده و گواهی جعلی خود را در این سایت وارد میکند.
- حمله کننده با استفاده از این گواهی جعلی و تغییر IP سایت بوسیله دستکاری DNS یک حمله mitm میکند و اطلاعات کاربران را سرقت میکند.
- این حمله تنها بوسیله دولتها قابل انجام است.
- همیشه مرورگرها و نرم‌افزارهای وابسطه به وب خود را به روز کنید.



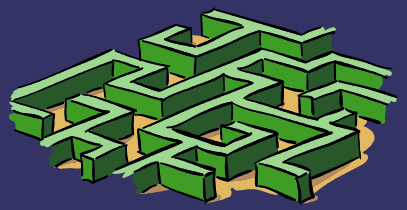
حمله در شبکه‌های ***IPV4***

- حمله MITM در شبکه‌های IPV4: در شبکه‌های بر پایه IPv4 یک هکر میتواند به ارسال درخواست به سیستم‌هایی که IPV6 در آنها فعال است خوب را به عنوان یک روتر جا بزند و حمله MITM را سازماندهی کند.
- در حمله عموما حمله‌کننده درخواست یک اینکریپشن ساده می‌دهد تا منابع کمتری مصرف کند.
-



ابزارهای مفید برای حمله

- http://ettercap.sourceforge.net
- hamster ferret
- TCPDUMP
- WIRESHARK
- sslstrip



منابع

- http://www.eweek.com/c/a/Security/Attackers-Can-
- http://en.wikipedia.org
- http://www.f-secure.com/weblog/archives/0000222
- ویکی‌پدیا فارسی اس‌اس‌ال
- http://en.wikipedia.org/wiki/DigiNotar
- http://en.wikipedia.org/wiki/Osi_layer
- http://en.wikipedia.org/wiki/Cryptography
- http://en.wikipedia.org/wiki/Certificate_authority