



فصل پنجم: IPSec

امنیت سیستم‌های کامپیوتری

ابوالفضل دیانت

آخرین ویرایش: ۱۷ اردیبهشت ۱۴۰۲ در ساعت ۱۳ و ۱۲ دقیقه - نسخه 1.0.1

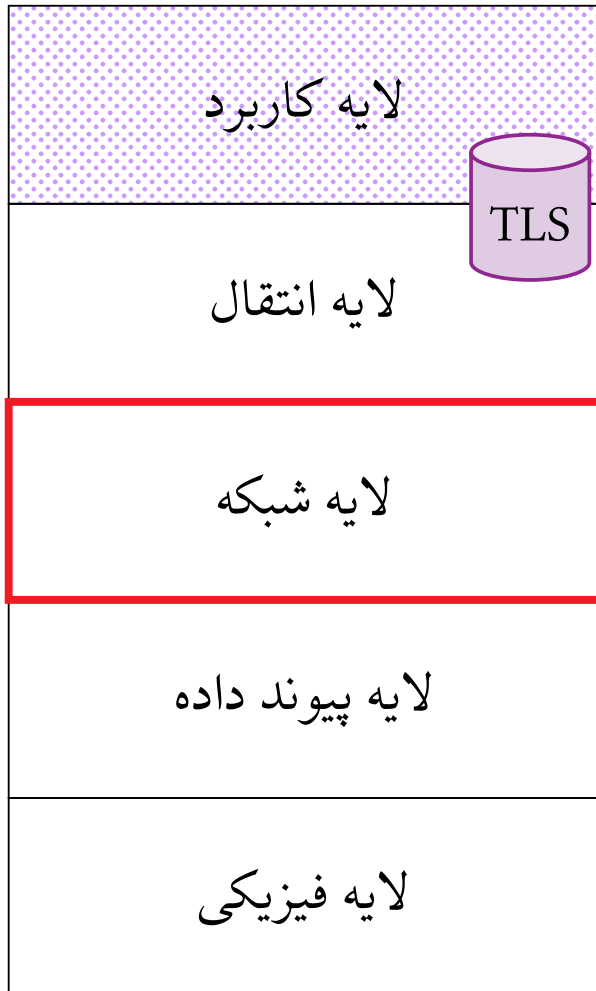
این پیوند مفید است و مطالب را خیلی خوب توضیح داده است. 

ویدئوهای آقای Keith Barker در Youtube نیز مفید است: 

- IPsec Site to Site VPN tunnels
- IPsec Site to Site VPN Tunnels Explained

IPSec

امنیت می تواند در لایه کاربرد (PGP) یا بین لایه کاربرد و لایه انتقال (TLS) باشد.




IPSec

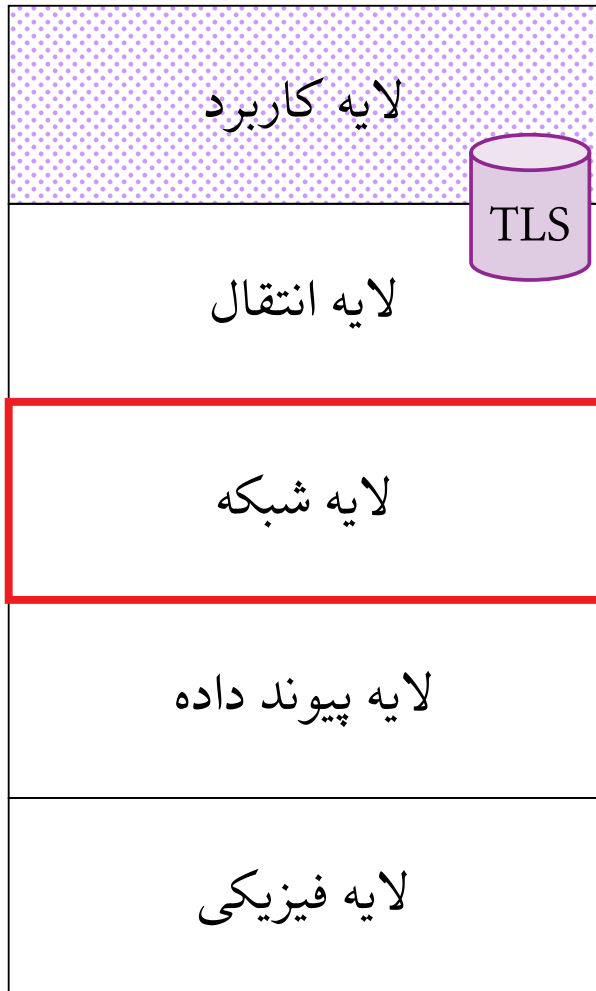
تعریف ۱


گروهی از پروتکل ها که می توان امنیت (حفظ محرمانگی + احراز اصالت + تامین یکپارچگی) را در لایه شبکه تامین کند، و یک تونل امن در یک شبکه ناامن برای ما ایجاد کند.


● **Transport Mode:** فقط محتوا (Payload) لایه شبکه رمز می شود.

● **Tunnel Mode:** کل بسته IP رمز می شود.

در Tunnel Mode، چگونه عملیات مسیریابی انجام می شود؟ 



چرا امنیت در لایه‌های مختلف؟ 

در TLS برنامه کاربردی باید تغییر کند، ولی در IPsec باید سیستم عامل تغییر کند. 

در حالت کلی پیچیده تر از TLS است. 

اکثر (Virtual Private Network) VPN ها ولی نه همه آنها از پروتکل IPSec بهره می گیرند.

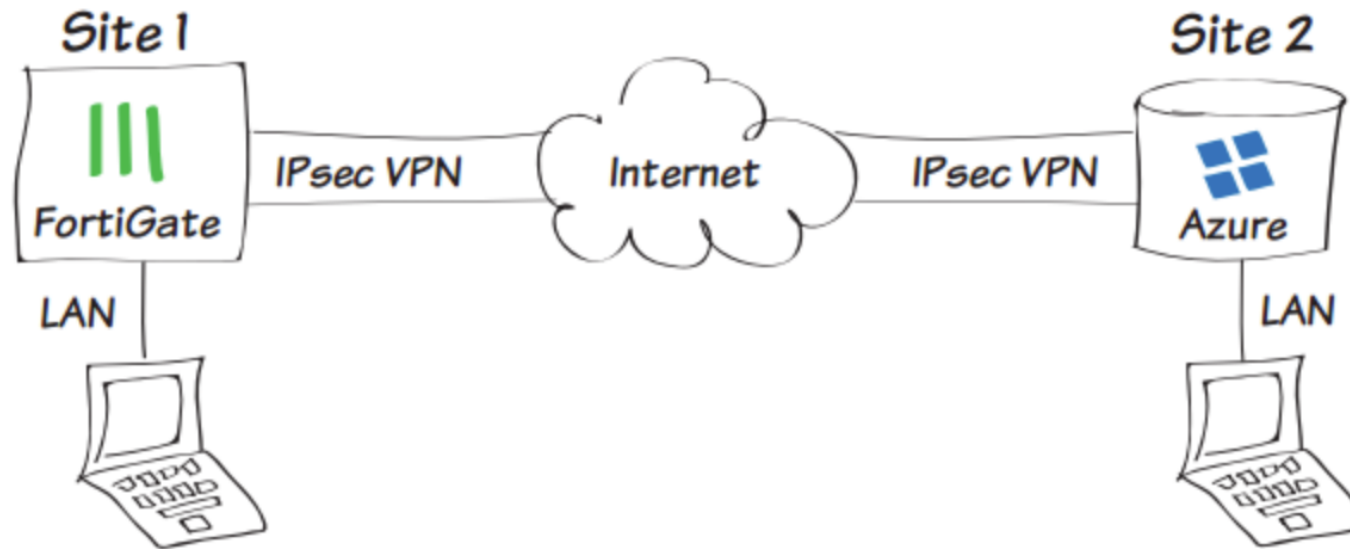
```

▶ Ethernet II, Src: 82:9a:ef:74:94:79 (82:9a:ef:74:94:79), Dst: 4a:67:bb:57:e7:fb
▼ Internet Protocol Version 4, Src: 192.168.42.168, Dst: 45.94.254.24
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
    ▼ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
        0000 00.. = Differentiated Services Codepoint: Default (0)
        .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 52
    Identification: 0x2daf (11695)
    ▼ Flags: 0x40, Don't fragment
        0... .... = Reserved bit: Not set
        .1.. .... = Don't fragment: Set
        ..0. .... = More fragments: Not set
    Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0xf64d [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.42.168
    Destination Address: 45.94.254.24
▶ Transmission Control Protocol, Src Port: 47696, Dst Port: 443, Seq: 2211, Ack: 2

```

0000	4a 67 bb 57 e7 fb 82 9a ef 74 94 79 08 00 45 00	Jg·W····· ·t·y··E·
0010	00 34 2d af 40 00 40 06 f6 4d c0 a8 2a a8 2d 5e	·4-·@·@· ·M··*·-^
0020	fe 18 ba 50 01 bb 28 1c 0d 02 c9 86 94 7e 80 10	··P··(· ·····~··
0030	02 62 2c 9b 00 00 01 01 08 0a f4 d4 6d 8a a1 b8	·b, ····· ····m··
0040	dd b1	··

کاربردها



● **Host To Host**: یک میزبان (Host) می‌خواهد به صورت امن به خدمت‌گزار (Server) وصل شود.

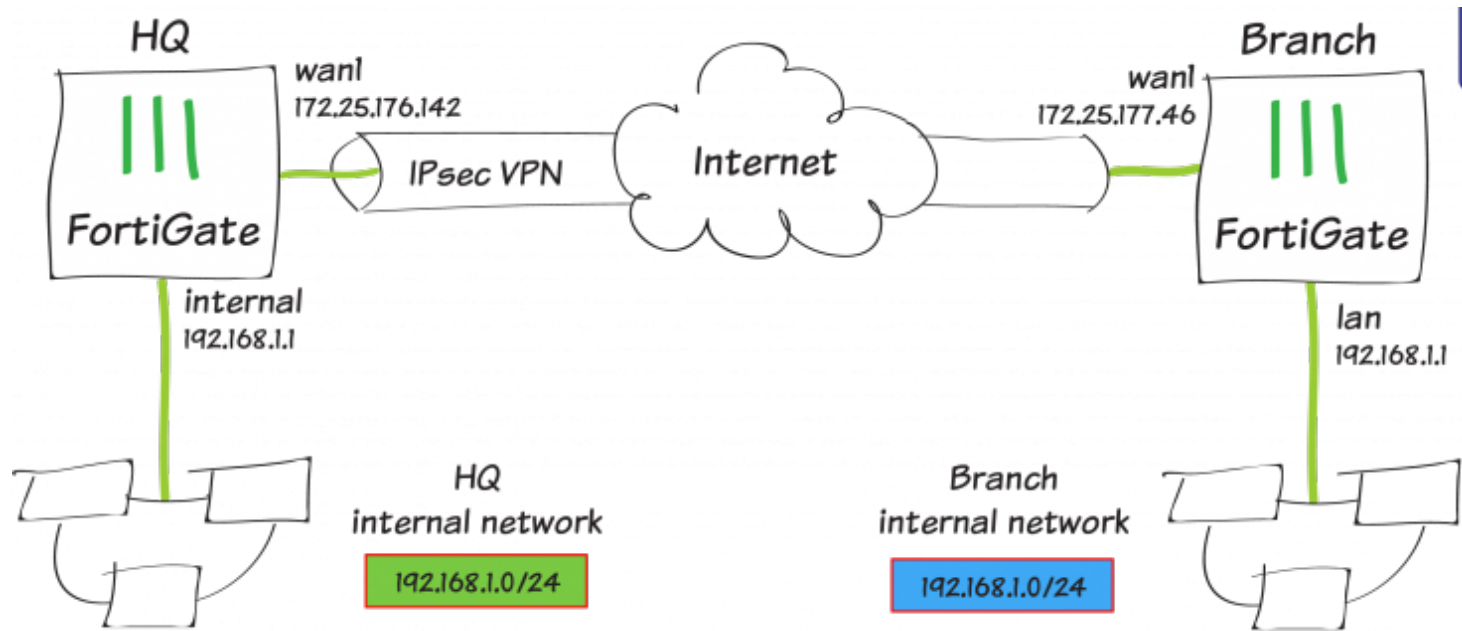
● **Host To Network**: فرض کنید شما می‌خواهید به صورت امن به عنوان یک میزبان (Host) به شبکه دانشگاه

متصل شوید و به طور کامل به عنوان جزئی از این شبکه محسوب گردید.

● **Network To Network**: دو یا چند شبکه به صورت امن از طریق یک بستر ناامن به یکدیگر متصل می‌شوند.

چند شبکه مجزا در نقاط مختلف ولی این‌ها فکر می‌کنند در یک شبکه Local هستند.

خدمات IPSec



✓ رمزگذاری بسته‌ها و جریان ترافیک (Traffic Flow)

✓ تامین یکپارچگی (Integrity)

✓ فرایند احراز اصالت (Authentication) و تبادل کلید (Key Exchange)

✓ تضمین تازگی (Freshness) پیام و جلوگیری از حمله حمله بازپخش (Replay Attack)

📌 پروتکل IPSec دو مرحله کلی دارد:

❶ پیمان امنیتی (Security Association): مجموعه‌ای از پروتکل‌ها برای مذاکره در مورد پارامترها و الگوریتم‌های

تامین امنیت. به عنوان نمونه به IKE می‌توان اشاره کرد RFC2409 - IKEv1 (1998) و - IKEv2 (2005) RFC7296.

❷ تامین امنیت:

● **ESP (Encapsulating Security Payload) (RFC 4303):** رمزگذاری (Encryption) و/یا یکپارچگی


(Integrity) با ارایه خدماتی نظیر احراز اصالت، یکپارچگی و جلوگیری از حمله بازپخش

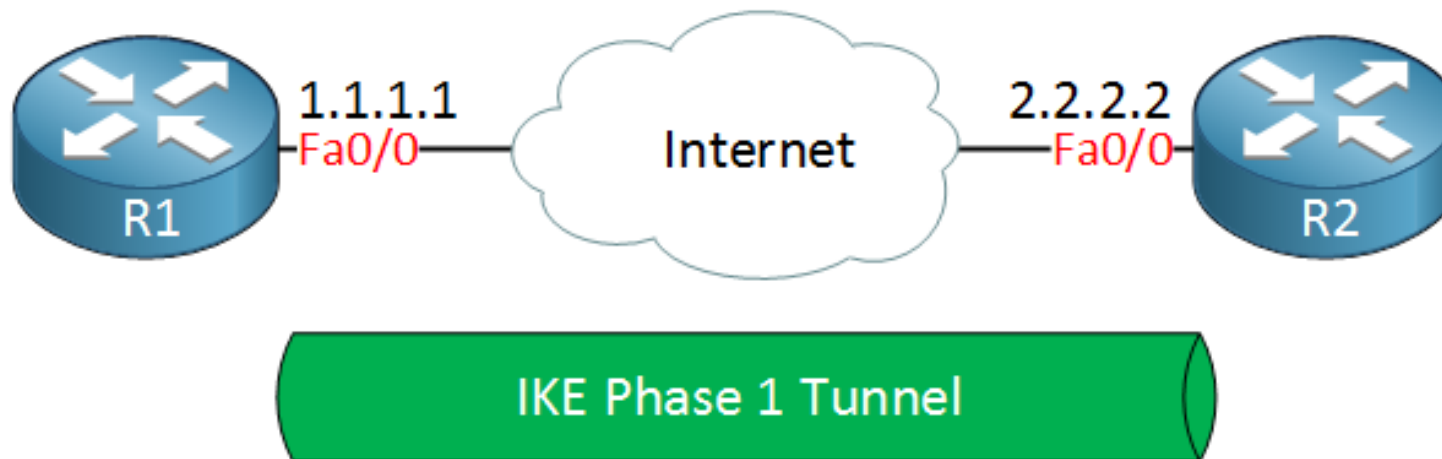
● **AH (Authentication Header) (RFC 4302):** تنها یکپارچگی (Integrity) که به منظور احراز اصالت،

یکپارچگی و جلوگیری از حمله بازپخش استفاده می‌شود.

ایجاد تونل (ISAKMP (Search Results Internet Security Association and Key Management Protocol) 

برای مدیریت ترافیک

صحبت در مورد الگوریتم تبادل کلید، رمزگذاری، تابع چکیده ساز، احراز اصالت و طول عمر 



مراحل IPSec - فاز اول IKE

```

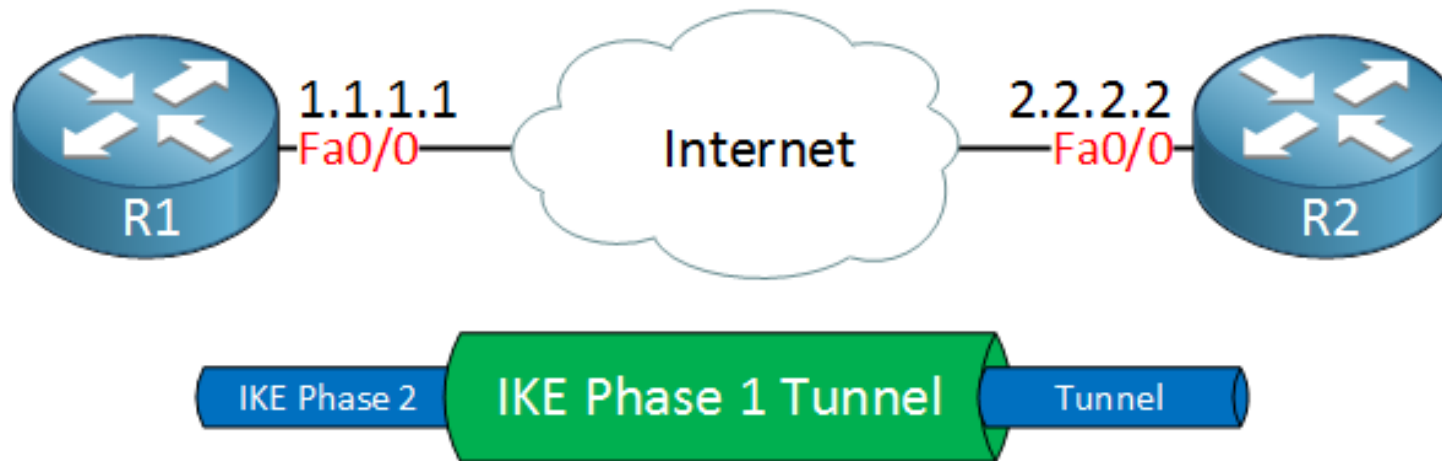
Ethernet II, Src: Cisco_8b:36:d0 (00:1d:a1:8b:36:d0), Dst: Cisco_ed:7a:f0 (00:17:5a:ed:7a:f0)
+ Internet Protocol Version 4, Src: 192.168.12.1 (192.168.12.1), Dst: 192.168.12.2 (192.168.12.2)
+ User Datagram Protocol, Src Port: 500 (500), Dst Port: 500 (500)
- Internet Security Association and Key Management Protocol
  Initiator SPI: e47a591fd057587f
  Responder SPI: 0000000000000000
  Next payload: Security Association (1)
+ Version: 1.0
  Exchange type: Identity Protection (Main Mode) (2)
+ Flags: 0x00
  Message ID: 0x00000000
  Length: 168
- Type Payload: Security Association (1)
  Next payload: Vendor ID (13)
  Payload length: 60
  Domain of interpretation: IPSEC (1)
+ Situation: 00000001
- Type Payload: Proposal (2) # 1
  Next payload: NONE / No Next Payload (0)
  Payload length: 48
  Proposal number: 1
  Protocol ID: ISAKMP (1)
  SPI Size: 0
  Proposal transforms: 1
- Type Payload: Transform (3) # 1
  Next payload: NONE / No Next Payload (0)
  Payload length: 40
  Transform number: 1
  Transform ID: KEY_IKE (1)
+ Transform IKE Attribute Type (t=1,l=2) Encryption-Algorithm : AES-CBC
+ Transform IKE Attribute Type (t=14,l=2) Key-Length : 128
+ Transform IKE Attribute Type (t=2,l=2) Hash-Algorithm : SHA
+ Transform IKE Attribute Type (t=4,l=2) Group-Description : Alternate 1024-bit MODP group
+ Transform IKE Attribute Type (t=3,l=2) Authentication-Method : PSK
+ Transform IKE Attribute Type (t=11,l=2) Life-Type : Seconds
+ Transform IKE Attribute Type (t=12,l=4) Life-Duration : 86400
+ Type Payload: Vendor ID (13) : RFC 3947 Negotiation of NAT-Traversal in the IKE
+ Type Payload: Vendor ID (13) : draft-ietf-ipsec-nat-t-ike-07
+ Type Payload: Vendor ID (13) : draft-ietf-ipsec-nat-t-ike-03
+ Type Payload: Vendor ID (13) : draft-ietf-ipsec-nat-t-ike-02\n
```

این برای IKEv1 است، که در حالت MainMode شش پیام باید مبادله شود، اما در IKEv2 ما تنها کافی است چهار پیام مبادله شود.

مراحل IPsec - فاز دوم IKE

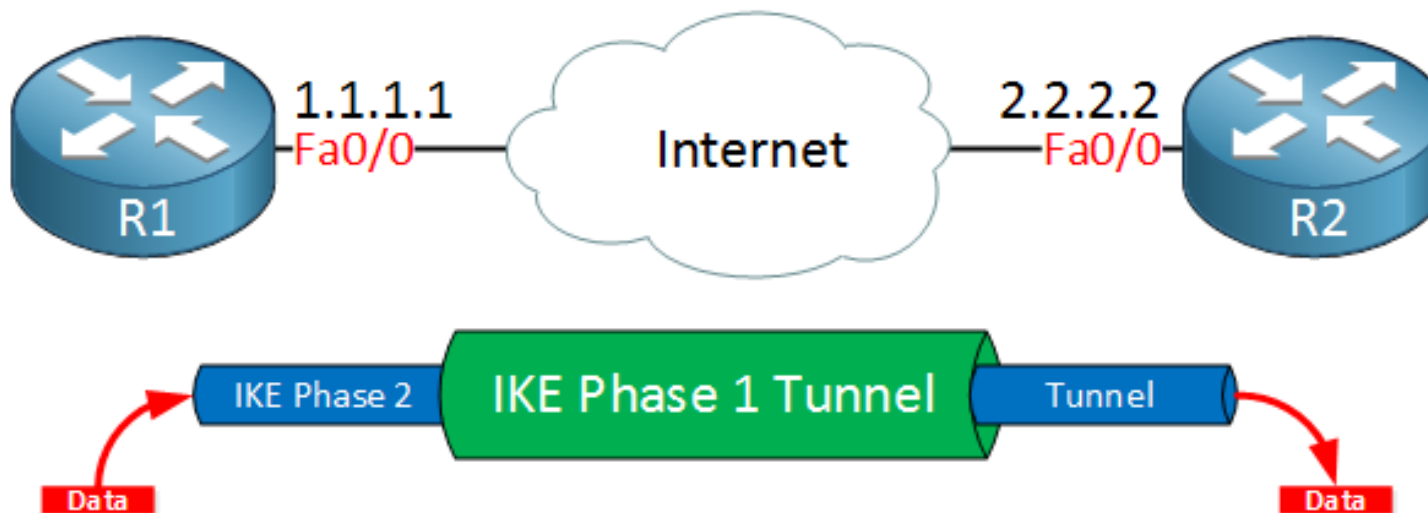
ایجاد تونل (Internet Key Exchange) IKE و مبادله سه پیام به منظور توافق بر روی IPsec Policy

توافق بر روی (AH or ESP) Mode، رمزگذاری و تابع چکیده ساز



مراحل IPSec - تبادل داده

📌 در این مرحله تبادل داده می‌تواند صورت بپذیرد. البته همان‌طور که قبلاً گفته شد، دو حالت با عناوین AH (Authentication Header) و ESP (Encapsulating Security Payload) داریم.



Authentication Header (AH)

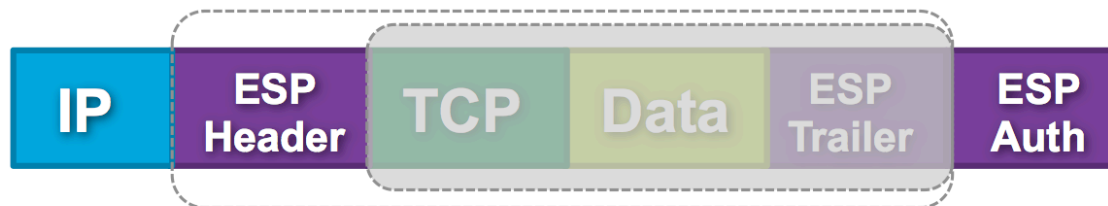


Transport Mode

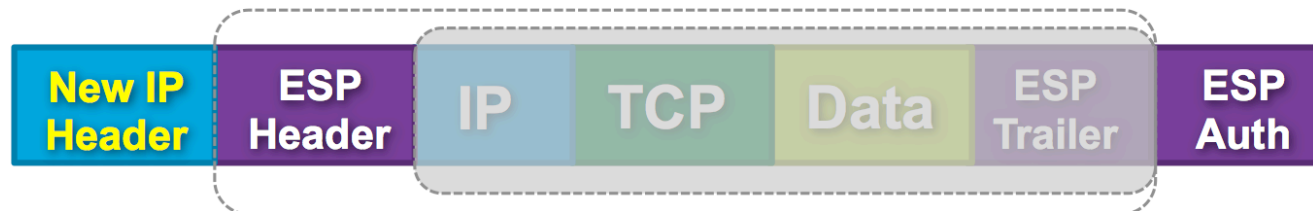


Tunnel Mode

Encapsulating Security Payload (ESP)



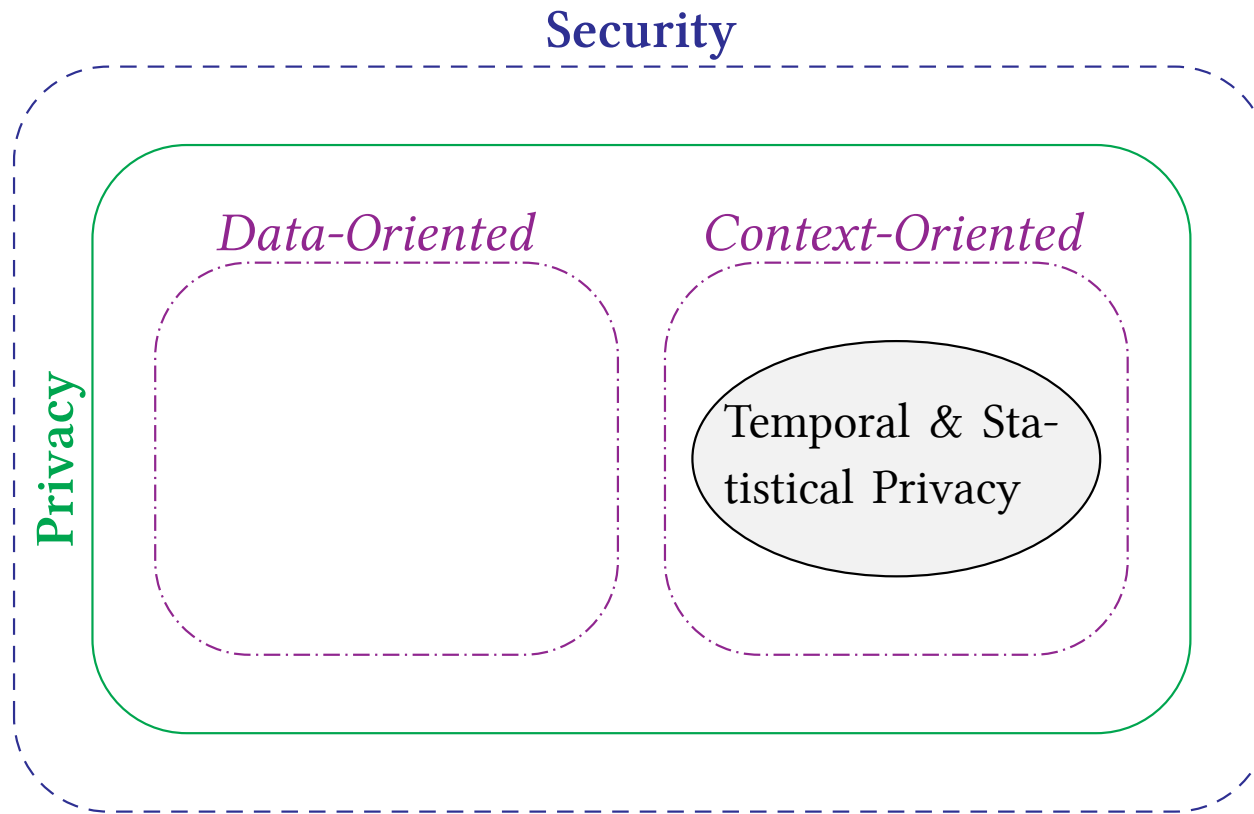
Transport Mode



Tunnel Mode

حریم خصوصی

تا مدت‌ها نگاه ما به امنیت به سه گانه C-I-A خلاصه می‌گشت، اما با گذر زمان مفاهیم جدیدی نظیر تازگی، انکارناپذیری، گمنامی و حریم خصوصی نیز مطرح گشت و جای خود را در این حوزه پیدا کرد.

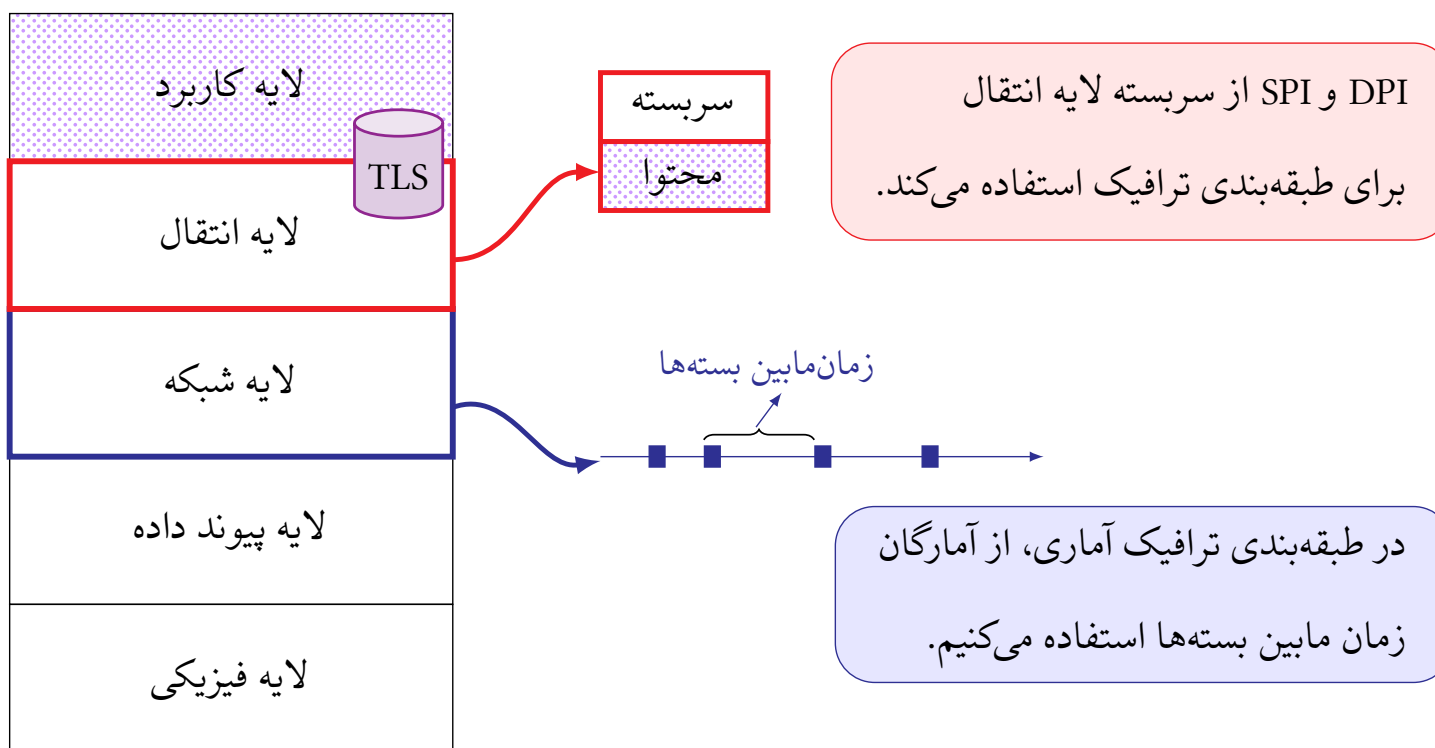


حریم خصوصی را می‌توان در دو دسته مبتنی بر داده و مبتنی بر اطلاعات جانبی طبقه‌بندی نمود [۱]، بخش 12.4.1، [۲، صفحه ۲۰۲]. نقطه تمرکز حریم خصوصی مبتنی بر داده، بر روی محتوای داده است و بدین‌سان سازوکارهایی نظیر رمزگذاری، یکپارچگی و غیره برای تامین چنین نیازی کارا و کافی خواهد بود. در این دسته بالعکس دسته نخست، هدف غایی کسب اطلاعات جانبی از داده‌ها است. فرض کنید جلسه‌ای محرمانه بین دو نفر تشکیل شده است. در این نوع از حریم خصوصی، محتوای داده (صحبت‌هایی که در جلسه مطرح شده) برای ما اهمیت ندارد، بلکه اطلاعات جانبی آن نظیر این که چه کسانی، در کجا، کی، چگونه و چرا این جلسه را برگزار کردند، از اهمیت بیشتری برخوردار خواهد بود.

در حریم خصوصی زمانی و آماری، هر نوع اطلاعاتی از زمان رخداد یک حادثه چه به صورت قطعی و چه به صورت آماری (به عنوان نمونه نرخ و پراش زمان رخداد آن حادثه) ممکن است حریم خصوصی کاربر را به مخاطره بیافکند.

حریم خصوصی کاربر در حوزه طبقه‌بندی ترافیک

📌 تا چند سال پیش، تقریباً همه برنامه‌های کاربردی‌هایی که بر روی رایانه‌ها اجرا می‌شدند، از پروتکل‌های شناخته شده با شماره درگاه مشخص استفاده می‌کردند؛ به مانند برنامه کاربردی FileZilla که از پروتکل FTP و شماره درگاه 20 و 21 استفاده می‌کند.



تا چند سال پیش، تقریباً همه برنامه کاربردی‌هایی که بر روی رایانه‌ها اجرا می‌شدند، از پروتکل‌های شناخته شده با شماره درگاه مشخص استفاده می‌کردند؛ به مانند برنامه کاربردی FileZilla که از پروتکل FTP و شماره درگاه 20 و 21 استفاده می‌کند. اما امروزه تعداد برنامه‌های کاربردی با پروتکل نامعلوم و اختصاصی، با شماره درگاه‌های غیراستاندارد و تصادفی بسیار فراگیر شده است. به عنوان نمونه‌ای از این برنامه‌های کاربردی می‌توان از Skype، BitTorrent و VPN نام برد. در ضمن استفاده از سازوکارهای امنیتی در بسته‌های تولید شده توسط کاربردهای یاد شده، موجب می‌شود که از محتوای بسته، نتوان پی به برنامه کاربردی تولید کننده آن برد.

یک مهاجم بنا به جهات بسیاری تمایل دارد که دریابد که در گره مبدا چه برنامه کاربردی اجرا شده است. این موضوع در حوزه‌ای از تحقیقات به نام طبقه‌بندی ترافیک و یا بازرسی بسته مورد بررسی قرار می‌گیرد. روش‌های مختلفی برای کمک به مهاجم در این زمینه وجود دارد که دو نمونه از مهم‌ترین این روش‌ها به شرح زیر است [۳]:

🔍 طبقه‌بندی ترافیک بر مبنای محتوا: در این روش محتوای سر بسته لایه انتقال مورد بازرسی قرار می‌گیرد.

در حالت کلی این روش دسته‌بندی، به دو صورت DPI و SPI انجام می‌پذیرد.

● در DPI، سعی می‌شود که محتوا با یک امضای ثابت مقایسه گردد. دسته‌بندی بر مبنای پروتکل و شماره درگاه، به عنوان یکی از زیردسته‌های DPI محسوب می‌گردد. DPI به صورت گسترده در نرم‌افزارها و دیوارهای آتش مورد استفاده قرار می‌گیرد.

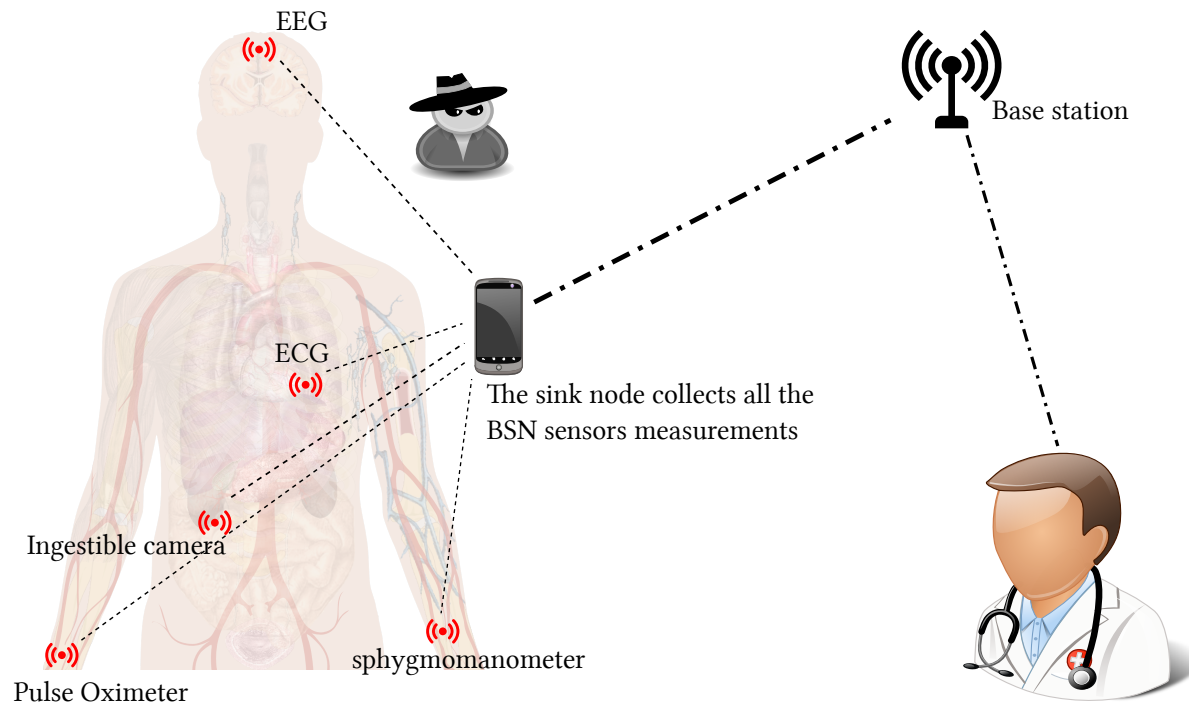
● در SPI، ویژگی‌های آماری سربسته و محتوای بسته لایه انتقال، مورد پوشش قرار می‌گیرد.

📖 **طبقه‌بندی ترافیک آماری:** در این شیوه به ویژگی‌های آماری زمان مابین خروج و طول بسته‌ها در لایه شبکه توجه می‌شود. لازم به ذکر است که در دسته‌بندی آماری بر خلاف SPI نیازی به بازگشایی بسته وجود ندارد، بدین‌سان در این نوع از دسته‌بندی حجم پردازش و محاسبات، به مراتب کمتر از SPI است.

با زیاد شدن پروتکل‌ها، مخفی ماندن جزئیات کارکرد آن‌ها به دلایل تجاری و استفاده از سازوکارهای امنیتی نظیر IPSec، روش‌های DPI و SPI دیگر به خوبی نمی‌توانند جواب‌گوی ما در این مساله باشند، و بدین‌سان امروزه شاهد یک اقبال عمومی به روش‌های طبقه‌بندی ترافیک آماری هستیم [۴، ۵]. هیچ‌کدام از ما دوست نخواهیم داشت که کسی بداند که چه برنامه کاربردی را در هر بازه زمانی بر روی رایانه خود اجرا می‌کنیم.

حریم خصوصی زمانی و آماری در WBAN

حسگرهای نصب شده بر روی بدن بیمار در WBAN، در زمان‌های مشخص به اندازه‌گیری علائم حیاتی او می‌پردازد. یک مهاجم باهوش می‌تواند با بدست آوردن اطلاعات مربوط به زمان‌های اندازه‌گیری حسگرها، پی به بیماری فرد ببرد.



در WBAN تعدادی حسگر به منظور سنجش ضربان قلب، وضعیت مغز، قند، فشار، چربی و غیره، بر روی بدن بیمار نصب می‌گردد [۶]. بسته به نوع بیماری فرد، این حسگرها با نرخ‌های مختلفی سنجش‌های مذکور را انجام می‌دهند. به عنوان مثال فرض کنید که مریضی به علت بیماری دیابت در بیمارستان بستری شده است. پرواضح است که برای تنظیم میزان انسولین تزریقی به بیمار، نیاز است در طول روز، حداقل چهار بار میزان قند خون او سنجیده شود، در حالی که این تعداد اندازه‌گیری برای سنجش چربی خون و ضربان قلب نیاز نخواهد بود. در هر بار سنجش، حسگر سیگنالی را به گره مرکزی ارسال و سپس از آن جا این اطلاعات در صورت نیاز به پزشک معالج نیز ارایه می‌گردد.

فرض کنید که یک مهاجم دستگاهی را در کنار تخت بیمار کار گذاشته است که هنگام ارسال سیگنال توسط هر حسگر به گره مرکزی، متوجه ارسال سیگنال می‌گردد. گرچه به علت استفاده از سازوکارهای رمزنگاری، شاید نتواند به میزان سنجه مورد اندازه‌گیری پی ببرد. اما یک مهاجم باهوش می‌تواند با تحلیل اطلاعات مربوط به زمان‌های ارسال سیگنال توسط هر حسگر، پی به نوع بیماری فرد ببرد.

- [1] M. Guizani, H. H. Chen, and C. Wang. *The Future of Wireless Networks: Architectures, Protocols, and Services*. Wireless Networks and Mobile Communications, Taylor & Francis, 2015.
- [2] A. Mason, S. C. Mukhopadhyay, and K. P. Jayasundera. *Sensing Technology: Current Status and Future Trends III*. Smart Sensors, Measurement and Instrumentation, Springer International Publishing, 2014.
- [3] S. Valenti, D. Rossi, A. Dainotti, A. Pescapè, A. Finamore, and M. Mellia, “Reviewing Traffic Classification,” in *Data Traffic Monitoring and Analysis SE - 6* (E. Biersack, C. Callegari, and M. Matijasevic, eds.), vol.7754 of *Lecture Notes in Computer Science*, pp.123–147, Springer Berlin Heidelberg, 2013.
- [4] J. Muehlstein, Y. Zion, M. Bahumi, I. Kirshenboim, R. Dubin, A. Dvir, and O. Pele, “Analyzing

{HTTPS} Encrypted Traffic to Identify User Operating System, Browser and Application,” *CoRR*, vol.abs/1603.0, 2016.

- [5] M. Crotti, M. Dusi, F. Gringoli, and L. Salgarelli, “Traffic classification through simple statistical fingerprinting,” *Computer Communication Review*, vol.37, pp.5–16, jan 2007.
- [6] S. Ullah, H. Higgins, B. Braem, B. Latre, C. Blondia, I. Moerman, S. Saleem, Z. Rahman, and K. S. Kwak, “A comprehensive survey of wireless body area networks,” *Journal of medical systems*, vol.36, no.3, pp.1065–1094, 2012.

A

AH Authentication Header

C

C-I-A Confidentiality، Integrity and Availability

D

DPI Deep Packet Inspection

E

ESP Encapsulating Security Payload

F

FTP File Transfer Protocol

I

IKE Internet Key Exchange

IP Internet Protocol

ISAKMP Search Results Internet Security Association and Key Management Protocol

P

PGP Pretty Good Privacy

S

SPI Stochastic Packet Inspection

T

TLS Transport Layer Security

V

VPN Virtual Private Network

W

WBAN Wireless Body Area Network

واژه‌نامه انگلیسی به فارسی

C A

Context Oriented مبتنی بر اطلاعات جانبی مهاجم Adversary

Authentication احراز اصالت

D Anonymity گمنامی

Application برنامه کاربردی

Data Oriented مبتنی بر داده لایه کاربرد Application Layer

Header سر بسته E

Host میزبان Encryption رمز گذاری

I

F

Integrity یکپارچگی Firewall دیوار آتش

InterDeparture Time زمان مابین خروج Freshness تازگی

K

H

Key Exchange تبادل کلید Hash Function تابع چکیده ساز

N

Network Layer لایه شبکه

Non-repudiation انکارناپذیری

L

Lifetime طول عمر

M

O

Malware بدافزار

Operating System سیستم عامل Message پیام

Multi-Hop چندگامه

P

Packet بسته

S

Security امنیت

Security Association پیمان امنیتی

Sensor حسگر

Server خدمت‌گزار

Source Node گره مبدا

Statistical آمار

T

Temporal and حریم خصوصی زمانی و آماری

Packet Inspection بازرسی بسته

Payload محتوا

Port Number شماره درگاه

Privacy حریم خصوصی

R

Rate نرخ

Replay Attack حمله بازپخش

Routing مسیریابی

Traffic Classification طبقه‌بندی ترافیک

Traffic Flow جریان ترافیک

Transport Layer لایه انتقال

U

User کاربر

V

Variance پراش

ب

۱

Packet Inspection	بازرسی بسته	Statistical	آمار
Malware	بدافزار	Authentication	احراز اصالت
Application	برنامه کاربردی	Security	امنیت
Packet	بسته	Non-repudiation	انکارناپذیری

پ

ج

پراش Variance
پیام Message
پیمان امنیتی Security Association

چ

چندگامه Multi-Hop

ت

تابع چکیده ساز Hash Function

ح

تازگی Freshness
تبادل کلید Key Exchange
حریم خصوصی Privacy
حریم خصوصی زمانی و آماری Temporal and
Statistical Privacy

حسگر Sensor د

حمله بازپخش Replay Attack رمزگذاری Encryption

خ ز

خدمت‌گزار Server زمان مابین خروج InterDeparture Time

د س

دیوار آتش Firewall سر بسته Header

سیستم عامل Operating System

ش

گ

Source Node گره مبدا Port Number شماره درگاه
Anonymity گمنامی

ط

ل Traffic Classification طبقه‌بندی ترافیک

Transport Layer لایه انتقال Lifetime طول عمر
Network Layer لایه شبکه
Application Layer لایه کاربرد

ک

User کاربر

Context Oriented مبتنی بر اطلاعات جانبی

ی

Data Oriented مبتنی بر داده

Integrity یکپارچگی

Payload محتوا

Routing مسیریابی

Adversary مهاجم

Host میزبان

Rate نرخ