دوره اصول کاربری امن رایانه

CERTIFIED SECURE COMPUTER USER (CSCU) | EC-COUNCIL

دکتر رضا ابراهیمی آتانی

دانشیار گروه مهندسی کامپیوتر و مدیر مرکز آپای دانشگاه گیلان

رایانامه: cert@guilan.ac.ir

تلفن/ فکس: ۳۳۳۴۱۹۵۲-۰۱۳ همراه مرکز: ۰۹۳۷۷۳۶۹۹۳۵

- در صورت علاقه مندی به **عضویت در خبرنامه مرکز آپای دانشگاه گیلان** و دریافت آخرین راه حل های امنیتی یک ایمیل بلانک با عنوان درخواست عضویت به **cert@guilan.ac.ir** ارسال فرمایید. یا آدرس ایمیل خودتان را به شماره ۰۹۳۷۷۳۶۹۹۳۵ پیامک بزنید.
- شما می توانید آپای گیلان را در شبکه های اجتماعی هم دنبال نمایید.
- گروه آپا گیلان در شبکه اجتماعی بله **ble.ir/join/NjQwY2Q2MD**

- شماره همراه مرکز آپا نیز ۰۹۳۷۷۳۶۹۹۳۵

فهرست مطالب

- اهمیت امنیت اطلاعات و پدافند عامل در سازمان ها
- فرآیند پدافند سایبری مبتنی بر خود ارزیابی امنیتی زیر ساخت های سازمانی
- جمع آوری اطلاعات و پویش سرویس ها و زیر ساخت های سازمانی
- امنیت در لایه IP
- امنیت در لایه انتقال
- بررسی چالش های امنیتی خدمات SSL/TLS
- معرفی ابزار های رایگان ارزیابی امنیتی خدمات SSL/TLS
- جمع بندی بحث و آشنایی با خدمات اختصاصی مرکز آپا
- معرفی همایش ملی پدافند الکترونیکی و دفاع سایبری

اهمیت امنیت اطلاعات سازمان ها

- گسترش استفاده از ارتباطات و فناوری اطلاعات در خدمت های سازمانی
- افزایش تهدیدات و حملات به خدمات و زیر ساخت های شبکه
- لزوم توجه به مقوله امنیت از دیدگاه سازمانی و مدیریتی

اهمیت امنیت اطلاعات سازمان ها

- اطلاعات سازمانی نیازمند به محرمانگی
- اهمیت توانمند سازی نیروی انسانی سازمان ها برای افزایش امنیت

سرویس‌های امنیتی در سازمان ها

- حفظ صحت داده (Integrity)
- حفظ محرمانگی داده‌ها (Confidentiality)
- هویت شناسی، احراز هویت (Authentication)
- کنترل دسترسی (Access Control)
- عدم‌انکار (Non-repudiation)
- دسترسی پذیری (Availability)

انواع و ماهیت حملات

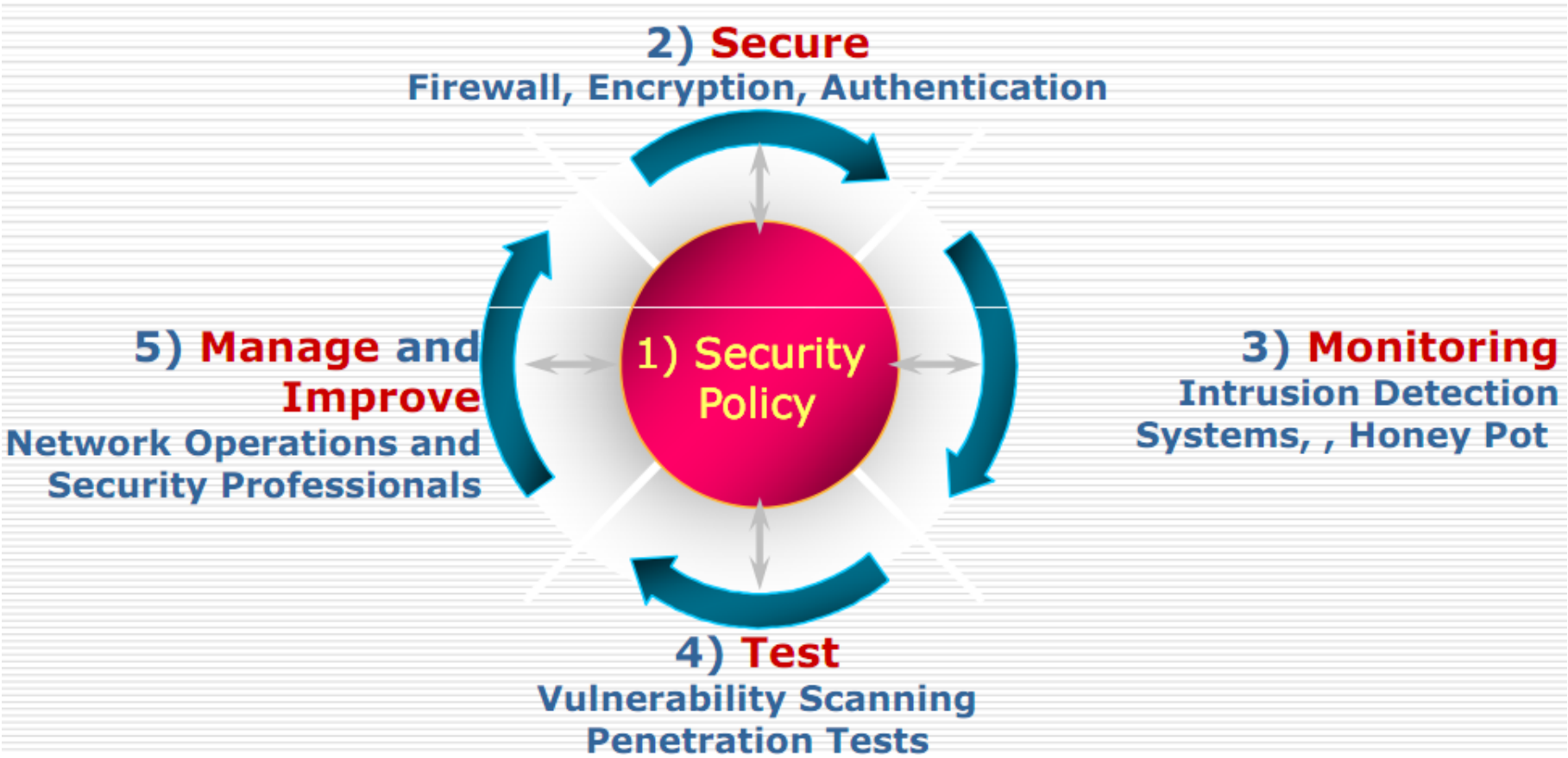
- انواع حملات بر حسب نتیجه
  - وقفه (Interruption): اختلال در شبکه و سرویس
  - شنود (Interception): استراق سمع ارتباطات شخصی یا مخفی سایرین
  - دستکاری داده‌ها (Modification): تغییر غیرمجاز داده‌های سیستم یا شبکه
  - جعل اطلاعات (Fabrication): ارسال داده توسط کاربران غیرمجاز با نام کاربران مجاز

انواع حملات

انواع حملات از نظر تاثیر در ارتباط:

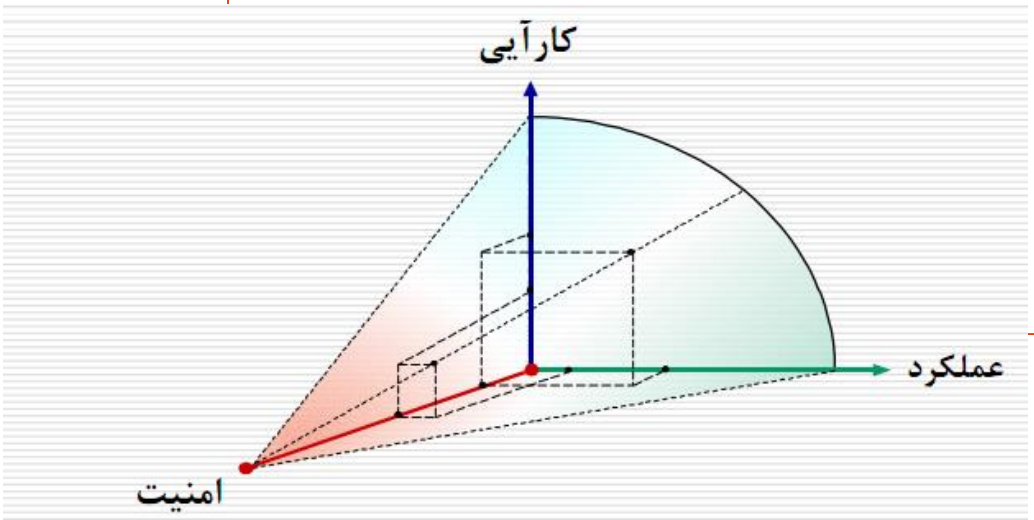
- **حملات غیرفعال (Passive)**
  - شنود
  - افشاء پیام (release of message content)
  - استراق سمع (Eavesdropping)
- **حملات فعال (Active)**
  - جعل هویت (Masquerade)
  - ارسال دوباره پیغام (Replay)
  - تغییر(Modification of message)
  - منع سرویس(Denial of Service – DoS)

حلقه پایان‌ناپذیر چرخه ایجاد امنیت



استراتژی های امنیت سازمانی

- مصالحه بین امنیت، کارآیی و عملکرد
- میزان امنیت مورد انتظار کاربران؟
- میزان ناامنی قابل تحمل سازمان؟



پدافند عامل در سازمان ها

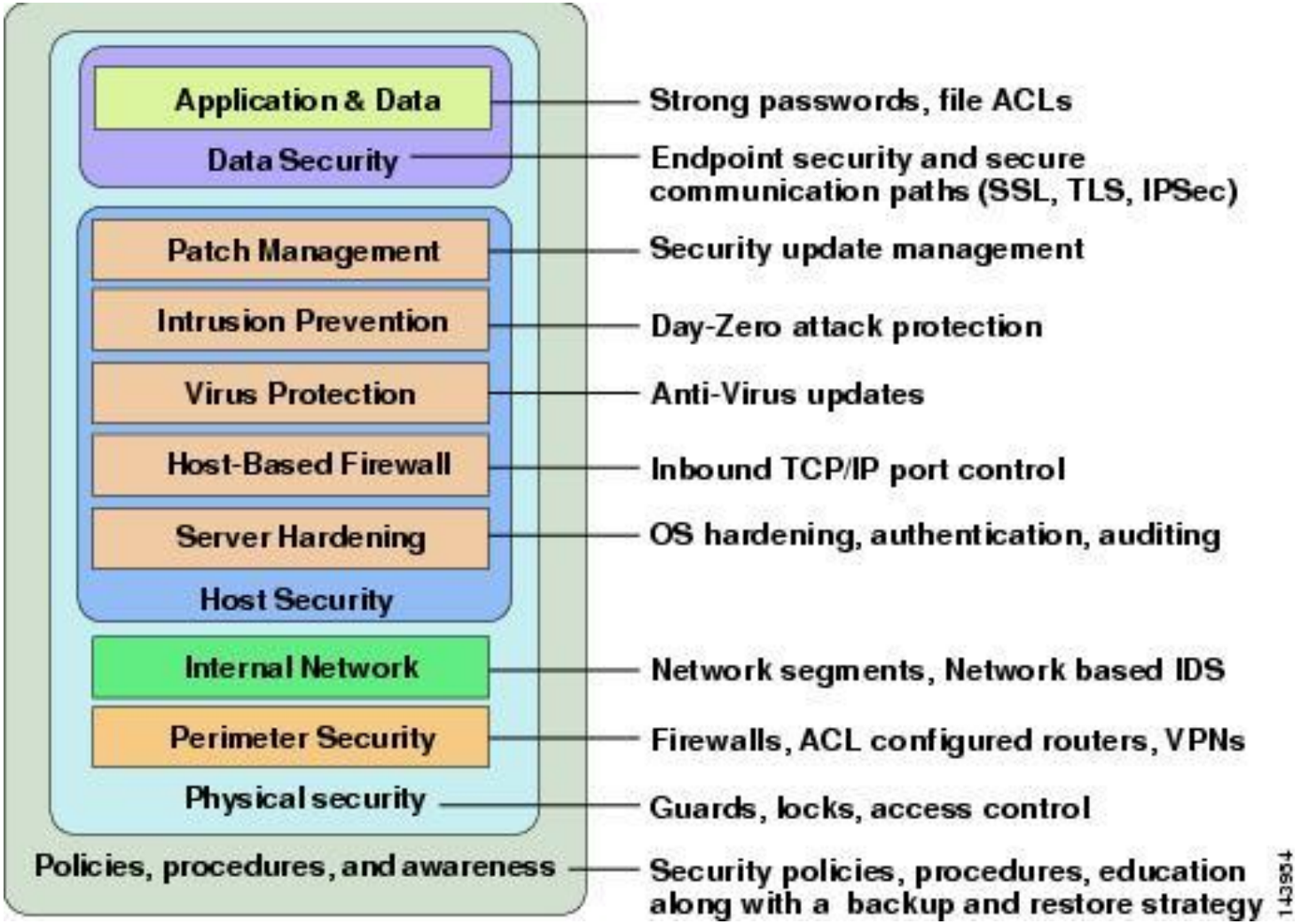
پدافند عامل سایبری: اقداماتی در جریان حمله یا قبل از حمله دشمن که می‌تواند موجب بهبود تشخیص، جلوگیری و پاسخگویی به حملات سایبری دشمن شود.

پدافند غیرعامل سایبری: کاهش ضرر و زیان خسارات ناشی از حملات سایبری است.

فرآیند پدافند سایبری مبتنی بر خود ارزیابی امنیتی زیر ساخت های سازمانی

- وجود متخصص با انگیزه و متعهد در سازمان ها
- آشنایی با معماری شبکه و خدمات سازمان
- ارتقای مهارت های کارشناسان و مدیران فناوری اطلاعات سازمان در شناخت آسیب پذیری ها
  - شناسایی
  - امن سازی
  - آشنایی اولیه با چرخه های ایجاد امنیت فیزیکی و امن نرم

فرآیند پدافند سایبری مبتنی بر خود ارزیابی امنیتی زیر ساخت های سازمانی



مهارت‌های مرتبط با آسیب پذیری ها

- **شناخت فنی آسیب پذیری**
  - چرا آسیب پذیری ایجاد می شود؟
  - چه اثری دارد؟
  - چگونه مورد سو استفاده قرار می گیرد؟
- **چگونه وجود آسیب پذیری را تشخیص دهیم؟**
- **چگونه آسیب پذیری را از بین ببریم؟**
  - وصله امنیتی (آسان)
  - تغییر معماری شبکه (سخت)
  - کدنویسی (سخت)

شناخت آسیب پذیری ها

- از کجا شروع کنیم؟
  - آسیب پذیری های در سطح سیستم عامل؟
  - آسیب پذیری های در سطح شبکه؟
  - آسیب پذیری های در سطح برنامه های کاربردی؟
- ریسک
  - کجا آسیب پذیری محتمل تر است؟
  - کجا وجود آسیب پذیری اثر تخریبی بیشتری دارد؟

روش‌های تامین امنیت سازمانی

عبارتند از:

- دفاع در عمق
- پیاده سازی راه حل های پیشگیرانه
- پیاده سازی راه حل های تشخیص
- پیاده سازی راه حل های ترمیم و پشتیبانی

جمع آوری اطلاعات و پویش سرویس ها و زیر ساخت های سازمانی

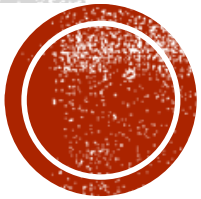
مراحل اصلی خودارزیابی امنیتی سازمانی

- جمع آوری اطلاعات اولیه
- پویش های محلی یا سیستمی سازمانی
- اعمال تست های نفوذ یا برگزاری مانور های حمله
- جمع آوری داده هاو تحلیل
- دسته بندی نتایج و حل منافذ رخنه
- ارتقا دانش کارکنان و برگزاری کلاس های آموزشی و توجیهی

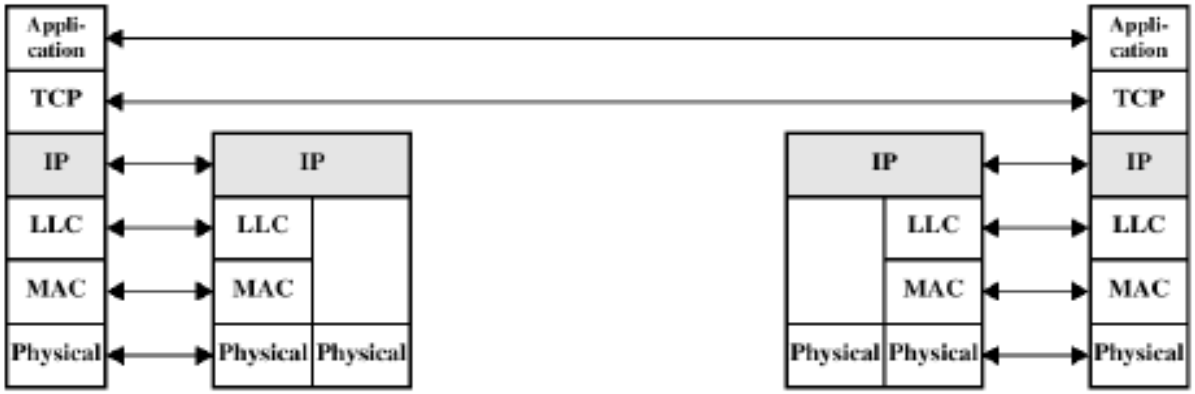
جمع آوری اطلاعات و پویش سرویس ها و زیر ساخت های سازمانی

Phase 1: Foot printing	Phase 2: Scanning	Phase 3: Enumeration
IP address ranges Namespaces Employee information Phone numbers Facility information Job information	Pings Ping sweeps Port scans Tracert	Usernames Group information Passwords Hidden shares Device information Network layout Protocol information Server data Service information

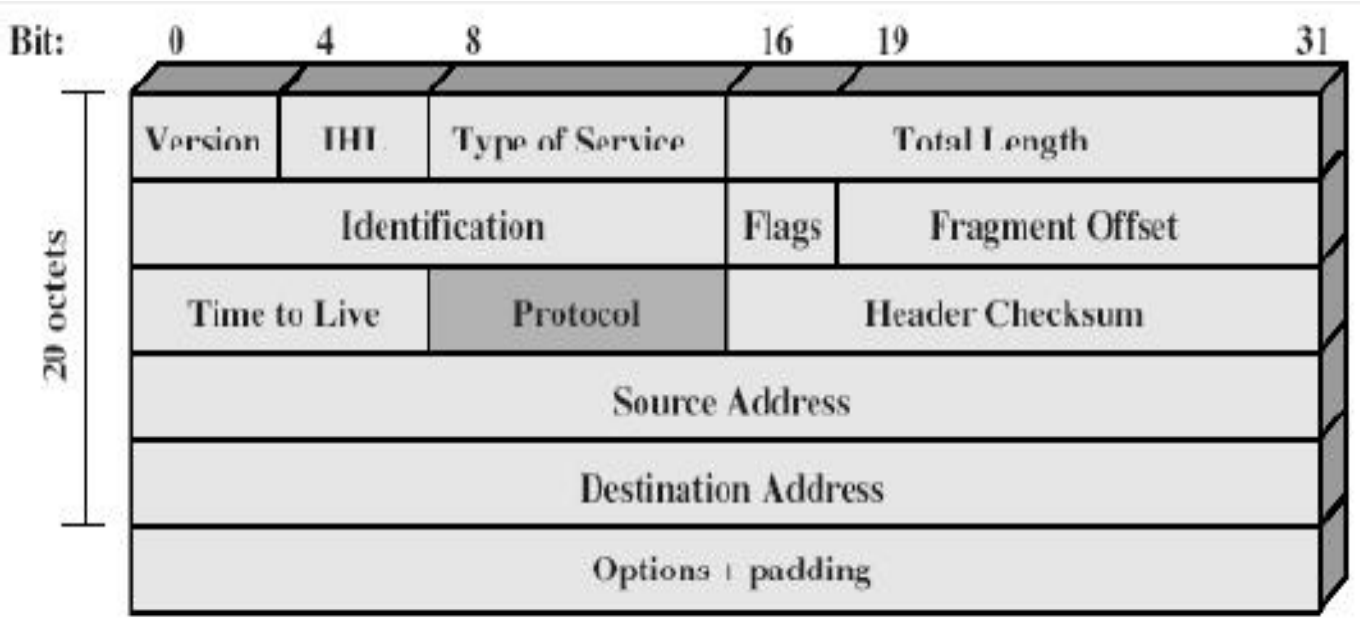
امنیت در لایه IP



مقدمه – مثالی از TCP/IP



IPV4


Bit:
0
4
8
16
19
31
Version
IHL
Type of Service
Total Length
Identification
Flags
Fragment Offset
Time to Live
Protocol
Header Checksum
Source Address
Destination Address
Options + padding
20 octets

مقدمه

- راه حل های امنیتی وابسته به کاربرد (تاکنون)
  - S/MIME و PGP: امنیت پست الکترونیکی
  - Kerberos: امنیت بین کاربر-کارگزار (احراز اصالت)
  - SSL: ایجاد یک کانال امن در وب
- نیاز به امنیت در سطح IP
  - محرمانگی محتوای بسته های IP
  - احراز اصالت فرستنده و گیرنده بسته ها

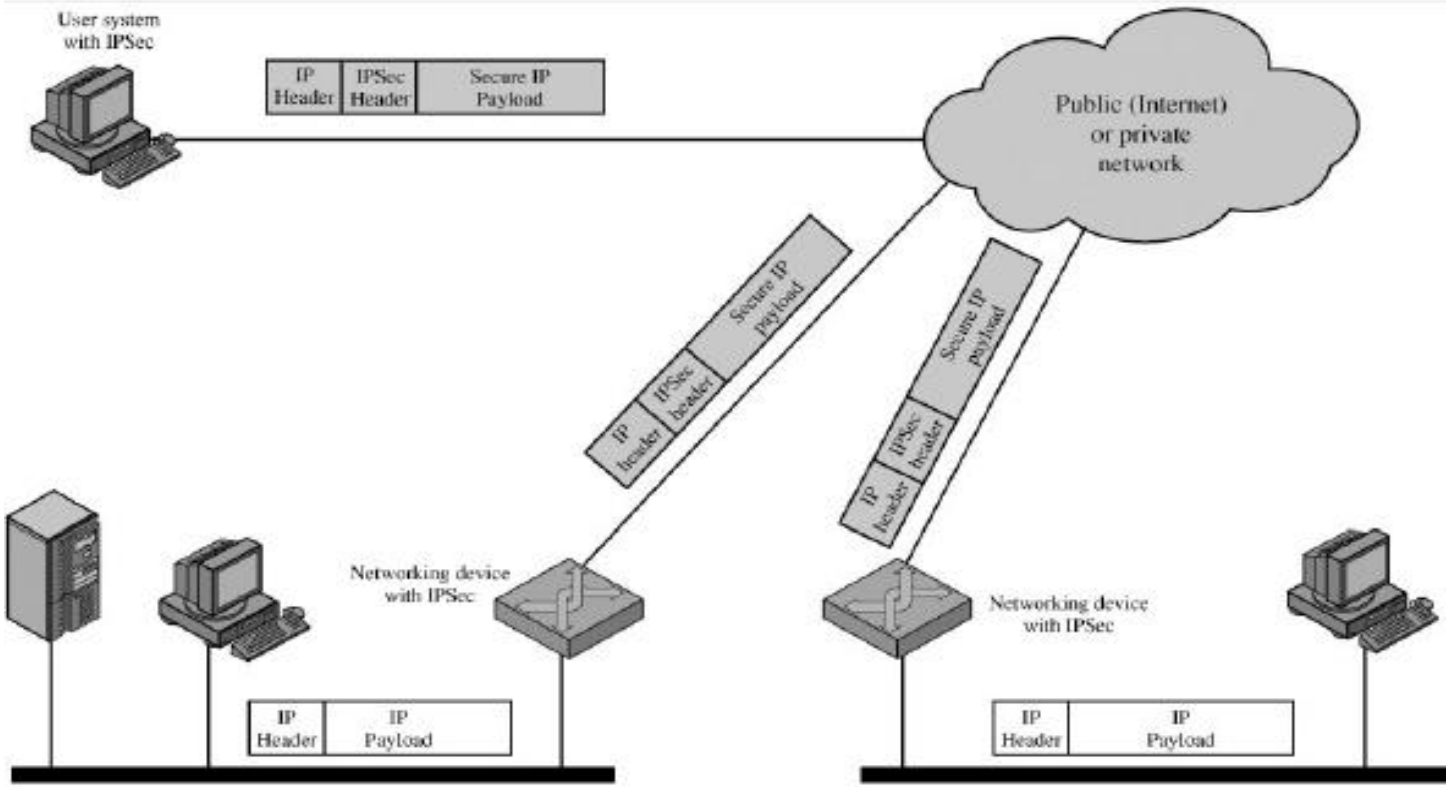
مقدمه

- IPSec یک پروتکل تنها نیست بلکه مجموعه ای از الگوریتم های امنیتی است که چارچوبی کلی را برای برقراری یک ارتباط امن فراهم می نماید.
- سرویس های امنیتی فراهم شده توسط IPSec
  - احراز اصالت (به همراه کنترل صحت داده ها)
  - محرمانگی بسته ها
  - مدیریت کلید (تبادل امن کلید)

کاربرد IPSec

- نمونه کاربردهای IPSec
  - ایجاد شبکه خصوصی مجازی (VPN) برای شعبه های مختلف یک سازمان از طریق اینترنت
  - دسترسی امن کارمندان شرکت به منابع شبکه از طریق اینترنت
  - امکان ارتباط امن بین چند سازمان
  - به وجود آوردن خدمات امنیتی برای کاربردهای دیگر (مثل تجارت الکترونیکی)

نمونه ای از کاربرد IPSec



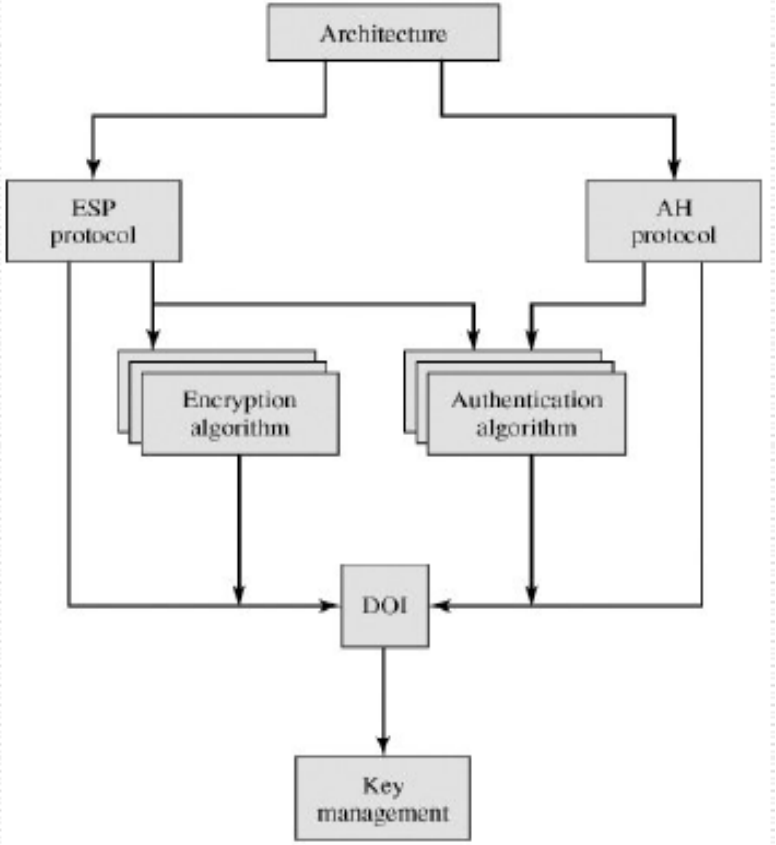
مقدمه

- مزایای استفاده از IPSec
  - تامین امنیت قوی بین داخل و خارج LAN در صورت بکارگیری در مسیریاب ها و حفاظ ها (Firewallها)
    - عدم سربار رمزنگاری در نقاط انتهایی
  - پنهانی از نظر کاربران
  - پنهانی از دید برنامه های کاربردی لایه های بالاتر (IPSec زیر لایه انتقال عمل می نماید)
  - ایجاد ارتباط امن بین کارکنان سازمان از خارج به داخل

ویژگیهای IPSec

- دارای توصیف نسبتا مشکل
- الزامی در IPv6 و اختیاری درIPv4
- پروتکل IPSec در سرآیندهای توسعه یافته و بعد از سرآیند اصلیIP پیاده سازی می شود.
- مستندات IPSec بسیار حجیم بوده و به صورت زیر دسته بندی شده است:
  - معماری (Architecture)
  - (ESP) Encapsulating Security Payload : رمزنگاری بسته ها (احراز اصالت به صورت اختیاری)
  - (AH) Authentication Header : احراز اصالت بسته ها
  - مدیریت کلید: تبادل امن کلیدها
  - الگوریتم های رمزنگاری و احراز اصالت

ساختار مستندات IPSec



سرویس های IPSec

- سرویسهای ارائه شده:
  - کنترل دسترسی
  - تضمین صحت داده ها در ارتباط Connectionless
  - احراز اصالت منبع داده ها (Data Origin)
  - تشخیص بسته های بازارسال شده و رد آنها (مقابله با حملات تکرار)
  - محرمانگی بسته ها
  - محرمانگی جریان ترافیک

سرویس های IPSec

- همه سرویس ها با دو پروتکل زیر ارائه می شوند:
  - Authentication Header (AH)
  - Encapsulating Security Payload (ESP)

ESP (encryption plus authentication)	ESP (encryption only)	AH	
✓	✓	✓	کنترل دسترسی
✓		✓	صحت connectionless
✓		✓	احراز اصالت منبع داده
✓	✓	✓	رد بسته‌های بازارسال شده
✓	✓		محرمانگی بسته‌ها
✓	✓		محرمانگی جریان ترافیک

مجمع امنیتی

- **تعریف:** مجمع امنیتی(Security Association) یک مفهوم کلیدی در مکانیزم های احراز اصالت و محرمانگی برای IP بوده و یک رابطه یک طرفه بین فرستنده و گیرنده بسته ایجاد می کند.

- SA در IP به نوعی معادل Connection در TCP است.

مجمع امنیتی

- **ویژگیها:**
- یک SA بصورت یکتا با ۳ پارامتر مشخص می شود:
  - Security Parameters Index (SPI): یک رشته بیتی نسبت داده شده به SA
  - IP Destination Address: آدرس مقصد نهایی SA
  - Security Protocol Identifier: بیانگر تعلق SA به AH یا ESP

مجمع امنیتی

- **پارامترهای SA**
  - Sequence Number Counter: شماره سریال بسته ها
  - Sequence Counter Overflow: نشانگر سرریز در شمارنده
  - Anti Replay Window: استفاده برای مشخص کردن تکراری بودن بسته دریافتی
  - AH Information: الگوریتم احراز اصالت، کلیدها و طول عمر آنها و ...
  - ESP Information: الگوریتم رمز و احراز اصالت، کلیدها و طول عمر آنها، مقادیر اولیه و ...
  - SA Lifetime:طول عمر SA
  - IPSec Protocol Mode: یک از مدهای انتقال و تونل
  - Maximum Transmission Unit: هرگونه مقدار MTU (حداکثر واحد قابل انتقال) مشاهده شده در مسیر

مدهای انتقال بسته در IPSec

- در هر دوی AH و ESP دو مد انتقال وجود دارد:
  - مد انتقال (Transport Mode)
    - تغییرات تنها روی محتوای بسته صورت می گیرد، بدون تغییر سرآیند IP
  - مد تونل (Tunnel Mode)
    - اعمال تغییرات روی کل بسته IP (سرآیند + Payload) و فرستادن نتیجه به عنوان یک بسته جدید

مد انتقال در IPSec

- **مد انتقال**
  - در کاربردهای انتها به انتها (end-to-end) مثل کارگزار/کارفرما استفاده می شود.
  - ESP : رمزنگاری (ضروری) و صحت (اختیاری) محتوای بسته
  - AH : صحت محتوای بسته و قسمتهای انتخاب شده سرآیند بسته

مد تونل در IPSec

- **مد تونل**
  - مورد استفاده در ارتباط Gateway به Gateway.
  - هیچ مسیریاب (router) میانی قادر به تشخیص سرآیند داخلی نیست.

قابلیت های مدهای انتقال و تونل

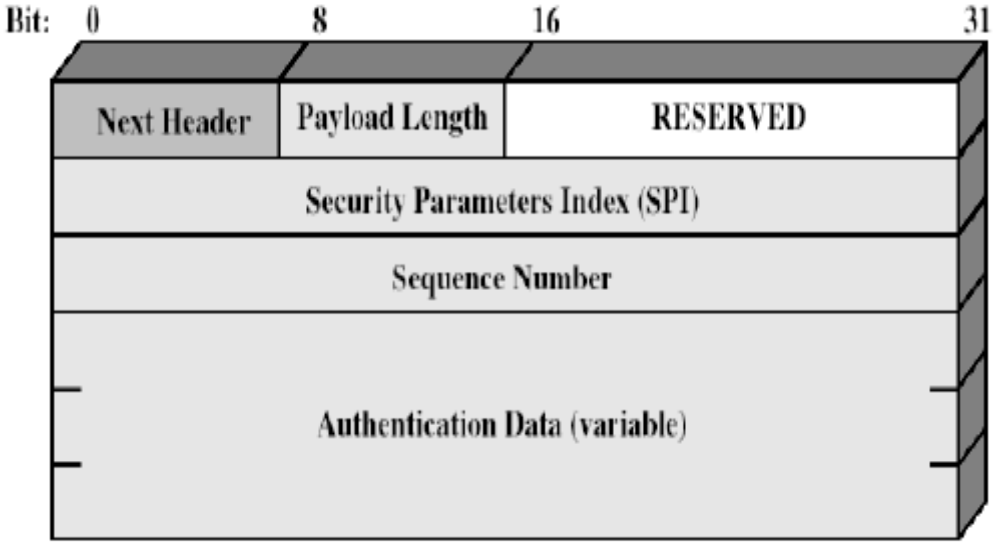
	مُد انتقال	مُد تونل
AH	احراز بخش داده‌ای IP و بخشهایی از سرآیند IP	احراز اصالت کل بسته IP داخلی به انضمام بخشهایی از سرآیند IP بسته بیرونی
ESP	رمز بخش داده‌ای IP که به دنبال سرآیند ESP قرار دارد.	رمز کل بسته IP داخلی
ESP with Authentication	رمز بخش داده‌ای IP که به دنبال سرآیند ESP قرار دارد. احراز اصالت بخش داده‌ای IP و نه سرآیند آن.	رمز کل بسته IP داخلی. احراز اصالت بسته IP داخلی

Authentication Header (AH)

- Authentication Header
  - تضمین صحت و احراز اصالت بسته های IP
  - تامین سرویس صحت داده ها با استفاده از MAC
    - HMAC-MD5-96 یا HMAC-SHA-1-96
  - به مقدار فیلد MAC در AH، مقدار کنترل صحت (ICV) گفته می شود.

  - طرفین نیاز به توافق روی یک کلید مشترک متقارن دارند.

Authentication Header (AH)



Authentication Header (AH)

- **فیلدهای AH:**
  - Next Header (۸ بیت): نوع سرآیند بعدی موجود در بسته
  - PayLoad Length (۸بیت) : بیانگر طول AH (با واحد کلمه۳۲ بیتی) منهای۲
  - Reserved (۱۶بیت) : رزرو شده برای استفاده های آینده
  - Sec. Param. Index (۳۲بیت) : برای تعیین SPI مربوط به SA
  - Sequence Number (۳۲ بیت) : شمارنده
  - Authentication Data (متغیر): دربرگیرنده MAC یا ICV (Integrity Check Value)

Authentication Header (AH)

- **محاسبه MAC**
  - طول پیش فرض ۹۶ بیت (۳ تا ۳۲ بیتی)
    - اولین ۹۶ بیت خروجی الگوریتم HMAC
    - HMAC-MD5 یا HMAC-SHA-1
  - محاسبه MAC روی مقادیر زیر انجام می گیرد:
    - سرآیند نامتغیر IP، سرآیند نامتغیر AH و محتوای بسته
  - قسمتهایی از سرآیند که احتمالا در انتقال تغییر می کنند (مانند TTL)، در محاسبه MAC صفر منظور می شوند.
  - آدرسهای فرستنده و گیرنده نیز در محاسبه MAC دخیل هستند (جهت جلوگیری از حمله جعلIP)

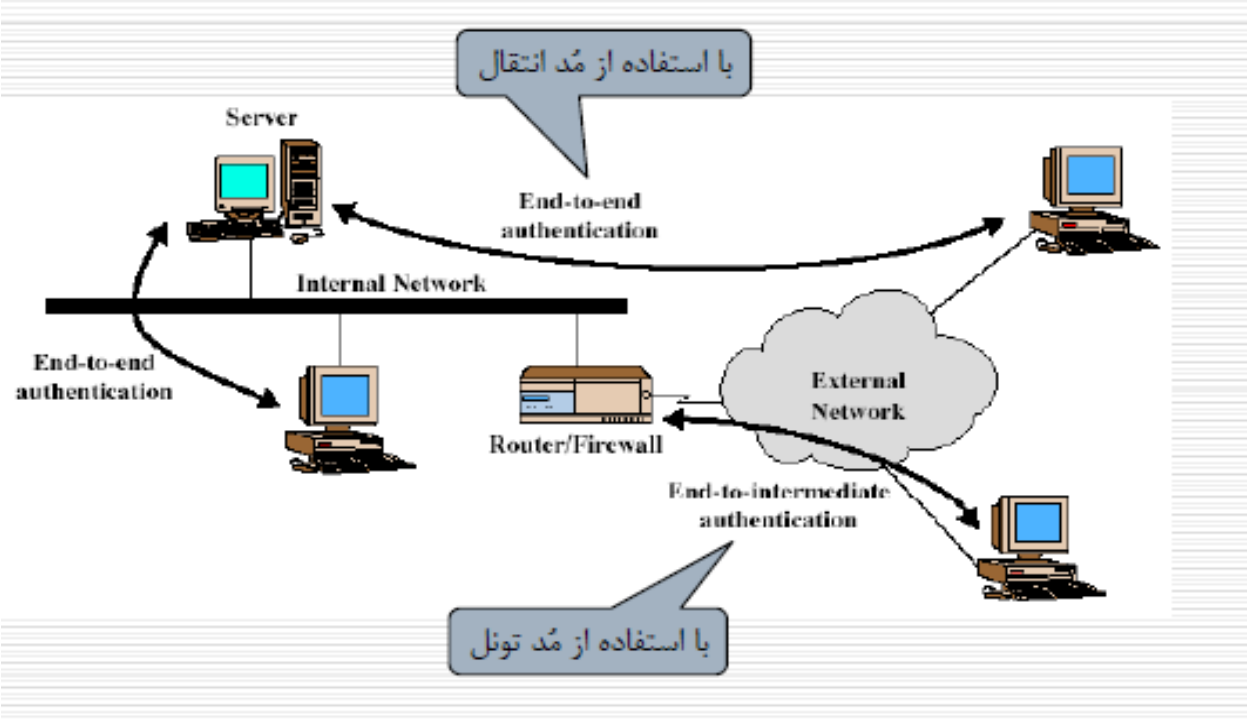
Authentication Header (AH)

- مدهای انتقال و تونل در AH:

- مد انتقال (Transport): برای احراز اصالت مستقیم بین کامپیوتر کاربر و کارگزار

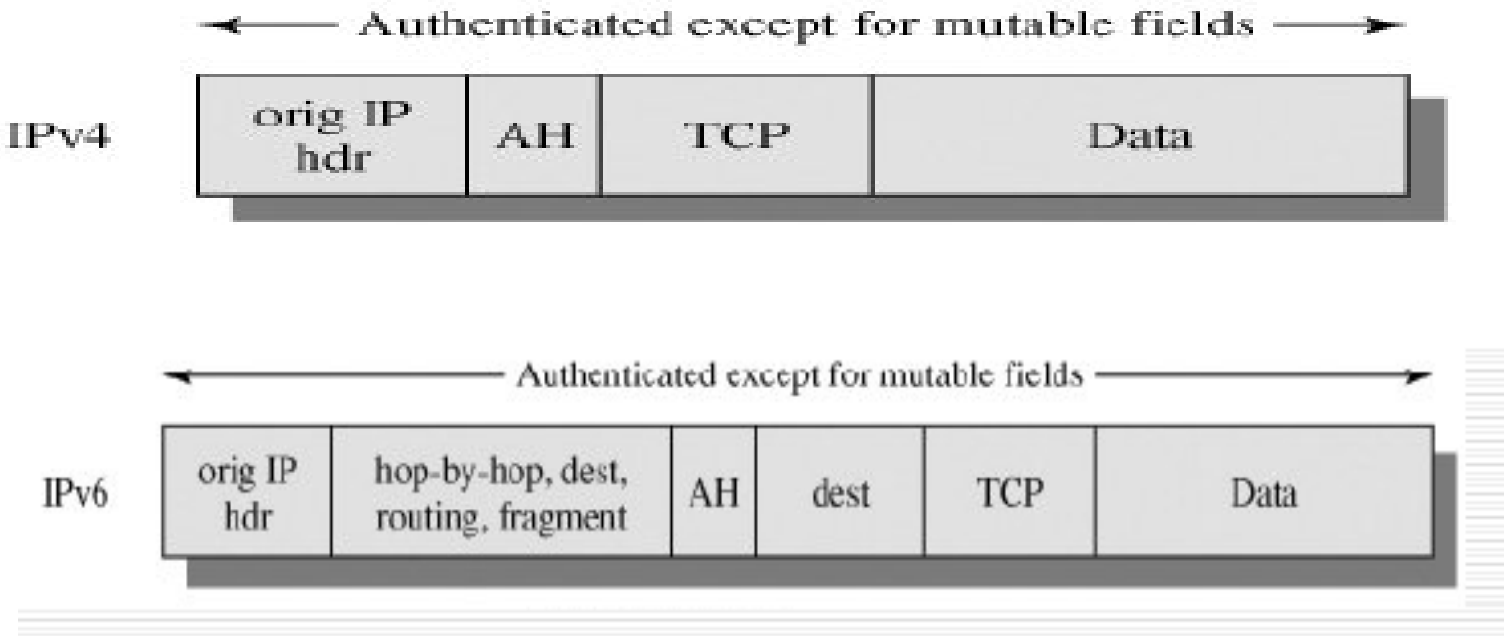
- مد تونل (Tunnel): برای احراز اصالت بین کاربر و حفاظ (firewall)

انواع احراز اصالت با AH



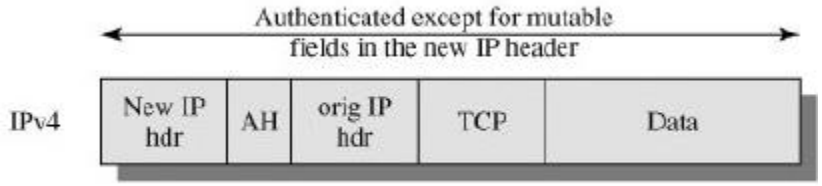
محدوده احراز اصالت AH

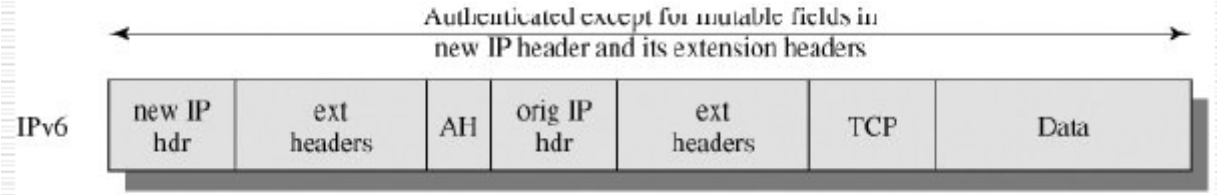
- **مد انتقال**



محدوده احراز اصالت AH

- مد تونل





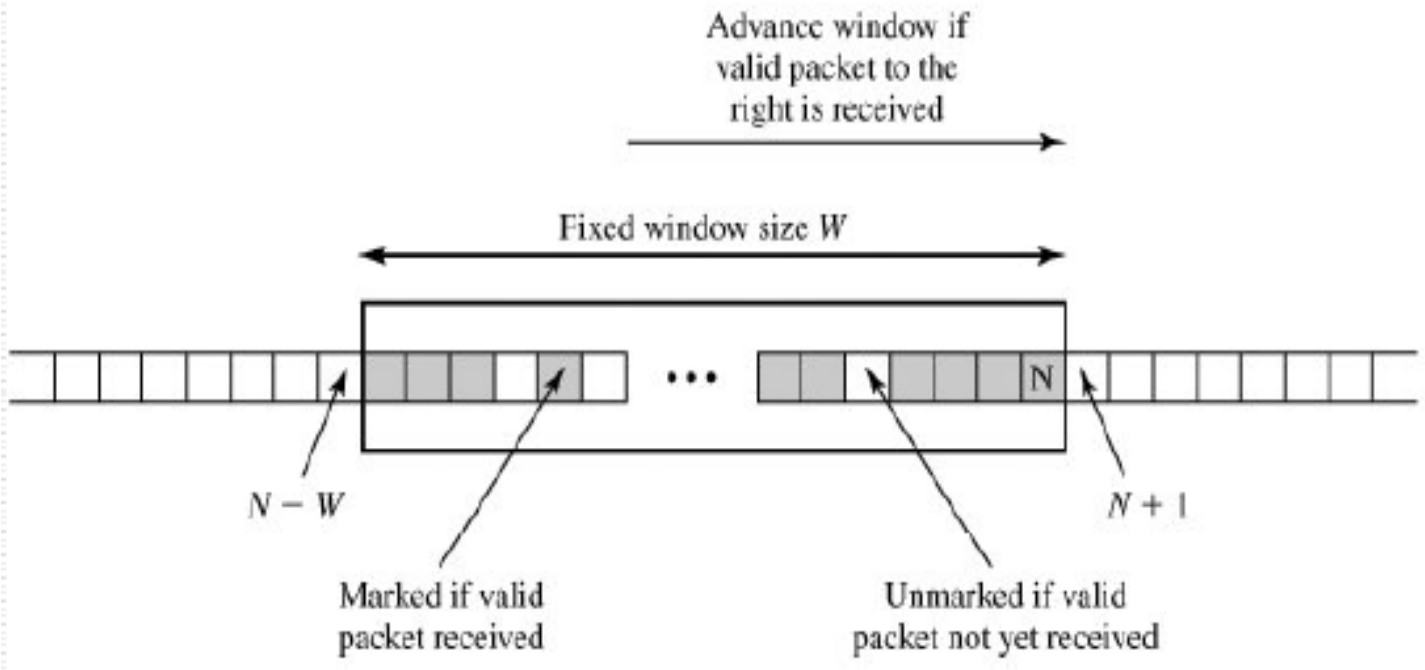
مقابله با حمله تکرار درAH

- روش مقابله با حمله تکرار (Replay)
  - اختصاص یک شمارنده با مقدار صفر به هر SA
  - افزایش شمارنده به ازای هر بسته جدید که با این SA فرستاده می شود.
  - اگر شمارنده به مقدار2^{32} -1 برسد، باید از یک SA جدید با کلید جدید استفاده کرد.
  - درنظرگرفتن یک پنجره به اندازه پیش فرض W =۶۴
  - لبه سمت راست پنجره به بزرگترین شماره بسته رسیده و تاییدشده از نظر صحت اختصاص می یابد.

مقابله با حمله تکرار درAH

- مکانیزم برخورد با بسته جدید در پنجره
  - بسته جدید و داخل محدوده پنجره
    - محاسبه MAC و علامت زدن خانه متناظر در پنجره در صورت احراز اصالت
  - بسته خارج از محدوده پنجره (سمت راست)
    - محاسبه MAC، احراز اصالت و شیفت پنجره به سمت راست، به طوری که خانه متناظر سمت راست لبه پنجره را نشان دهد.
  - بسته جدید خارج از محدوده پنجره یا عدم احراز اصالت آن
    - دور انداخته می شود!

مقابله با حمله تکرار درAH



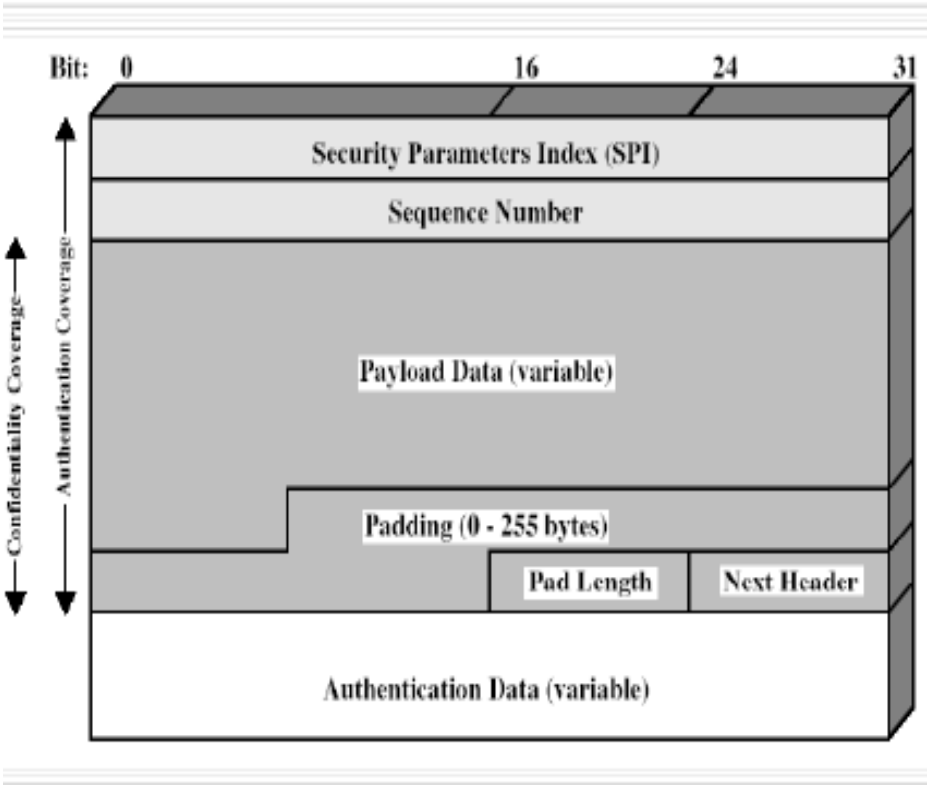
Encapsulation Security Payload(ESP)

- **ویژگیها**
  - پشتیبانی از محرمانگی داده و تا حدی محرمانگی ترافیک
  - امکان احراز اصالت (مشابه AH)
  - استفاده از الگوریتم DES در مد CBC (امکان استفاده از 3-IDEA,IDEA,RC5,3-DES, وCAST وBlowfish نیز وجود دارد).

Encapsulation Security Payload(ESP)

- **فیلدهای ESP**
  - SPI :شناسه SA
  - Sequence Number : شمارنده برای جلوگیری از حمله تکرار مشابه AH
  - Payload: محتوای بسته که رمز می شود
  - Padding : بیتهای اضافی
  - Pad Length : طول فیلد بالا
  - Next Header : نوع داده موجود در Payload Data
  - Authentication Data:مقدار MAC محاسبه شده (بدون در نظر گرفتن خود فیلد)

Encapsulation Security Payload(ESP)

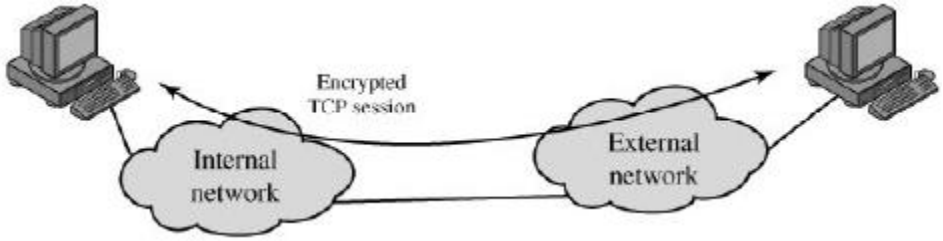


مد انتقال درESP

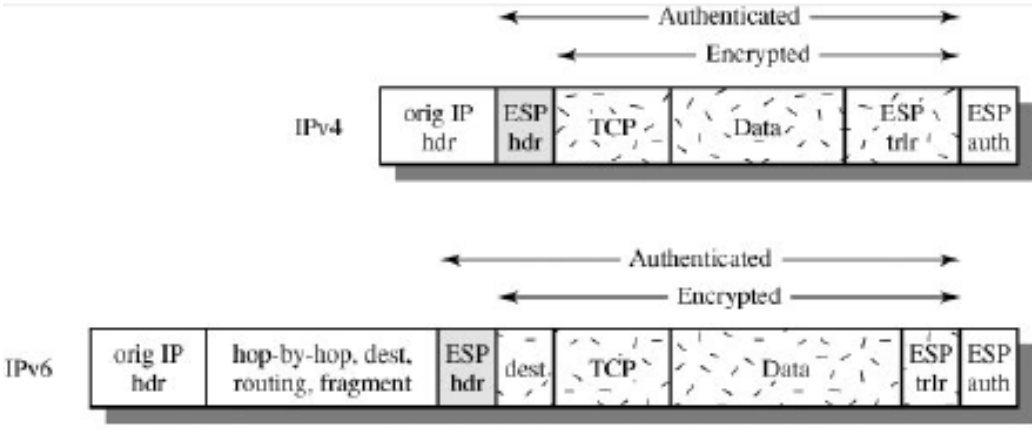
- **مد انتقال**
  - تضمین محرمانگی بین hostها
  - رمزنگاری بسته داده، دنباله ESP و اضافه شدن MAC درصورت انتخاب احراز اصالت توسط مبداء
  - تعیین مسیر توسط مسیریابهای میانی با استفاده از سرآیندهای اصلی(که رمز نشده اند)
  - چک کردن سرآیندIP توسط مقصد و واگشایی رمز باقیمانده پیام
  - امکان آنالیز ترافیک

مد انتقال در ESP

- برای ارتباط بین میزبان ها



- محدوده ESP

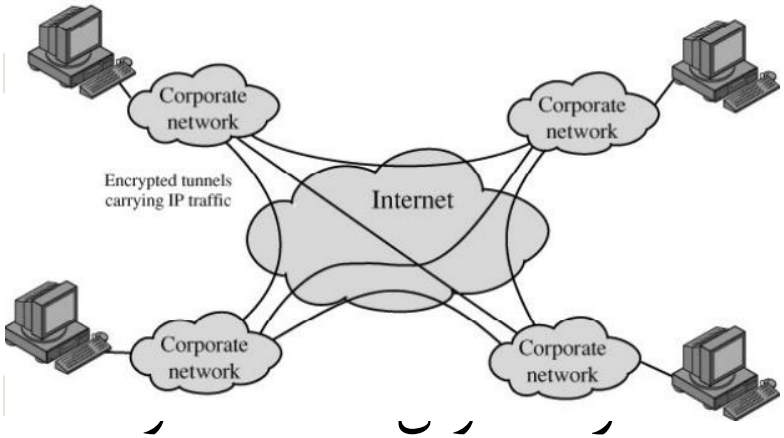


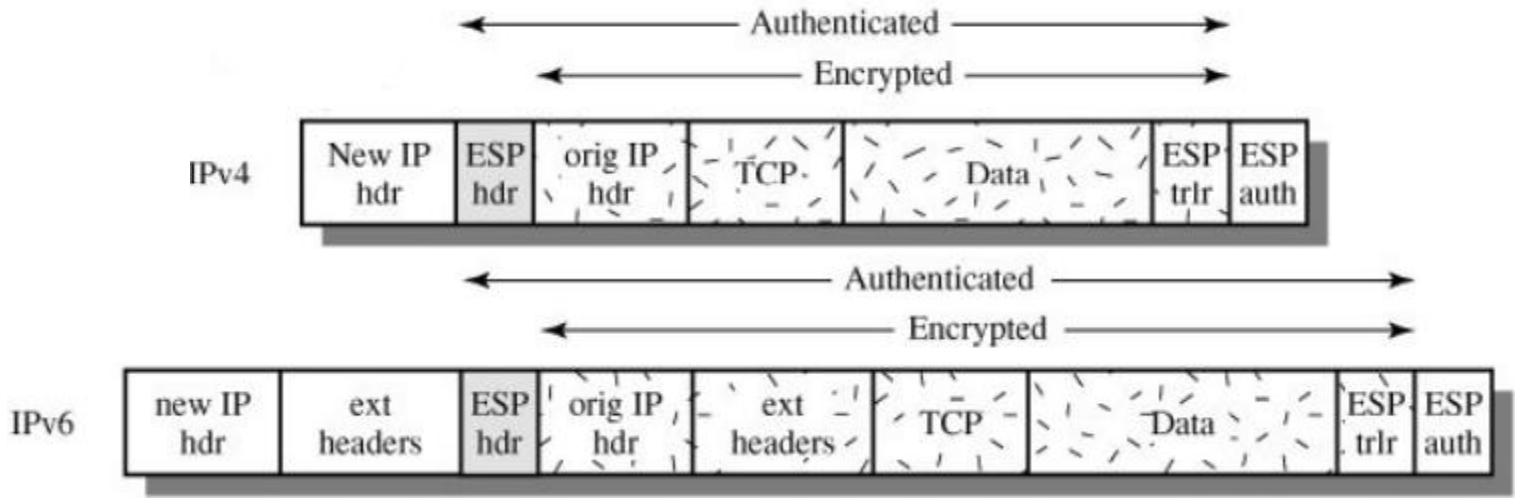
ESP trailer =
Padding, Pad Length, and Next Header Fields

مد تونل در ESP

- **مد تونل**
  - اضافه شدن آدرس مبداء و مقصد دروازه های خروجی فرستنده و گیرنده، سرآیند ESP و دنباله ESP و قسمت مربوط به MAC در صورت نیاز (برای احراز اصالت)
  - انجام مسیریابی در مسیریاب های میانی از روی آدرس های جدید
  - رسیدن بسته به فایروال شبکه مقصد و مسیریابی از روی آدرس IP قبلی تا گره نهایی
  - مد تونل IPSec یکی از روش های ایجاد شبکه های خصوصی مجازی (VPN) است.

مد تونل در ESP





ترکیب SAها

- با توجه به اینکه هر SA تنها یکی از سرویس های AH یا ESP را پیاده سازی کرده است، برای استفاده از هر دو سرویس باید آنها را باهم ترکیب کرد.

- ترکیبهای مختلف
  - پیاده سازی IPSec توسط host های متناظر
  - پیاده سازی IPSec توسط gateway ها
  - ترکیب دو حالت بالا

ترکیب SAها

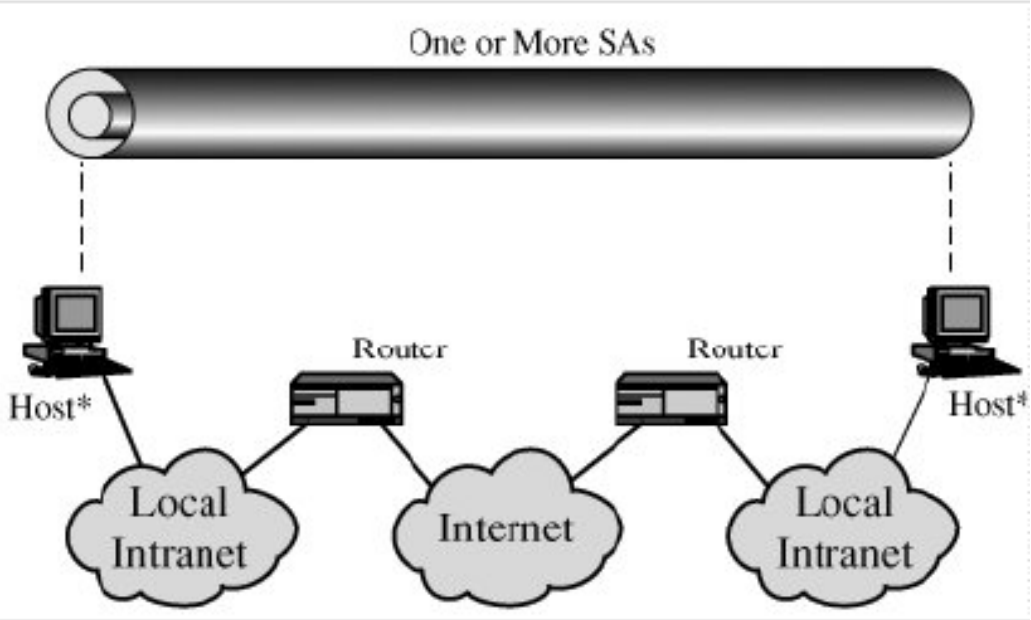
- ترتیبی از SAها که باید بر روی یک بسته اعمال شوند، bundle نامیده می شوند.
- SAها در یک bundle به دو طریق قابل ترکیب هستند:
  - Transport Adjacency
    - اعمال چند SA در مد انتقال به بسته
    - صرفاً یک سطح از ترکیب را برای AH وESP فراهم می نماید.
  - Iterated Tunneling
    - ایجاد چند لایه امنیتی با تونلهای تو در تو
    - مبدا و مقصد هر تونل می تواند در سایتهای مختلفی از مسیر باشد.

ترکیب SAها

- امکان داشتن احراز اصالت و محرمانگی به صورت توأم از طریق:
  - ESP with Authentication Option:احراز اصالت محتوای رمزشده
    - مد انتقال: عدم حفاظت سرآیندIP
    - مد تونل: حفاظت کل بسته داخلی
  - Transport Adjacency:اعمال ESP وسپس AH بر روی آن در مد انتقال
    - حفاظت از سرآیند IP و سرآیند ESP، حفظ محرمانگی بسته
  - Transport-Tunnel Bundle:اعمال AH در مد انتقال و سپسESP در مد تونل
    - احراز اصالت داده و سرآیند IP (به غیر فیلدهای متغیر)
    - محرمانگی کل بسته و امضای آن

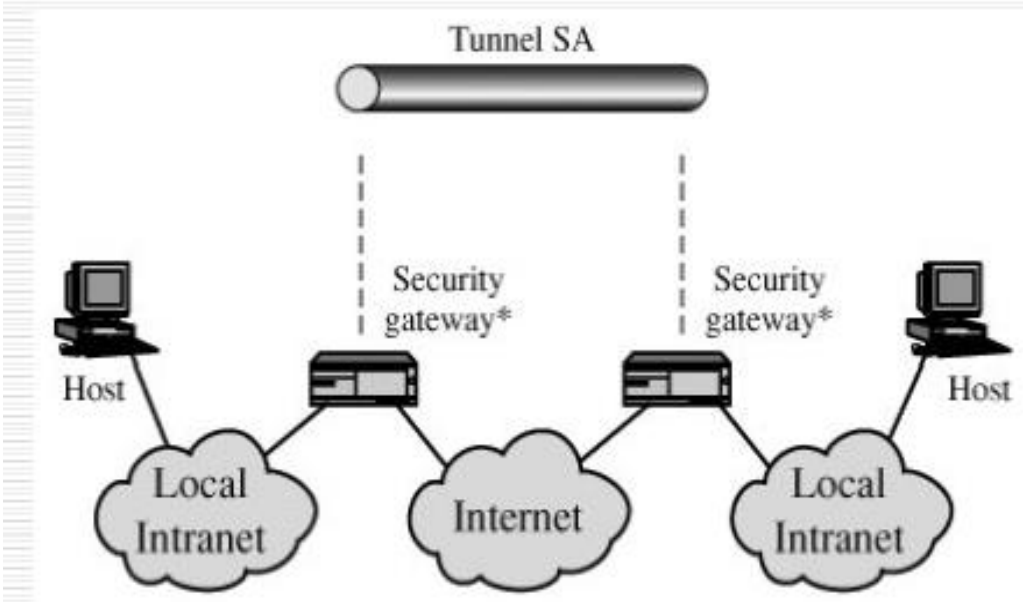
ترکیب SAها: حالت ۱

- پیاده سازی IPSec به صورت انتها-به-انتها
- امکان استفاده از هر یک از ترکیبات ممکن از انواع SAها



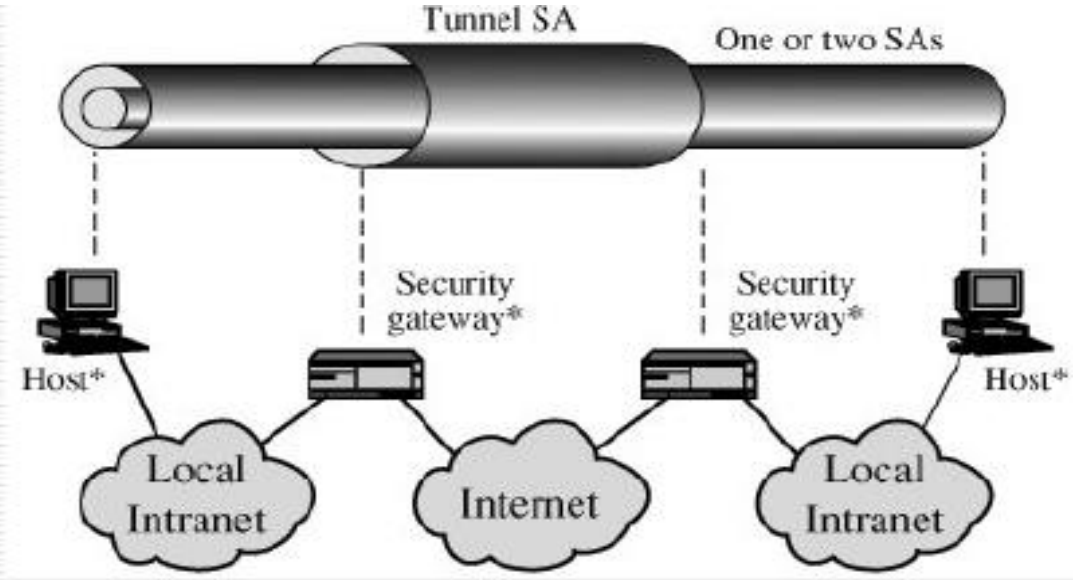
ترکیب SAها: حالت ۲

- برقراری تونل اَمن بین دروازه ها: شبکه خصوصی مجازی
- ایجاد تونل در یکی از مدهایAH، ESP و یا.ESP with Auth.



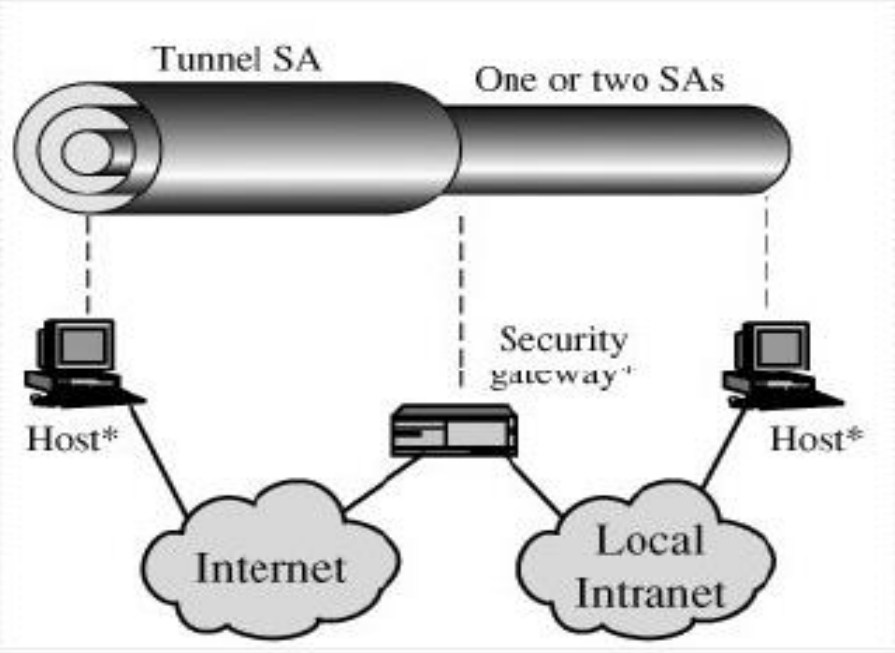
ترکیب SAها: حالت ۳

- ترکیب دو حالت ۱ و۲
- اگر تونل بین دروازه ها از نوعESP باشد، به طور محدود محرمانگی ترافیک نیز فراهم می گردد.



ترکیب SAها: حالت ۴

- برای اتصال یک میزبان بیرونی به یک سیستم شبکه داخلی
- ایجاد تونل تا دروازه شبکه داخلی، ترکیب چند SA



مدیریت کلید

- عموما به ۴ کلید سری، دو تا برای AH و دو تا برای ESP (در دو جهت) نیازمندیم.

- برای تولید و توزیع این کلیدها به یک مکانیزم مدیریت کلید نیازمندیم.

مدیریت کلید

- مدیریت کلید دستی: تنها در سیستم های ایستا و کوچک قابل استفاده است.

- مدیریت کلید خودکار:
  - پروتکل اتوماتیک و پیش فرض مدیریت و توزیع کلید IPSec اصطلاحا ISAKMP/Oakley نامیده می شود.

Internet Security Association and Key Management Protocol

مدیریت کلید

- مدیریت کلید خودکار به نام ISAKMP/Oakley معروف است و شامل دو پروتکل است:
  - پروتکل تعیین کلیدOakley
  - فرم توسعه یافته پروتکل Diffie-Hellman که ضعفهای آن را برطرف کرده است.
  - پروتکل مدیریت کلید و SA در اینترنت (ISAKMP)
  - تعریف رویه ها و قالب بسته ها برای برقراری، مذاکره، تغییر یا حذف SA

پروتکل Oakley

- خصوصیات پروتکل Oakley
- مقابله با حمله Clogging در DH: منابع قربانی با درخواستهای مکرر تبادل کلید تلف می شود.
  - با استفاده از تعریف مفهومی تحت عنوان کوکی(Cookie) مشکل این حمله را برطرف می کند.
- مقابله با حمله مرد میانی در DH:
  - احراز اصالت در تبادل کلید DH
- مقابله با حمله تکرار:
  - با استفاده از نانس با حمله های تکرار مقابله می کند.

پروتکل Oakley

- مقابله با حمله Clogging
  - استفاده از کوکی (توسط هر یک از طرفین) به صورت زیر:
    - ارسال عدد تصادفی کوکی توسط هریک از طرفین ارتباط
    - ارسال ack توسط طرف دیگر
    - نیاز به ارسال ack توسط مبدأ در اولین پیام DH
  - اگر مهاجم از آدرس جعلی برای ارسال کوکی استفاده کرده باشد، چون ack را دریافت نمی کند، نمی تواند DH را آغاز نماید.
  - باید تولید و وارسی کوکی کم هزینه باشد تا حملات اتلاف منابع ممکن نباشد.

پروتکل ISAKMP

- تعریف رویه ها و قالب بسته ها برای برقراری، مذاکره، تغییر یا حذف SA
- قالب بسته های ISAKMP
  - یک پیام ISAKMP شامل سرآیند و یک نوع بخش داده ای برای تبادل داده های مربوط به تولید کلید و احراز اصالت است.
- رویه ها
  - شامل مجموعه ای از تعامل های (پروتکل های) از قبل تعریف شده برای امور مختلف

انواع بخش داده ای در ISAKMP

Type	Description
Security Association (SA)	Used to negotiate security attributes and indicate the DOI and Situation under which negotiation is taking place.
Proposal (P)	Used during SA negotiation; indicates protocol to be used and number of transforms.
Transform (T)	Used during SA negotiation; indicates transform and related SA attributes.
Key Exchange (KE)	Supports a variety of key exchange techniques.
Identification (ID)	Used to exchange identification information.
Certificate (CERT)	Used to transport certificates and other certificate- related information.
Certificate Request (CR)	Used to request certificates; indicates the types of certificates requested and the acceptable certificate authorities.
Hash (HASH)	Contains data generated by a hash function.
Signature (SIG)	Contains data generated by a digital signature function.
Nonce (NONCE)	Contains a nonce.
Notification (N)	Used to transmit notification data, such as an error condition.
Delete (D)	Indicates an SA that is no longer valid.

انواع تعاملات در ISAKMP

- Base Exchange: تبادل کلید و احراز اصالت بدون محافظت از شناسه.
- Identity Protection Exchange: توسعه تعامل پایه با حفاظت از شناسه طرفین.
- Authentication Only Exchange: صرفاً احراز اصالت دوطرفه بدون تبادل کلید.
- Aggressive Exchange: کاهش تعداد پیامهای تبادلی با عدم حفاظت از شناسه.
- Informational Exchange: ارسال یکطرفه اطلاعات برای مدیریت SA.

مرکز آپای دانشگاه گیلان

مرکز ماهر

وزارت ارتباطات و فناوری اطلاعات
سازمان فناوری اطلاعات ایران

امنیت در لایه انتقال

خطرات تهدیدکننده وب

- با وجود سادگی راه اندازی خدمات مبتنی بر وب و گستردگی استفاده از مرورگرها، برنامه های تحت وب از پیچیدگی بالا و تهدیدات بالقوه فراوانی برخوردار است.
- نمونه ای از خطرات متداول:
  - حمله به وب سرورها
  - تهدید اعتبار برنامه های تجاری مهم
  - وجود کاربران عام و ناآشنا به خطرات امنیتی
  - دسترسی به حریم خصوصی افراد و آزار و اذیت آنها

دسته بندی حملات تهدیدکننده وب

- دسته بندی بر اساس تاثیر حمله
  - حملات منفعل: شنود، دسترسی به داده های حفاظت شده در وب سایت
  - حملات فعال: تغییر در داده های در حال انتقال، جعل کاربر یا سرور
- دسته بندی بر اساس مکان رخداد حمله
  - حملات به وب سرور
  - حملات به مرورگر وب
  - حملات به ترافیک شبکه وب

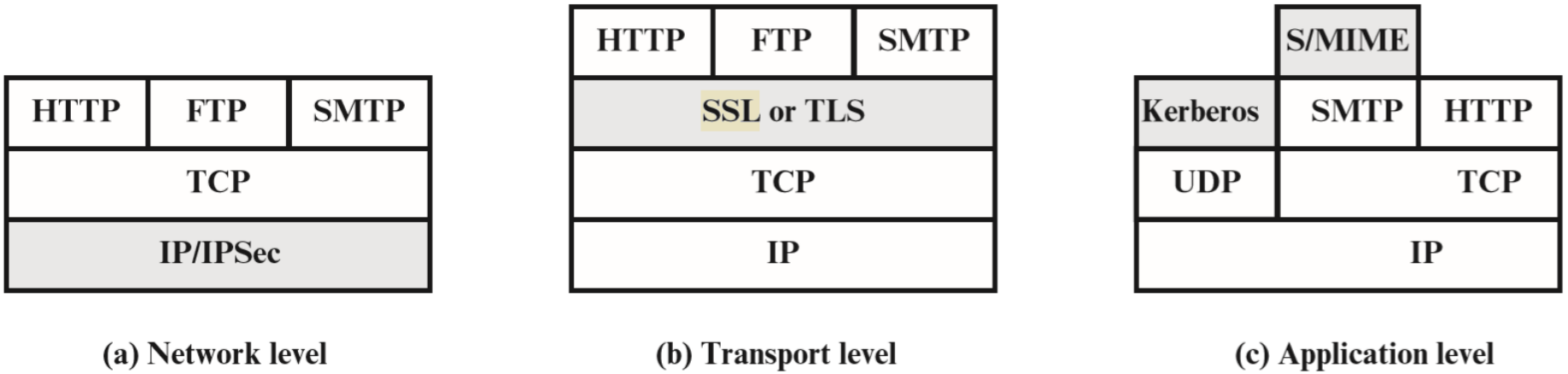
تهدیدات در وب

	Threats	Consequences	Countermeasures
Integrity	• Modification of user data • Trojan horse browser • Modification of memory • Modification of message traffic in transit	• Loss of information • Compromise of machine • Vulnerability to all other threats	Cryptographic checksums
Confidentiality	• Eavesdropping on the net • Theft of info from server • Theft of data from client • Info about network configuration • Info about which client talks to server	• Loss of information • Loss of privacy	Encryption, Web proxies
Denial of Service	• Killing of user threads • Flooding machine with bogus requests • Filling up disk or memory • Isolating machine by DNS attacks	• Disruptive • Annoying • Prevent user from getting work done	Difficult to prevent
Authentication	• Impersonation of legitimate users • Data forgery	• Misrepresentation of user • Belief that false information is valid	Cryptographic techniques

روشهای مختلف تامین امنیت وب

- استفاده از IPSec
  - همه منظوره
  - پنهان از دید کاربران لایه بالاتر
  - سربار استفاده ازIPSec (به خصوص در سمت کارفرما)
- استفاده از SSL/TLS
  - پنهان از دید برنامه های کاربردی
  - پشتیبانی مرورگرها و نیز بسیاری از وب سرورها
- سرویسهای امنیتی وابسته به کاربرد خاص
  - تراکنش های مالی امن (SET)

روشهای مختلف تامین امنیت وب



(a) Network level

(b) Transport level

(c) Application level

SSL -تاریخچه

- July, 1994
  - شرکت Netscape طراحی SSL 1.0 را انجام داد.
  - این نسخه هیچ گاه منتشر نشد!
- Dec, 1994
  - مرورگر Netscape همراه با SSL 2.0 به بازار عرضه شد.
  - آسیب پذیر بود. کمتر از ۱ ساعت می شد به آن نفوذ کرد.
  - محدودیت استفاده از کلیدهای بیتی ۴۰ بیتی در خارج آمریکا

SSL -تاریخچه

- July, 1995
  - مایکروسافت نسخه جدیدی از IE را به بازار عرضه کرد که از SSL پشتیبانی می کرد.
  - پشتیبانی از مدهای کاری جدید و افزایش طول کلیدهای قابل استفاده
- Nov, 1995
  - شرکت Netscape توصیف SSL 3.0 را منتشر کرد.
  - با تغییرات و جهش عمده نسبت به نسخه های قبلی همراه بود.
  - ضمن اینکه نسبت به نسخه SSl 2.0، Backward compatible بود.

SSL -تاریخچه

- May, 1996
  - IETF گروه کاری TLS را تشکیل داد و مسئولیت پاسخگویی به مشکلات قرارداد SSL را برعهده گرفت.
- Jan, 1999
  - TLS 1.0بطور رسمی همراه با RFC 2246 به بازار عرضه شد.
  - در واقع همان SSL V3.1 بود که به دلایل تجاری تغییر نام داده بود.

SSL -تاریخچه

SSL and TLS protocols

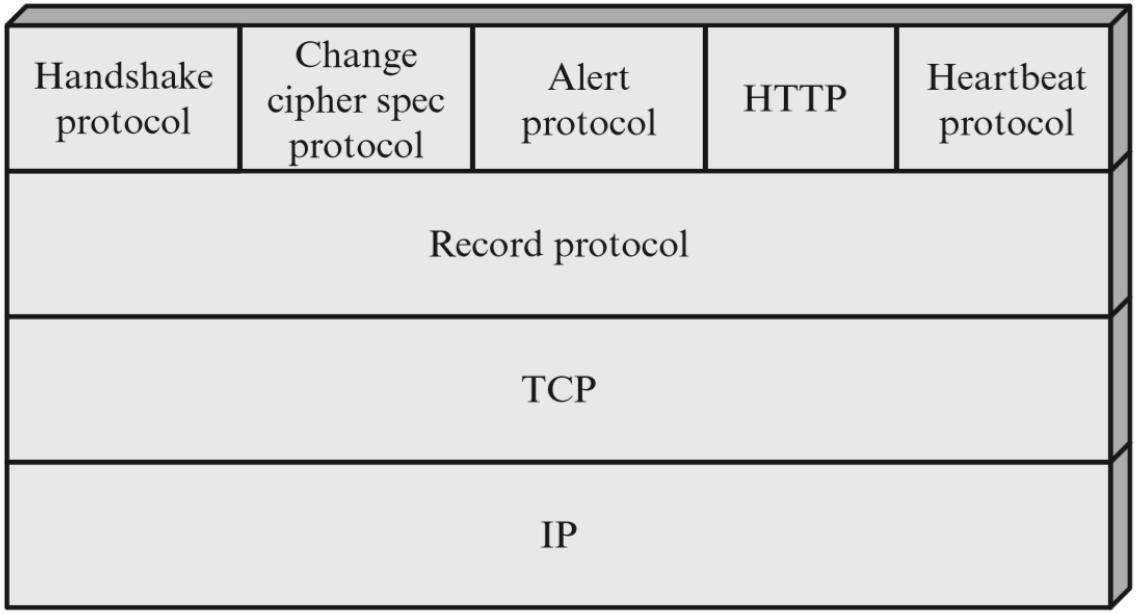
Protocol	Published	Status
SSL 1.0	Unpublished	Unpublished
SSL 2.0	1995	Deprecated in 2011 (RFC 6176)
SSL 3.0	1996	Deprecated in 2015 (RFC 7568)
TLS 1.0	1999	Deprecation planned in 2020[11]
TLS 1.1	2006	Deprecation planned in 2020[11]
TLS 1.2	2008	
TLS 1.3	2018	

SSL -معرفی

- لایه امنیتی در بالای لایه انتقال
- ارائه شده توسط شرکت Netscape و نسخه TLS 1.3 با RFC 8446 آن نسخه استاندارد اینترنت است.
- سرویس قابل اطمینان انتها به انتها (end to end) و مبتنی بر TCP
- پروتکل آن در دو لایه پیاده سازی می شود.

SSL -معماری

- لایه اول بالای لایه انتقال و لایه دوم در لایه کاربرد
- لایه اول شامل پروتکل Record و لایه دوم مربوط به سرویس های مدیریتی بوده و شامل پروتکل های زیر است.



SSL -مفاهیم

- اتصال (Connection)
  - یک ارتباط همتا-به-همتای امن (رمزگذاری همراه با MAC) در لایه انتقال
  - هر اتصال به یک نشست نگاشت می شود.
- نشست (Session)
  - یک نشست SSL، یک پیوند بین کارفرما و کارگزار است.
  - هر نشست SSL با پروتکل Handshake شکل می گیرد.
  - هر نشست مجموعه ای از پارامترهای رمزنگاری است که بین چند اتصال می تواند به اشتراک گذارده شود، تا هزینه ارتباطات کاهش یابد.

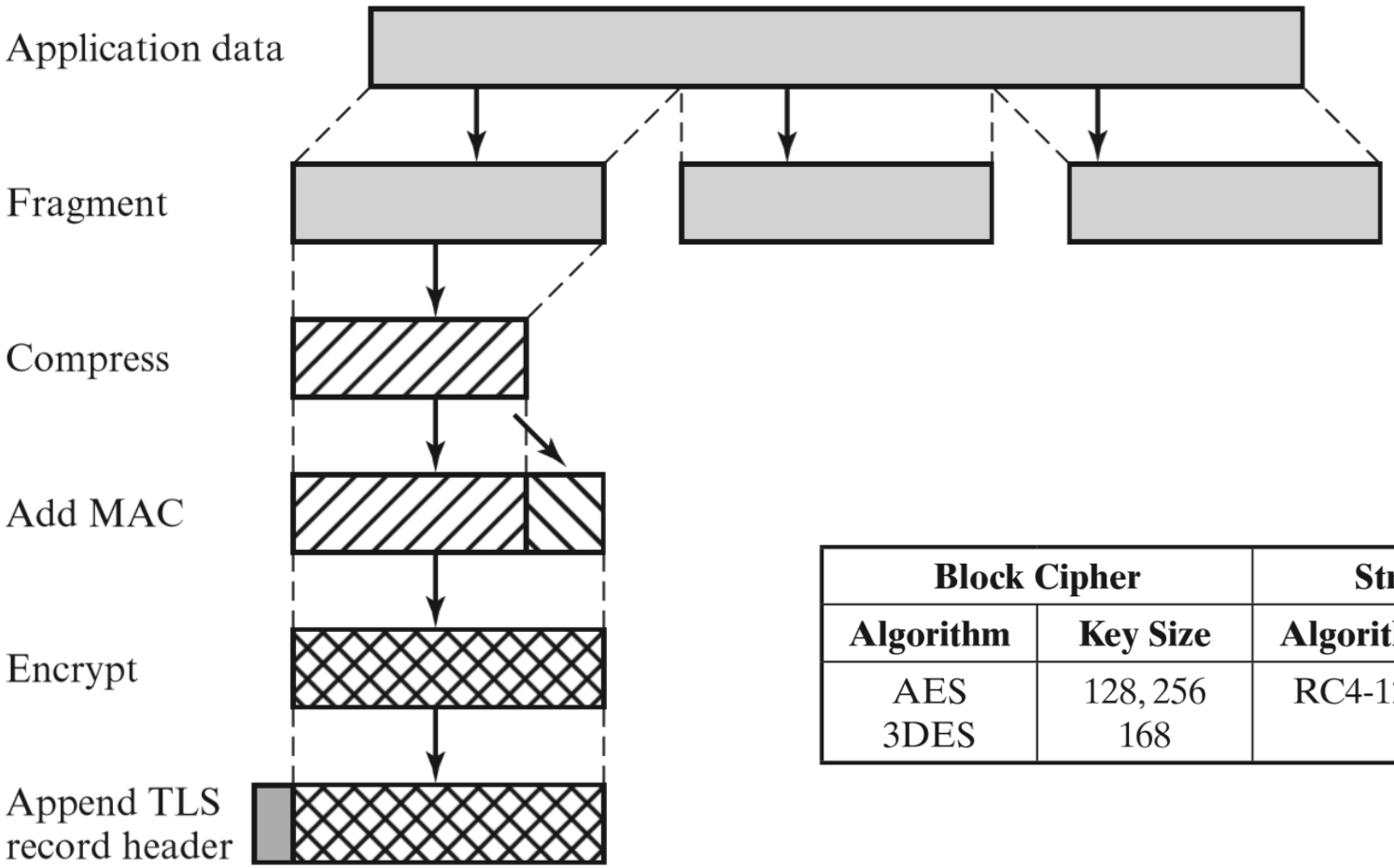
SSL- پروتکل ها

- **پروتکل SSL Record**

دو سرویس برای SSL فراهم می کند:

- محرمانگی پیام
  - با استفاده از یک کلید متقارن مخفی که در پروتکل Handshake به اشتراک گذاشته شده است.
  - استفاده از یکی از الگوریتم های IDEA، RC2-40، DES-40، DES، 3DES، Fortezza، RC4-40، RC4-128، AES.
- صحت پیام
  - تولید MAC با استفاده از کلید متقارن مخفی
  - استفاده از SHA-1 یا MD5

اَعمال پروتکل Record

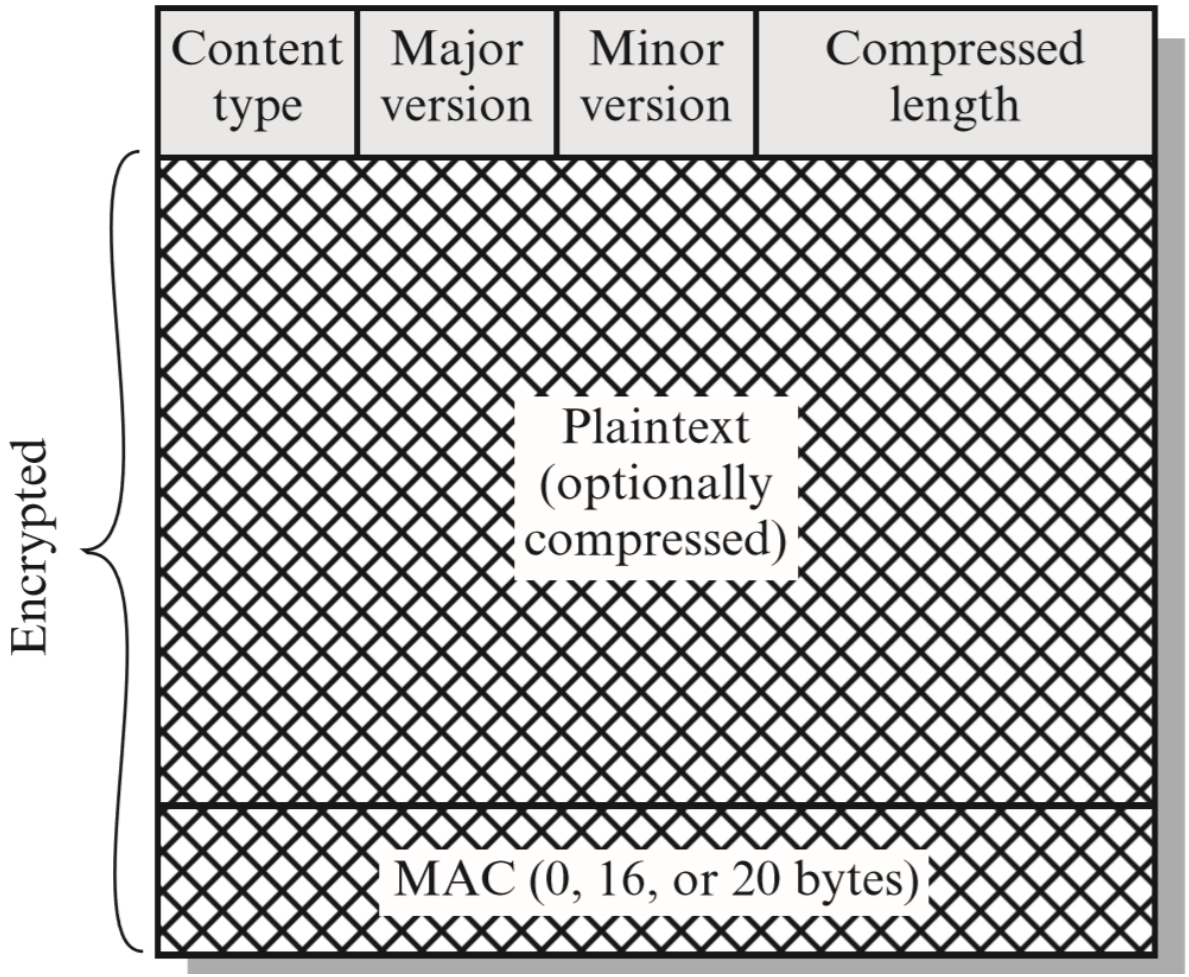


Block Cipher		Stream Cipher	
Algorithm	**Key Size**	**Algorithm**	**Key Size**
AES 3DES	128, 256 168	RC4-128	128

SSL- پروتکل ها

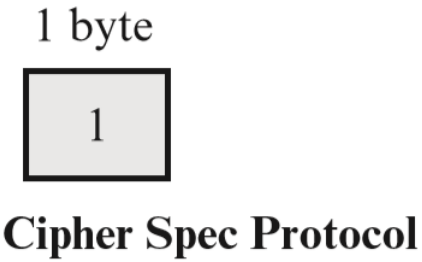
- اعمال انجام شده در پروتکل Record
  - قطعه بندی: تولید قطعاتی به طول 2^{14} یا کمتر .
  - فشرده سازی: اختیاری و بدون از دست رفتن داده.
  - تولید MAC: مشابه HMAC و روی ورودی زیر انجام می گیرد:
    - (محتوای قطعه، طول قطعه، نوع فشرده سازی، شماره سریال)
    - الگوریتم درهمساز مورد استفاده، MD5 یا SHA-1 است.
  - رمزنگاری: استفاده از رمز قطعه ای یا جریانی.
  - اضافه کردن سرآیند: به ابتدای قطعه رمزشده می چسبد و شامل عناصر زیر است:
    - (نوع محتوا، نسخه اصلی SSL، نسخه فرعی SSL ، طول داده فشرده شده)
    - نوع محتوا (Content Type) بیان کننده پروتکل استفاده کننده از این سرویس در لایه بالاتراست.

قالب SSL Record



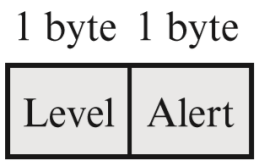
SSL- پروتکل ها

- **پروتکل Change Cipher Spec:**
  - یکی از ۳ پروتکل لایه دوم SSL که از پروتکل Record استفاده می کنند.
  - شامل یک بایت است که حاوی مقدار ۱ است.
  - در انتهای اجرای پروتکل handshake، منجر به جایگزینی اطلاعات (حالت) یک نشست جدید معلق (pending) به جای نشست فعلی می شود تا در اتصال جاری مورد استفاده قرار گیرد.



SSL- پروتکل ها

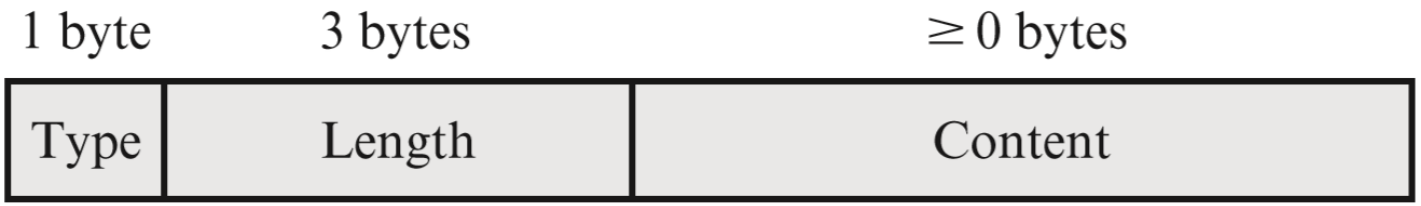
- **پروتکل SSL Alert:**
  - هشدارها و خطاهای مربوط به SSL را به طرف مقابل منتقل می کند.
  - Level :شدت خطای پیش آمده؛ Warning یا Fatal.
  - Alert: کد نمایانگر نوع خطا از جمله:
    - unexpected message, bad record mac, decompression failure, handshake failure
  - مانند بقیه داده های SSL فشرده سازی و رمزنگاری می شود.
  - خطای Fatal موجب خاتمه یک اتصال و عدم ایجاد اتصال جدید در آن نشست می شود.



Alert Protocol

SSL- پروتکل ها

- **پروتکل SSL Handshake**
  - پیش از انتقال هر نوع داده ای تحت SSL انجام می شود.
  - با استفاده از آن کارفرما و کارگزار می توانند:
    - همدیگر را احراز اصالت کنند.
    - الگوریتم های رمزنگاری، توابع درهم ساز مورد استفاده و کلیدهای رمزنگاری متقارن و نامتقارن را رد و بدل کنند.



Handshake Protocol

انواع پیامهای پروتکل Handshake

TLS Handshake Protocol Message Types

Message Type	Parameters
hello_request	null
client_hello	version, random, session id, cipher suite, compression method
server_hello	version, random, session id, cipher suite, compression method
certificate	chain of X.509v3 certificates
server_key_exchange	parameters, signature
certificate_request	type, authorities
server_done	null
certificate_verify	signature
client_key_exchange	parameters, signature
finished	hash value

پروتکل SSL Handshake

- **پروتکل SSL Handshake**
  - شامل ۴ فاز اصلی زیر است:
    - مشخص کردن قابلیت های رمزنگاری دو طرف
    - احراز اصالت کارگزار به کارفرما و مبادله کلیدهای آن
    - احراز اصالت کارفرما به کارگزار و مبادله کلیدهای آن
    - جایگزینی پارامترهای رمزنگاری جدید به جای قبلی و خاتمه توافق

فاز تبیین توانمندیهای امنیتی در پروتکل Handshake

- ارسال پیغام Hello توسط کارفرما (آغازگر جلسه)
- پیشنهاد نسخه پروتکل: آخرین نسخه پشتیبانی شده توسط کارفرما
- پیشنهاد الگوریتم های رمزنگاری و درهمسازی مناسب و روش تبادل کلید آنها
- پیشنهاد مکانیزم فشرده سازی مناسب
- انتخاب برترین الگوریتم رمزنگاری و فشرده سازی مورد توافق طرفین توسط کارگزار

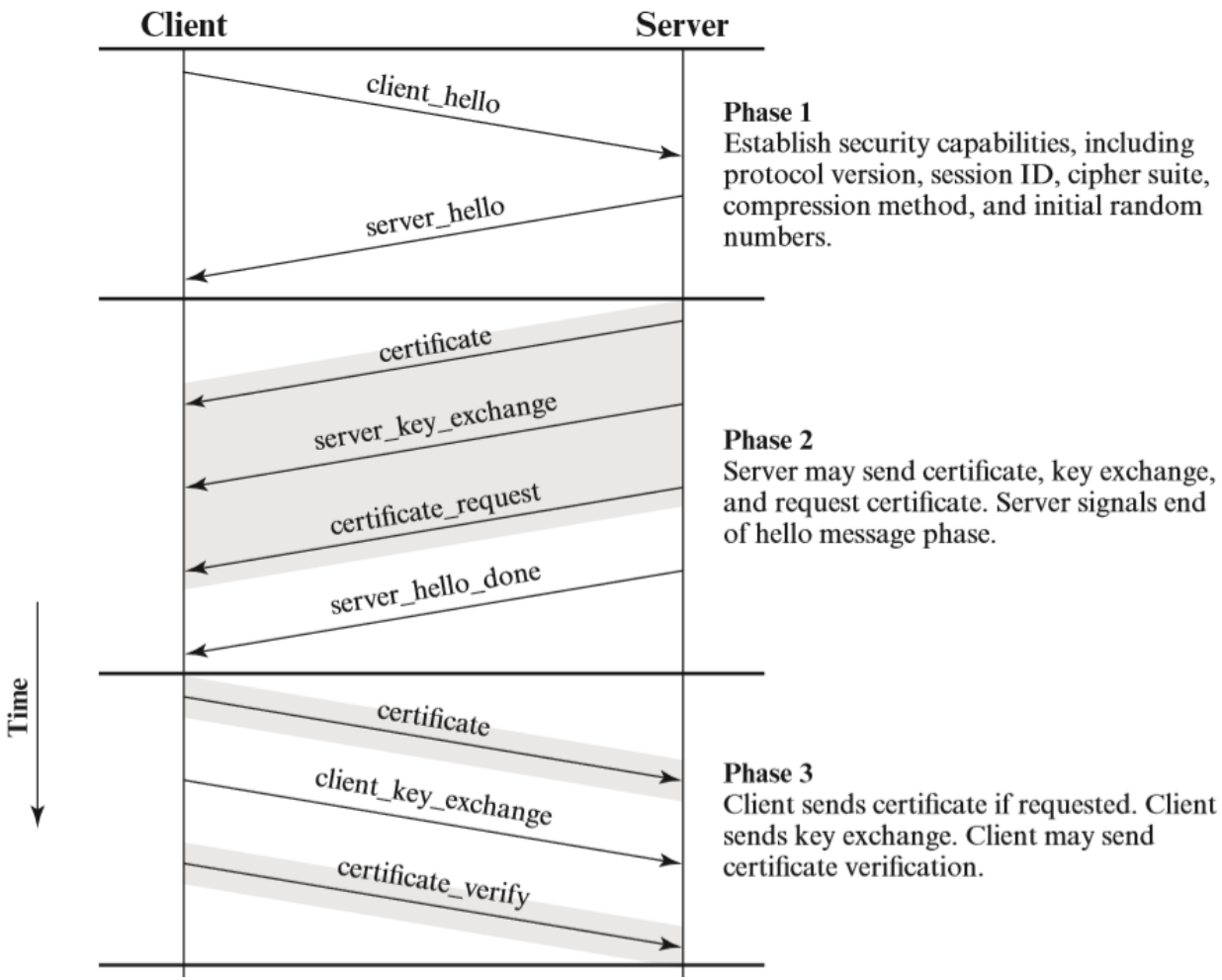
فاز احراز اصالت و تبادل کلید در پروتکل Handshake

- ارسال گواهی کارگزار برای کارفرما
  - همراه با کلید عمومی (RSA) یا پارامترهای DH
- تولید و ارسال کلید سری
  - کارفرما گواهی کلید عمومی کارگزار را وارسی می کند.
  - کارفرما کلید سری را تولید کرده و رمزشده به کارگزار می فرستد.
  - یا این که هر دو با استفاده از پارامترهای DH کلید سری را محاسبه می کنند.
  - در صورت درخواست کارگزار، کارفرما گواهی کلید عمومی خود را به همراه امضای تمام پیامهای ارسالی و دریافتی (برای احراز اصالت خود) به کارگزارمی فرستد.

فاز خاتمه در پروتکل Handshake

- فعال کردن پروتکل تغییر مشخصات رمز (Change Cipher Spec)
  - کارفرما پیام پروتکل تغییر مشخصات رمز را برای کارگزار می فرستد.
  - کارگزار حالت خود را بروز کرده (با پارامترهای توافق شده در پروتکل Handshake) و پیام پروتکل تغییر مشخصات رمز را برای کارفرما ارسال می کند.
- پایان
  - ارسال پیام پایانی finished از کارفرما (همراه با پیام تغییر رمز بالا)
  - ارسال پیام پایانی finished از کارگزار (همراه با پیام تغییر رمز بالا)
  - آغاز تبادل اطلاعات به صورت محرمانه و با پارامترهای جدید

پروتکل SSL Handshake

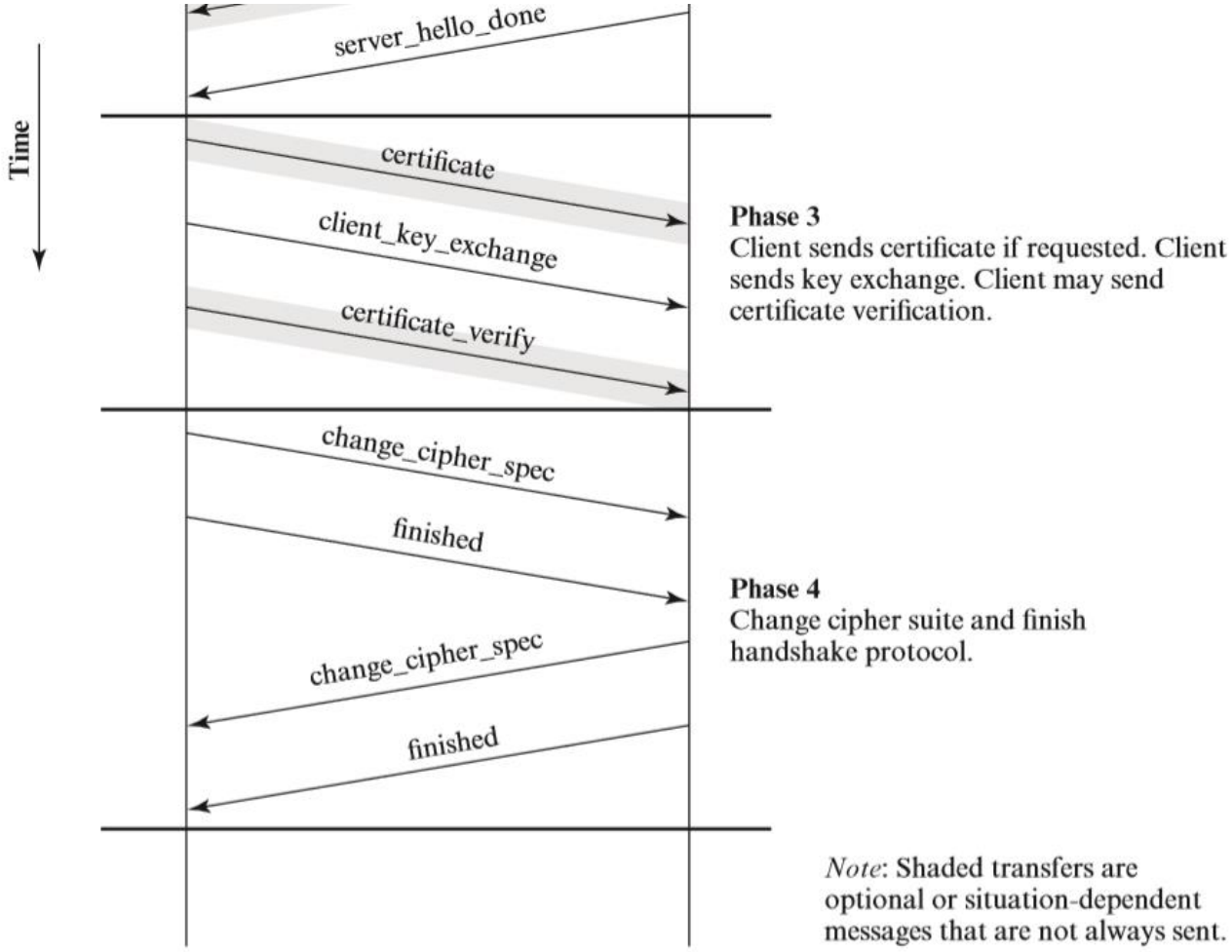


Phase 1
Establish security capabilities, including protocol version, session ID, cipher suite, compression method, and initial random numbers.

Phase 2
Server may send certificate, key exchange, and request certificate. Server signals end of hello message phase.

Phase 3
Client sends certificate if requested. Client sends key exchange. Client may send certificate verification.

پروتکل SSL Handshake



جمع بندی – SSL

- SSL نیازهای امنیتی زیر را فراهم می کند:
  - محرمانگی داده
    - با استفاده از رمزنگاری متقارن
  - صحت داده
    - با استفاده از کد احراز اصالت داده
  - احراز اصالت کارگزار (و در صورت نیاز کارفرما)
    - بر اساس استاندارد X.509
- امروزه مهمترین کاربرد SSL در قرارداد HTTPS است.

TLS (Transport Layer Security)

- یک استاندارد از IETF
- به دنبال ایجاد یک نسخه استاندارد اینترنتی از SSL است.
- بسیار شبیه SSL نسخه ۳ بدون در نظرگرفتن تفاو تهای جزئی زیر:
  - بهره گیری از HMAC واقعی در محاسبه MAC (استفاده از عملگرXOR).
  - در TLS کد خطای no-certificate قابل قبول نیست و مجموعه کد خطاها افزایش یافته است.
  - الگوریتم Fortezza از الگوریتم های توزیع کلید و رمزگذاری حذف شد.

SSL/TLS

- رمزنگاری داده‌های لایه کاربرد و تأمین امنیت ارتباطات
- تأمین ارتباطی امن بین یک وب سرور و یک مرورگر اینترنت
- در سرویس وب با پیشوند **HTTPS** شناخته می‌شود
- نیاز به یک گواهینامه **SSL/TLS**
- پیاده‌سازی و استفاده ایمن از پروتکل **SSL/TLS** دارای جزئیات فنی متعددی است که باید به‌درستی رعایت شوند.
  - پیکربندی ناصحیح این پروتکل می‌تواند خطرات بیشتری نسبت به عدم استفاده از آن در بر داشته باشد

مزایا

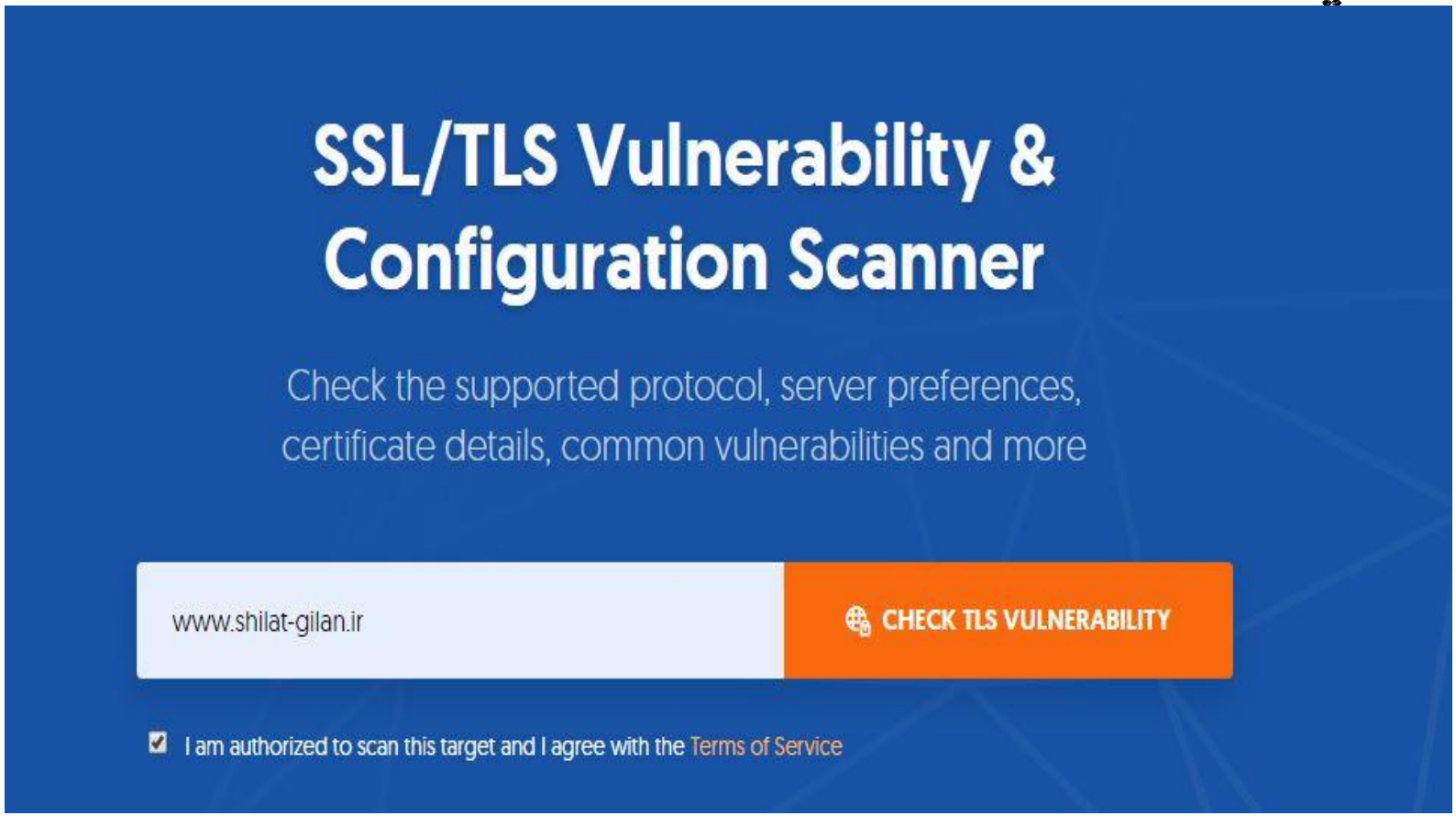
- تامین امنیت ارتباطات و محرمانگی پیام‌ها
- تایید هویت سایت و جلب اعتماد
- کاهش کلاهبرداری و سوء استفاده از کاربران
- افزایش رتبه در گوگل

سایت WWW.SSLLABS.COM

خدمات

- نسخه‌های فعال
- مکانیزم‌های امنیتی
- حملات

سایت GE.DEV


SSL/TLS Vulnerability &
Configuration Scanner
Check the supported protocol, server preferences,
certificate details, common vulnerabilities and more
www.shilat-gilan.ir
CHECK TLS VULNERABILITY
I am authorized to scan this target and I agree with the Terms of Service

WWW.HUBSPOT.COM/SSL-CHECKER

TLS.IMIRHIL.FR/HTTPS

[HTTPS] www.shilat-gilan.ir (Mon, 07 Oct 2019 12:29:52 +0000)

www.shilat-gilan.ir - 136.243.32.122 : 443

Scores A	
Protocol	100 / 100
Key exchange	50 / 100
Cipher	90 / 100
Overall	81.0 / 100

Protocols	TLSv1_2
Keys	Certificats: RSA 2048 bits Diffie Hellman : ECC 256 bits
Good practices	PFS

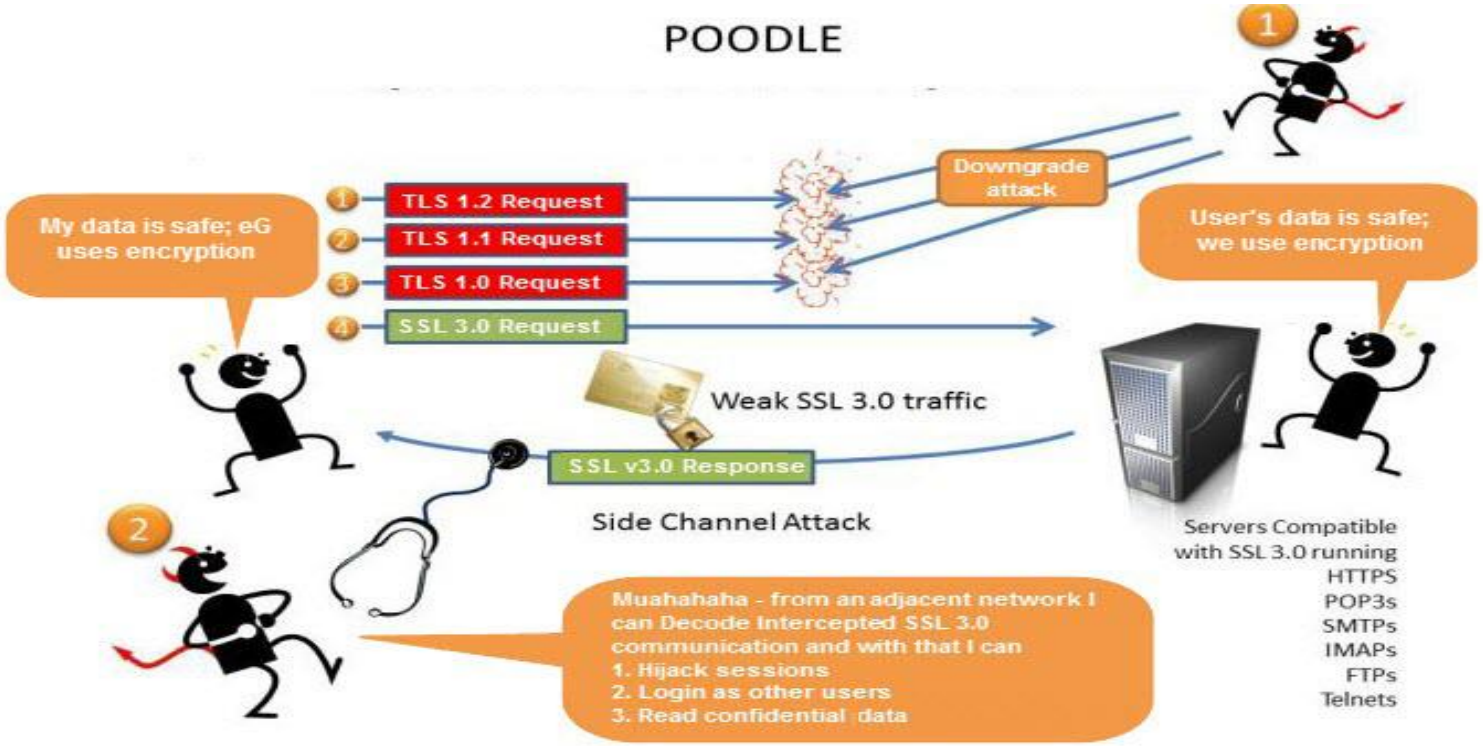
	Key exchange		Authentication		Encryption				MAC		
Name	Type	Key size	Type	Key size	Type	Key size	Block size	Mode	Type	Size	PFS
TLSv1_2											
ECDHE-RSA-AES256-GCM-SHA384	ECDH	256	RSA	2048	AES	256	128	GCM	SHA384	384	PFS
ECDHE-RSA-AES256-SHA384	ECDH	256	RSA	2048	AES	256	128	CBC	SHA384	384	PFS
ECDHE-RSA-AES128-GCM-SHA256	ECDH	256	RSA	2048	AES	128	128	GCM	SHA256	256	PFS
ECDHE-RSA-AES128-SHA256	ECDH	256	RSA	2048	AES	128	128	CBC	SHA256	256	PFS

حملات

- POODLE (SSL3, TLS, Zombie POODLE)
- DROWN
- Heartbleed
- CRIME
- FREAK
- Downgrade
- ROBOT
- RC4

ZOMBIE POODLE و GOLDENDOODLE (CVE-2019-6593)

این دو حمله روی نسخه‌های ۱ تا ۱.۲ **TLS** و در صورتی‌که از حالت رمزنگاری قالبی **CBC** استفاده شود، قابل انجام خواهند بود. این حملات می‌تواند منجر به بازیابی متن اصلی پیام‌های درحال تبادل که مهاجم توسط حمله مردی میانی به آن‌ها دست یافته بدون نیاز به کلید شود.



(CVE-2014-3566) POODLE

- حمله poodle (Padding Oracle On Downgraded Legacy Encryption) یک نوع حمله **man-in-the-middle** است. این حمله از ویژگی بازگشت به **SSL 3.0** که در سرویس‌گیرنده‌های اینترنت و نرم‌افزارهای امنیتی وجود دارد سوءاستفاده می‌کند. اگر مهاجمی بتواند این حمله را با موفقیت انجام دهد با ارسال ۲۵۶ تقاضای **SSL 3.0** محتوای یک بایت از پیام رمز شده را بدست می‌آورد.

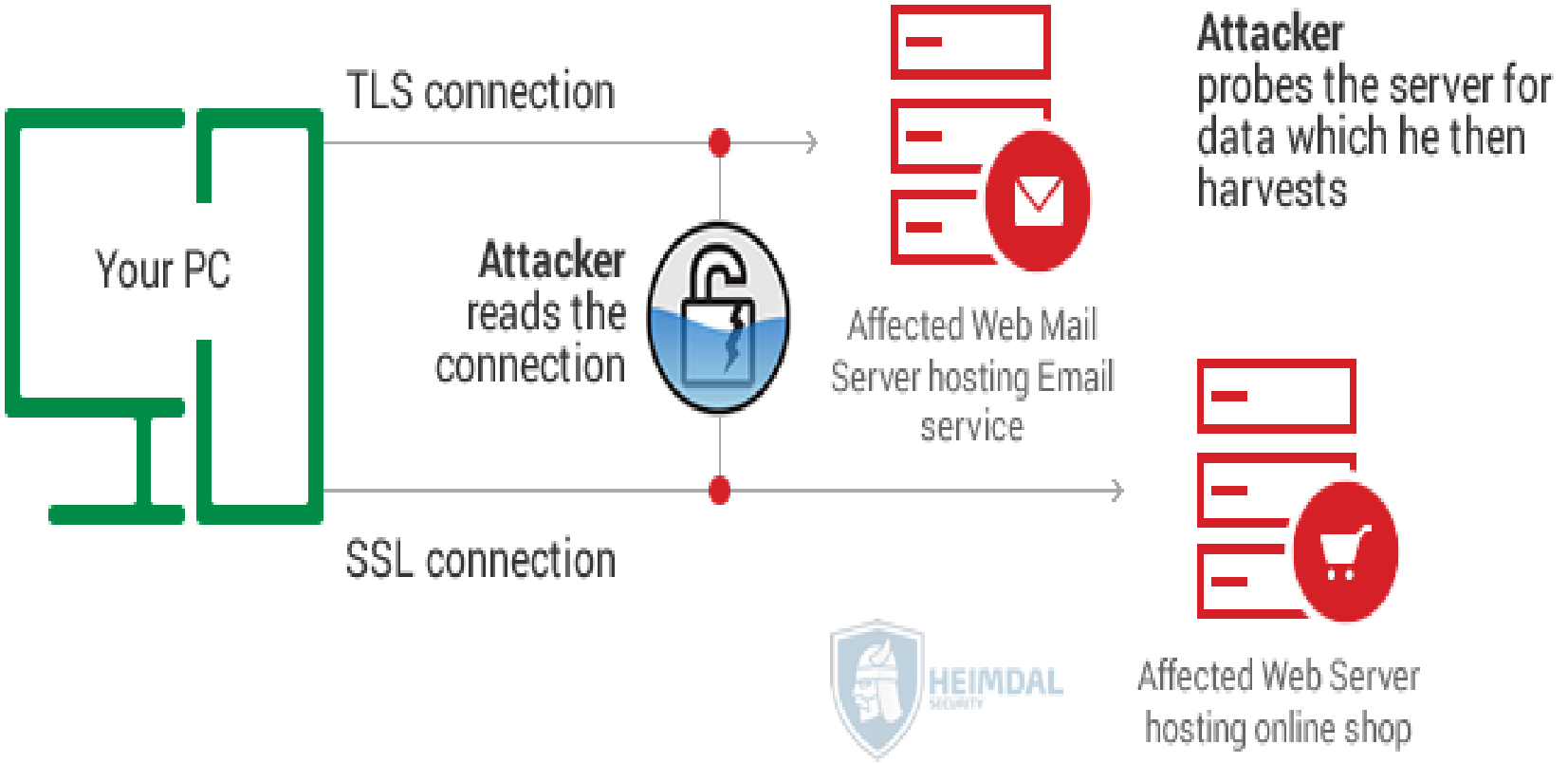
(CVE-2015-3642) POODLE (TLS)

- این حملات مشابه حملات POODLE (SSL3) هستند. این حملات روی برخی پیاده‌سازی‌های TLS که در آن‌ها ساختار padding پس از رمزگشایی بررسی نمی‌شود، رخ می‌دهد. در این حمله برخلاف POODLE (SSL3) نیازی به تغییر ترافیک شبکه و downgrade کاربران به SSL3 نیست و برای حمله تنها کافی است یک کد مخرب JavaScript به مرورگر کاربر تزریق شود. پس از آن، مهاجم با استفاده از ۲۵۶ درخواست می‌تواند یک کاراکتر از کوکی را رمزگشایی نماید. این موضوع بدین معنا است که برای رمزگشایی ۱۶ کاراکتر کوکی تنها نیاز به ۴۰۹۶ درخواست خواهد بود. در صورت وجود آسیب‌پذیری، باید از وصله ارائه شده توسط توزیع‌کننده استفاده شود.

(CVE-2016-0800) DROWN ATTACK

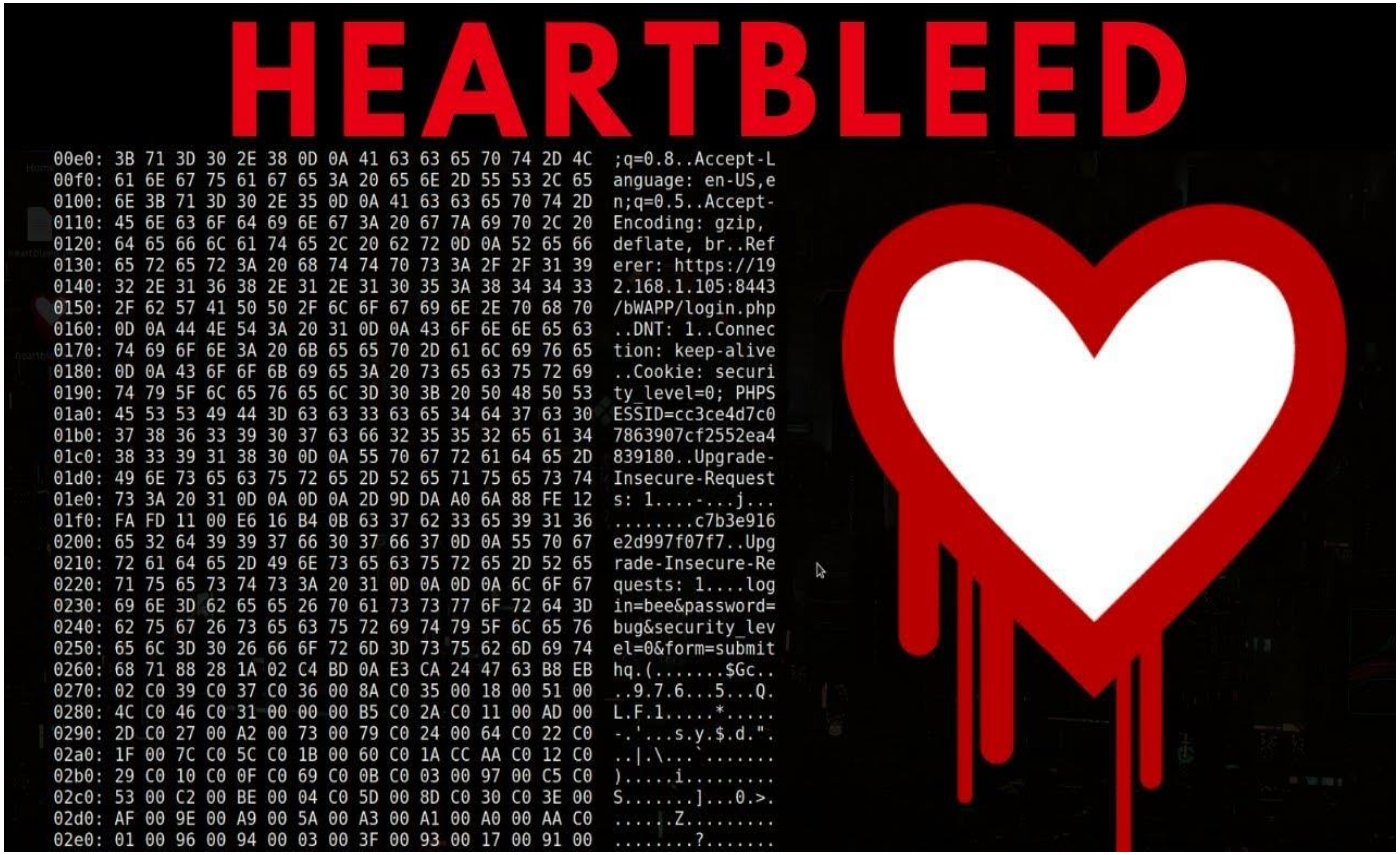
- این حمله یک آسیب‌پذیری جدی است که تمامی ارتباطات **HTTPS**و سرویس‌هایی که از پروتکل **SSL/TLS**بهره می‌برند، تحت تأثیر قرار می‌دهد. در اثر این حمله به مهاجم این اجازه داده می‌شود تا سیستم رمز را شکسته و تمامی اطلاعات و ارتباطات حساس ازجمله رمزهای عبور، شماره‌های حساب و اطلاعات مالی را خوانده و به سرقت ببرد. تحت بعضی سناریوها مهاجم حتی می‌تواند خود را به‌جای یک سرویس امن برای کاربر جا بزند و اطلاعاتی را که کاربر مشاهده می‌کند دست‌کاری نماید.

(CVE-2016-0800) DROWN ATTACK



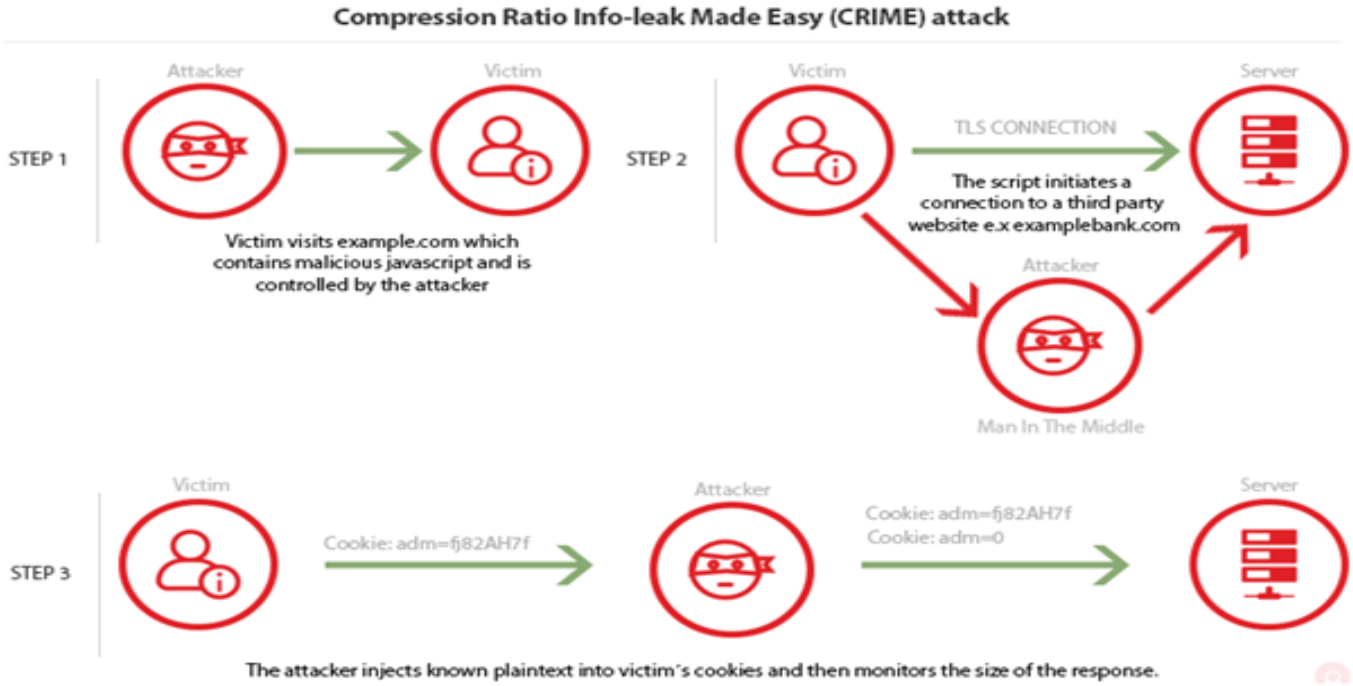
(CVE-2014-0160) HEARTBLEED

یک آسیب‌پذیری در کتابخانه رمزنگاری **OpenSSL** که به مهاجم اجازه خواندن اطلاعات از حافظه رایانه‌ای که در حال اجرای این نرم‌افزار است را از طریق بسته‌های دستکاری شده می‌دهد. این باگ همچنین به مهاجم اجازه بازیابی کلیدهای شخصی اس‌اس‌ال را می‌دهد.



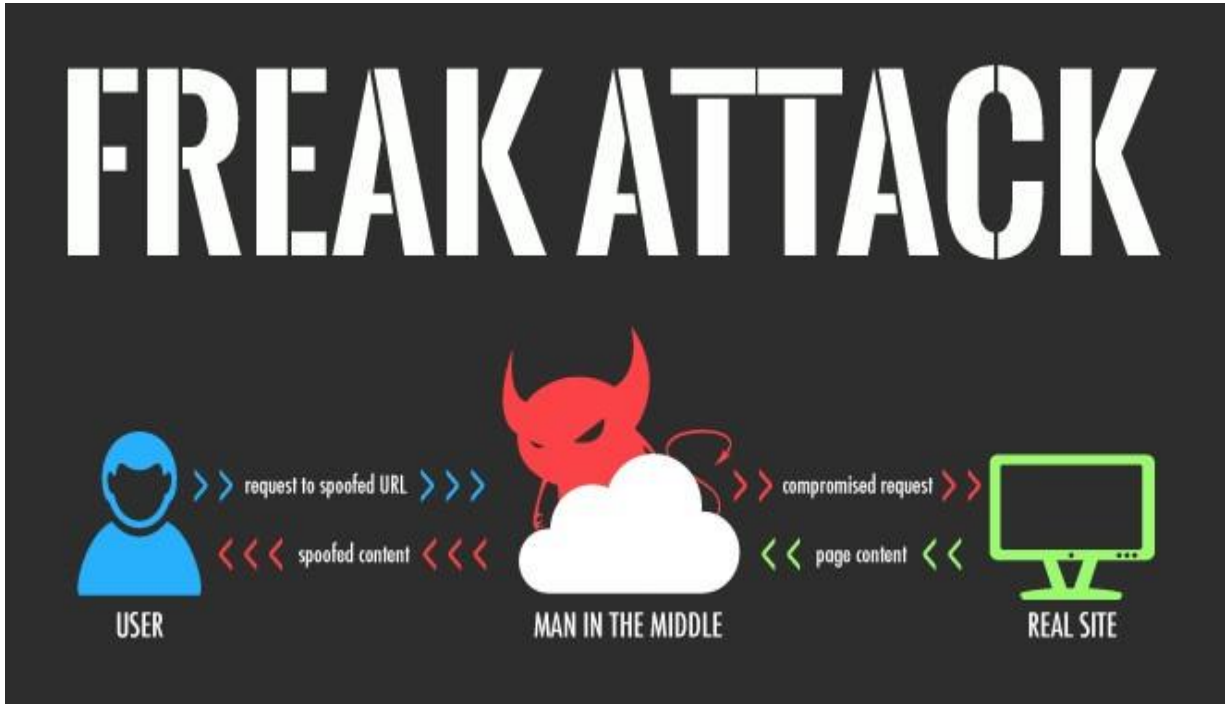
(CVE-2012-4929) CRIME

این حمله که مخفف **Compression Ratio Info-leak Made Easy** است، با سوءاستفاده از آسیب‌پذیری موجود در **TLS Compression** (**CVE-2012-4929**) ممکن می‌شود. در صورت موفقیت حمله، مهاجم می‌تواند یک جلسه تصدیق اصالت شده را **hijack**کند. برای جلوگیری از این حمله توصیه می‌شود ویژگی **TLS Compression** در پیکربندی **TLS**غیرفعال شود

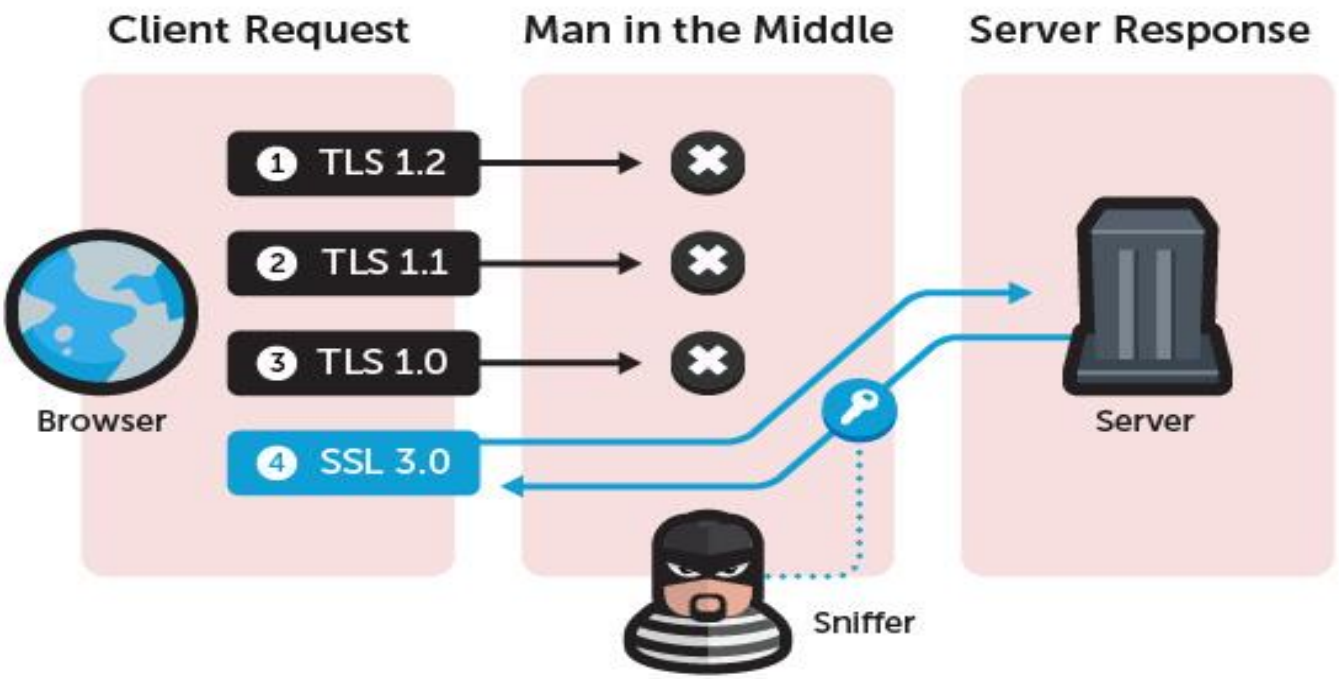


(CVE-2015-2319) FREAK

آسیب پذیری فریک موجب حمله به کلیدهای رمزگذاری RSA-EXPORT از طریق ترافیک دستکاری‌شده می‌دهد.

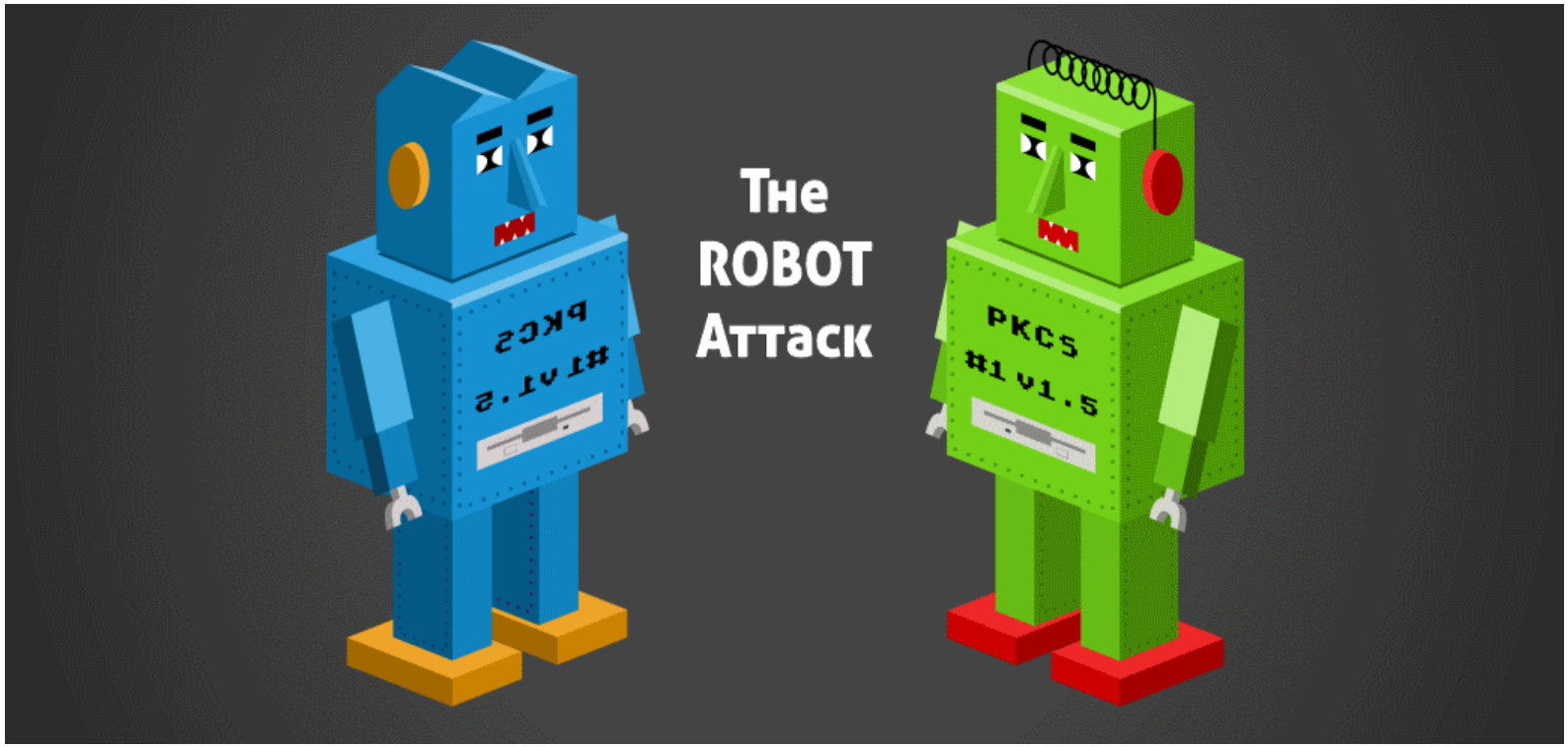


DOWNGRADE


Client Request
Man in the Middle
Server Response
1 TLS 1.2
2 TLS 1.1
3 TLS 1.0
4 SSL 3.0
Browser
Server
Sniffer

(CVE-2017-13099) ROBOT

ROBOT یک آسیب‌پذیری است که به مهاجم امکان رمزگشایی یا امضا با استفاده از کلید خصوصی یک سرور TLS را می‌دهد. این آسیب‌پذیری در استفاده از الگوریتم RSA وجود دارد. در واقع امکان انجام حمله متن رمزشده انتخابی با استفاده پیام‌های خطای سرور TLS به‌وجود می‌آید. این حمله محرمانگی پیام‌های رمزشده با TLS را به کلی از میان می‌برد.



RC4 (CVE-2013-2566 و CVE-2015-2808)

- الگوریتم RC4مورد استفاده در TLS به‌صورت مناسبی اطلاعات وضعیت را با اطلاعات کلید ترکیب نمی‌کند. این مسئله موجب می‌شود مهاجم قادر به بازیابی بایت‌های اولیه پیام جریانی باشد. همچنین در این الگوریتم مهاجم در صورت در اختیار داشتن تعداد زیادی نشست با متن آشکار یکسان، قادر به بازیابی متن آشکار با استفاده از تحلیل آماری متن رمزشده خواهد بود.

(CVE-2016-2183) SWEET32

- امکان انجام حمله روز تولد روی نشست‌های با زمان طولانی در رمزنگاری‌های **DES** و **Triple DES** که در پروتکل‌های **TLS**، **SSH** و **IPSec** استفاده می‌شود، وجود دارد.

(CVE-2016-2107) OPENSSL PADDING ORACLE

- پیاده‌سازی AES-NI در برخی نسخه‌های OpenSSL 1 تخصیص حافظه را هنگام بررسی پد در نظر نمی‌گیرد. این مسئله به مهاجم اجازه می دهد تا از طریق حمله به یک نشست AES CBC، اطلاعات حساسی درباره متن آشکار به‌دست آورد. این آسیب‌پذیری در نتیجه وصله نادرست آسیب‌پذیری CVE-2013-0169 به‌وجود آمده است.

(CVE-2015-4000) LOGJAM

- هنگامی که یک رمزنگاری **DHE_EXPORT** روی سرور فعال باشد در حالی‌که روی کلاینت فعل نباشد، انتخاب **DHE_EXPORT** به درستی منتقل نمی شود. این مسئله به مهاجمان اجازه حمله مرد میانی جایگزینی **DHE_EXPORT** با **DHE** در پاسخ به کلاینت و جایگزینی **DHE** با **DHE_EXPORT** در پاسخ به سرور را می‌دهد. این مسئله موجب کاهش سطح امنیتی رمزنگاری و درنتیجه کاهش محرمانگی تبادل کلید می‌شود.

(CVE-2013-0169) LUCKY13

- در صورتی‌که حملات کانال جانبی زمانی در بررسی **MAC** به‌خوبی بررسی نشود، مهاجم با استفاده از ارسال پد مخرب **CBC** می‌تواند اقدام به بازیابی متن اصلی از طریق تحلیل آماری زمانی داده برای بسته‌های دستکاری شده نماید.

(CVE-2014-0224) CCS

- در برخی نسخه‌های OpenSSL 1 روند محدودسازی پیام‌های ChangeCipherSpec به‌خوبی انجام نشده است. این مسئله به مهاجم اجازه می‌دهد تا با استفاده از حمله مرد میانی استفاده از کلید اصلی با طول صفر را در ارتباطات میان دو OpenSSL فعال نماید. در نتیجه این اقدام، وی می‌توان نشست را سرقت نموده یا از طریق دستکاری TLS Handshake اطلاعات حساسی به‌دست آورد.

(CVE-2016-9244) TICKETBLEED

- یک آسیب‌پذیری در سرور مجازی **BIG-IP** است که امکان به‌دست آوردن ۳۱ بایتی از حافظه غیرمستقیم را می‌دهد. با کمک این آسیب‌پذیری مهاجم می‌تواند شناسه نشست **SSL** را از طریق نشست‌های دیگر و با استفاده از حافظه غیر مستقیم به‌دست آورد.

مکانیزم‌های امنیتی

- Forward Secrecy
- Heartbeat Extension
- OCSP stapling

FORWARD SECRECY

- ویژگی **Forward Secrecy** تضمینی برای عدم افشای کلید جلسه در صورت افشای کلید خصوصی سرویس‌دهنده ایجاد می‌کند. بدون وجود این ویژگی، برای رمزنگاری ارتباط میان سرویس‌گیرنده و سرویس‌دهنده در یک جلسه، ابتدا کلیدی برای رمزنگاری متقارن ایجاد می‌شود. این کلید با کلید عمومی سرویس‌دهنده رمز می‌شود تا محرمانگی آن حفظ شود. اگر کلید خصوصی سرویس‌دهنده افشا شود، کلیه کلیدهای جلسه‌ای که میان سرویس‌دهنده و سرویس‌گیرندگان ایجادشده است افشا خواهد شد.
- در **Forward Secrecy** از الگوریتم مبادله کلید **Elliptic Curve Diffie-Hellman (ECDHE)** برای تبادل کلید میان سرویس‌دهنده و سرویس‌گیرنده استفاده می‌شود. در این الگوریتم کلید جلسه به کلید خصوصی سرویس‌دهنده وابسته نیست. بنابراین مهاجم تنها با بدست آوردن کلید خصوصی سرویس‌دهنده نمی‌تواند کلید جلسه را به دست آورد.

HEARTBEAT EXTENSION

- **Heartbeat Extension**
- افزونه ضربان قلب یک پروتکل جدید برای **TLS/DTLS**است که قابلیت زنده نگه داشتن ارتباط بدون انجام تعاملات اولیه را مهیا می‌کند. برای این منظور طرفین ارتباط از اکوی تعدادی بایت استفاده می‌نمایند.
- **Session Resumption(Caching)**
- یک ویژ گی عملکردی برای کاهش تاخیر درخواست‌های بعدی به همان سرور در طول زمان کوتاه است.
- **Session Resumption(Tickets)**
- یک ویژ گی عملکردی برای کاهش تاخیر درخواست‌های بعدی به همان سرور در طول زمان کوتاه است.

OCSP STAPLING

- OCSP stapling روشی برای بالا بردن سرعت چک کردن لیست ابطال کلید برای گواهی است. با استفاده از OCSP Staplingنیازی نیست که سرویس گیرنده درخواستی به سرور OCSPبدهد. بلکه تنها با استفاده از اطلاعات مهیا شده همراه گواهی می‌تواند از اعتبار (باطل نبودن) گواهی اطمینان حاصل کند.

ابزار های سنجش امنیت SSL پرتال های وب

1. cdn77.com/tls-test
2. geocerts.com/ssl-checker
3. gf.dev/tls-scanner
4. immuniweb.com/ssl
5. ionos.com/tools_ssl-checker
6. **sslcheck.cert.ir**
7. sslchecker.com/sslchecker
8. tls.imirhil.fr/https
9. wormly.com/test_ssl
10. digicert.com/help/
11. hubspot.com/ssl-checker
12. ssllabs.com/ssltest

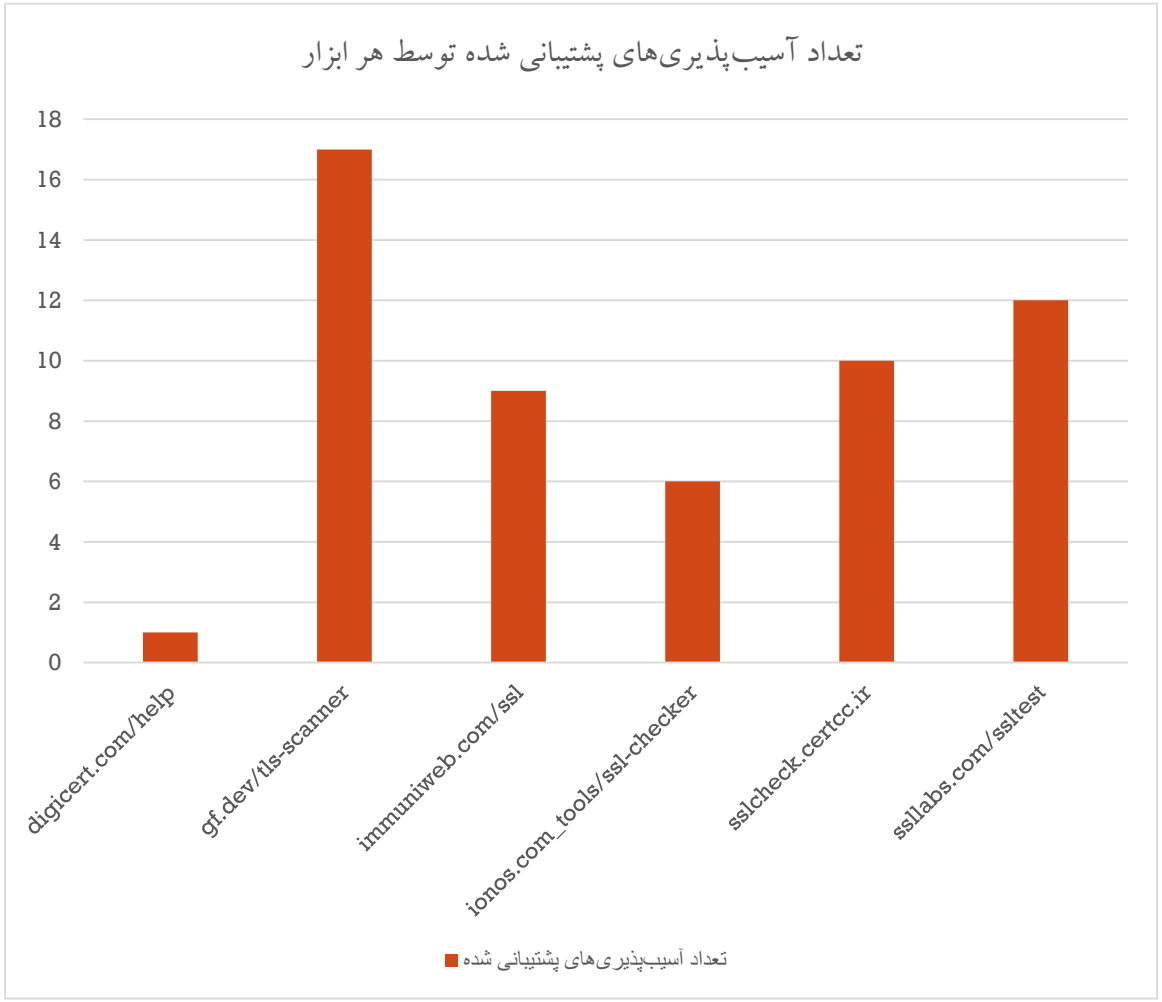
آسیب‌پذیری‌های بررسی شده توسط ابزارهای موجود

آسیب‌پذیری‌های بررسی شده توسط ابزارهای موجود						
حملات	ssllabs.com/ssltest	gf.dev/tls-scanner	immuniweb.com/ssl	sslcheck.certcc.ir	ionos.com_tools/ssl-checker	digicert.com/help
BEAST attack	✓	✓	×	×	✓	×
POODLE (SSL3)	✓	✓	×	✓	✓	×
POODLE (TLS)	✓	×	✓	×	✓	×
Zombie POODLE	✓	×	✓	×	×	×
GOLDENDOODLE	✓	×	✓	×	×	×
OpenSSL 0-Length	✓	×	✓	×	×	×
Sleeping POODLE	✓	×	✓	×	×	×
Heartbleed	✓	✓	✓	✓	✓	✓
Ticketbleed	✓	✓	×	×	×	×
OpenSSL CCS vuln	✓	✓	✓	×	×	×
OpenSSL Padding Oracle	✓	×	✓	✓	×	×
ROBOT	✓	✓	✓	✓	×	×
Secure Renegotiation	×	✓	×	✓	×	×
Secure Client-Initiated Renegotiation	×	✓	×	×	×	×
CRIME	×	✓	✓	×	✓	×
BREACH	×	✓	×	×	×	×
TLS_FALLBACK_SCSV	×	✓	×	×	×	×
SWEET32	×	✓	×	×	×	×
FREAK	×	✓	✓	×	✓	×
DROWN	×	✓	×	×	×	×
LOGJAM	×	✓	×	×	×	×
LUCKY13	×	✓	×	×	×	×
RC4	×	✓	✓	×	×	×

رتبه‌بندی ابزارها براساس آسیب‌پذیری‌های مورد بررسی

رتبه‌بندی ابزارها براساس آسیب‌پذیری‌های مورد بررسی		
رتبه	آدرس سامانه	تعداد آسیب‌پدیری‌های
۱	gf.dev/tls-scanner	۱۷
۲	ssllabs.com/ssltest	۱۲
۳	sslcheck.certcc.ir	۱۰
۴	immuniweb.com/ssl	۹
۵	ionos.com_tools/ssl-checker	۶
۶	digicert.com/help	۱

رتبه‌بندی ابزارها براساس آسیب‌پذیری‌های مورد بررسی

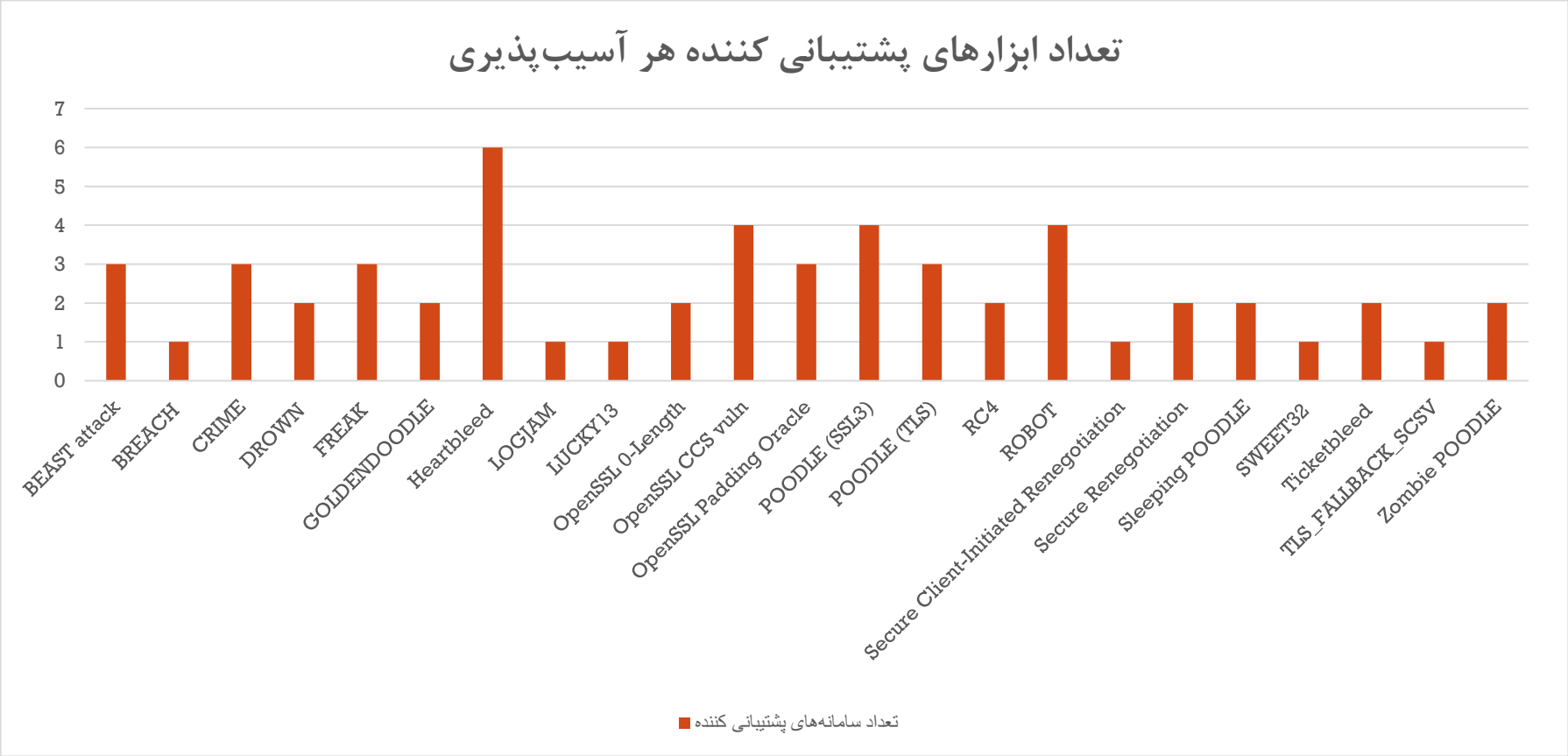


رتبه‌بندی آسیب‌پذیری‌ها بر اساس تعداد ابزارهای پشتیبانی کننده

رتبه‌بندی آسیب‌پذیری‌ها بر اساس تعداد ابزارهای پشتیبانی کننده

رتبه	نام آسیب‌پذیری	آخرین نمرهCVSS	تعداد پشتیبانی کننده	نمره تأثیر آسیب‌پذیری	ابزار پیشنهادی (امتیاز آسیب‌پذیری)	ابزار پیشنهادی (امتیاز کل)
۱	Heartbleed	۷.۵	6	۷.۵	gf.dev	gf.dev
۲	POODLE (SSL3)	۳.۴	4	۱۰.۲	gf.dev	gf.dev
۲	OpenSSL CCS vuln	۷.۴	4	۲۲.۲	gf.dev	gf.dev
۲	ROBOT	۵.۹	4	۱۷.۷	gf.dev	gf.dev
۳	BEAST attack	۴.۳	3	۱۷.۲	gf.dev	gf.dev
۳	POODLE (TLS)	۵.۹	3	۲۳.۶	ssllabs	ssllabs
۳	OpenSSL Padding Oracle	۵.۹	3	۲۳.۶	ssllabs	ssllabs
۳	CRIME	۲.۶	3	۱۰.۴	gf.dev	gf.dev
۳	FREAK	۷.۵	3	۳۰	gf.dev	gf.dev
۴	Zombie POODLE	۵.۹	2	۲۹.۵	ssllabs	ssllabs
۴	GOLDENDOODLE	۵.۹	2	۲۹.۵	ssllabs	ssllabs
۴	OpenSSL 0-Length	۷.۴	2	۳۷	ssllabs	ssllabs
۴	Sleeping POODLE		2		ssllabs	ssllabs
۴	Ticketbleed	۷.۵	2	۳۷.۵	gf.dev	gf.dev
۴	Secure Renegotiation	۵	2	۲۵	gf.dev	gf.dev
۴	DROWN	۵.۹	2	۲۹.۵	gf.dev	gf.dev
۴	RC4	۵.۹	2	۲۹.۵	gf.dev	gf.dev
۵	Secure Client-Initiated Renegotiation	۵	1	۳۰	gf.dev	gf.dev
۵	BREACH	۵	1	۳۰	gf.dev	gf.dev
۵	SWEET32	۷.۵	1	۴۵	gf.dev	gf.dev
۵	LOGJAM	۳.۷	1	۲۲.۲	gf.dev	gf.dev
۵	LUCKY13	۲.۶	1	۱۵.۶	gf.dev	gf.dev

رتبه‌بندی آسیب‌پذیری‌ها بر اساس تعداد ابزارهای پشتیبانی کننده



مکانیزم‌های امنیتی بررسی شده توسط ابزارهای موجود

مکانیزم‌های امنیتی بررسی شده						
حملات	ssllabs.com/ssltest	gf.dev/tls-scanner	immuniweb.com/ssl	sslcheck.certtcc.ir	ionos.com_tools/ssl-checker	digicert.com/help
OCSP stapling support	✓	✓	✓	✓	✓	✓
Forward Secrecy	✓	×	×	✓	×	×
Strict Transport Security	✓	×	×	✓	✓	×
Heartbeat Extension	✓	×	×	✓	✓	×
Session Resumption(Caching	✓	×	×	✓	✓	×
Session Resumption(Tickets	✓	×	×	✓	✓	×
OSCP Must Estaple	×	✓	✓	×	×	×

راه‌اندازی سرویس SSL/TLS

- انتخاب یک مرکز صدور گواهی بین‌المللی و رابط/نماینده آن در ایران
- انتخاب نوع گواهی مورد نظر
- تولید کلیدهای رمزنگاری و Certificate Signing Request (CSR)
- بررسی درخواست شما توسط مرکز صدور گواهی و صدور گواهی
- نصب گواهی و کلیدهای رمزنگاری روی سرویس‌دهنده

مرکز آپای دانشگاه گیلان

مرکز ماهر

وزارت ارتباطات و فناوری اطلاعات
سازمان فناوری اطلاعات ایران

انتخاب یک مرکز صدور گواهی بین‌المللی

LET'S ENCRYPT

مرکز آپای دانشگاه گیلان

مرکز ماهر

وزارت ارتباطات و فناوری اطلاعات
سازمان فناوری اطلاعات ایران

معرفی مرکز آپای دانشگاه گیلان

آشنایی اولیه

- آپا مخفف واژه‌های آگاهی‌رسانی، پشتیبانی و امداد
- معادل **CERT** یا **CSIRT**
- پیشینه ایجاد و راهبری مراکز امداد امنیت رایانه‌ای به سال ۱۹۸۸ و انتشار گسترده کرم موریس بر می‌گردد.
- آلودگی ۶۰ تا ۸۰ هزار رایانه در شبکه اینترنت آن زمان (آرپانت)، تقریبا ۱۰٪ کل رایانه‌های موجود
- انستیتوی مهندسی نرم‌افزار دانشگاه **Carnegie Mellon** به عنوان میزبان اولین مرکز **CERT** انتخاب شد.

مرکز آپای دانشگاه گیلان

مرکز ماهر

وزارت ارتباطات و فناوری اطلاعات
سازمان فناوری اطلاعات ایران

تاریخچه تاسیس در دانشگاه گیلان

- شروع فعالیت های پژوهشی
- پیگیری های اخذ مجوز
- راه اندازی مرکز
- www.cert.guilan.ac.ir

گواهی‌نامه راه‌اندازی مرکز آپای دانشگاه گیلان

به استناد اقدام چهارم از راهبرد دوم سند افتا و نظام ملی مقابله با حوادث رایانه‌ای، همچنین نظر به اهمیت و ضرورت راه‌اندازی و گسترش مراکز همکار در زمینه تشخیص، تحلیل و هماهنگی ملی پاسخ به حوادث امنیتی رایانه‌ای، و با توجه به ظرفیت‌های ایجاد شده در :

دانشگاه گیلان

مرکز آگاهی‌رسانی، پشتیبانی و امداد رایانه‌ای (آپا) دانشگاه گیلان به عنوان یکی از مراکز همکار مرکز ملی مدیریت امداد و هماهنگی رخدادهای رایانه‌ای (ماهر) اعلان می‌گردد.

آدرس: رشت، بلوار حافظ، خیابان ملت، روبروی پارک قدس، پردیس دانشگاهی دانشگاه گیلان

(013-33341952 09377369935)

آگاهی رسانی

- اعلان آسیب‌پذیری‌های مهم
- صدور هشدارهای مهم
- رصد و اعلان اخبار و رویدادهای مهم
- انتشار اطلاعیه در خصوص فعالیت‌های مرکز
- انتشار مطالب علمی و آموزشی
- انتشار مقاله سفید
- انتشار راهنمای امن‌سازی
- انتشار تحلیل آسیب‌پذیری

آموزش

- مدیریت آسیب‌پذیری
- مدیریت حوادث
- امن‌سازی پایه
- آفند و پدافند
- امنیت نرم‌افزار

خدمات تحلیل

- تحلیل آسیب‌پذیری: تحلیل و بررسی تکنیکی آسیب‌پذیری در سخت افزار یا نرم افزارها
- تحلیل دسیسه: تحلیل و بررسی تکنیکی بر روی هر دسیسه‌ای که روی یک سیستم پیدا می‌شود.
- تحلیل حادثه: بازرسی کردن کلیه اطلاعات در اختیار و کلیه شواهد و دسایس در ارتباط با حادثه
- تولید هشدار: منتشر کردن اطلاعاتی که حمله‌ی یک مهاجم، آسیب‌پذیری امنیتی، هشدار نفوذ و یا یک ویروس کامپیوتری را توصیف می‌کند و به همراه آن توصیه‌هایی نیز برای مقابله با مشکلات احتمالی منتشر می‌شود.

خدمات ارزیابی

- ارزیابی زیرساخت: این فعالیت شامل بررسی تنظیمات سخت‌افزار، نرم‌افزار، مسیریاب‌ها، **firewall**ها، **server**ها و سیستم‌های **desktop** برای حصول اطمینان از این است که این تنظیمات مطابق با سیاست‌های سازمان و تنظیمات استاندارد صورت گرفته است.
- تست نفوذ: این فعالیت شامل بررسی تنظیمات سخت‌افزار، نرم‌افزار، مسیریاب‌ها، **firewall** ها، **server** ها و سیستم‌های **desktop** برای حصول اطمینان از این است که این تنظیمات مطابق با سیاست‌های سازمان و تنظیمات استاندارد صورت گرفته است.
- پویش: در این فعالیت از ابزارهای پویش ویروس‌ها یا آسیب‌پذیری‌ها استفاده می‌شود تا سیستم‌ها و یا شبکه‌های آلوده یا آسیب‌پذیر تشخیص داده شوند.

خدمات عملیات

- دو دسته فعالیت توسط اعضای تیم عملیات در واحد فنی و عملیات این مرکز انجام می‌شود:

- رسیدگی به حادثه: رسیدگی به حادثه شامل دریافت و پاسخ‌گویی به یک درخواست یا گزارش و تحلیل حوادث و رخ‌دادها است.
- رسیدگی به آسیب‌پذیری: رسیدگی به آسیب‌پذیری شامل دریافت اطلاعات و گزارش‌ها درباره آسیب‌پذیری‌های سخت‌افزارها و نرم‌افزارها، تحلیل منشا آن‌ها، نحوه عملکرد و چگونگی تاثیر آسیب‌پذیری‌ها و ایجاد راه‌کارهایی برای تشخیص و ترمیم آسیب‌پذیری‌ها است.

خدمات تحقیقاتی (۱/۲)

- خلاقیت بر پایه ایده‌ها و مفاهیم به‌دست آمده از مباحث و فرصت‌ها در زمینه امنیت فن آوری اطلاعات و شبکه
- کمک به تبیین استراتژی‌های سازمان در زمینه امنیت فن آوری اطلاعات و شبکه
- سازماندهی و اجرای پروژه‌های تحقیق و توسعه مبتنی بر استراتژی‌های مرکز
- بررسی زمینه‌های کاری رقبا و مشتریان در زمینه امنیت فن‌آوری اطلاعات و شبکه
- عملیات تحقیق و توسعه

خدمات تحقیقاتی (۲/۲)

- اجرا و مستندسازی کارهای مبتنی بر تحقیق و توسعه شامل جستجو و جمع‌آوری اطلاعات مورد نیاز در زمینه امنیت فناوری اطلاعات و شبکه
- مشاوره و همکاری با سایر واحدها
- بررسی و ارزیابی پیشنهادات و نیازهای اعلام شده توسط پروژه‌ها و همکاری در تعیین راه حل مطلوب و اجرای آن‌ها
- طراحی و پیشنهاد پروژه‌های آتی مرکز
- طراحی و حمایت پروژه‌های کارشناسی، کارشناسی ارشد و دکترا در حوزه امنیت فناوری اطلاعات و شبکه

خدمات توسعه

- تیم توسعه‌ی مرکز تخصصی آپا دانشگاه گیلان به منظور رفع نیاز داخلی خود و همچنین رفع نیاز سازمان‌های تحت پوشش، توانایی تحلیل، طراحی و پیاده‌سازی ابزارها و نرم‌افزارهای ضروری در حوزه‌ی امنیت را دارد.
  - تولید ابزارهای امن‌سازی بستر توسعه و منبع پروژه‌ها در سیستم‌های کنترل صنعتی ICS
  - تولید وصله‌های امنیتی برای نرم‌افزارهای اختصاصی که توسط مرکز آپا یا سازمان‌های تحت پوشش استفاده می‌شوند.
  - تولید کد یا ابزارهایی برای بهبود عملکرد ابزارهای امنیتی موجود (برای مثال تولید افزونه‌هایی برای پویش‌گرهای شبکه)
  - تولید نرم‌افزارهایی جهت توزیع میان افراد سازمان برای بازیابی سیستم‌ها پس از یک حادثه
  - ایجاد مکانیزم‌هایی برای توزیع اتوماتیک وصله‌های نرم‌افزاری

بیانیه عملیاتی مرکز آپا دانشگاه گیلان

امنیت شبکه‌های رایانه‌ای و سامانه‌های نرم‌افزاری و سخت افزاری مورد کاربرد در تبادل اطلاعات و ارتباطات، امروزه بعنوان دغدغه ای بسیار پر اهمیت برای تمامی کاربران فضای سایبری خصوصا مدیران ارشد حوزه فناوری اطلاعات و ارتباطات کشور تبدیل شده است. مرکز آپای دانشگاه گیلان در بدو تاسیس خود را موظف می داند تا در راستای سیاست‌های ابلاغی نظام توسط مقم معظم رهبری در امور امنیت فضای تولید و تبادل اطلاعات و ارتباطات تمامی توصیه‌ها و روال‌های آگاهی‌رسانی و آموزش را به تمامی ادارات و دستگاه ها استان گیلان و همچنین استان های همجوار در دستور کار خود قرار دهد. این مرکز علاوه خدمت رسانی در حوزه های عمومی مراکز آپا در خصوص خدمات فنی و عملیاتی، با عنوان تخصصی "***امنیت سامانه های سخت افزاری و هوشمند***" با تمرکز بیشتر روی آسیب پذیری های سخت افزاری بستر های پردازشی و ارتباطی داده بدنبال شناسایی، تحلیل و ارزیابی سخت افزار های مورد استفاده در حوزه فتا خواهد بود.

پرسش و پاسخ