بسم ایزد بخشنده

پروتکل های امنیت و الگوریتم های رمزنگاری

فردین صیاد منزه پور
اسفند ماه ۱۳۸۳

گروه مطالعاتی امنیت
شبکه ارتباطات داده ها

پروتکل های امنیت وآلگوریتم های رمزنگاری

انواع پروتکل های امنیت

- **CDPD /GPRS**

  Cellular Digital Packet Data / General Packet Radio Services
- **DNSSEC**

  Domain Name System SECurity
- **DOCSIS**

  Data Over Cable Service Interface Specification
- **WEP – WAP**

  Wired Equivalent Privacy / Wireless Application Protocol
- **IPSec**

  IP Security Protocol

پروتکل های امنیت وآلگوریتم های رمزنگاری

انواع پروتکل های امنیت

- **PPTP /L2F/L2TP**

  Point-to-Point Tunneling Pro.. / Layer 2 Forwarding /Layer 2 Tunneling Pro…

- **SET**

  Secure Electronic Transactions

- **S/MIME –PGP**

  Secure/Multipurpose Internet Mail Extensions / Pretty Good Privacy

- **SSH**

  Secure Shell

- **SSL / TLS**

  Secure Sockets Layer / Transport Layer Security

پروتکل های امنیت وآلگوریتم های رمزنگاری

Communication layers	Security protocols
Application layer	ssh, S/MIME, PGP, http digest
Transport layer	SSL, TLS, WTLS
Network layer	IPsec
Data Link layer	CHAP, PPTP, L2TP, WEP (WLAN), A5 (GSM), Bluetooth
Physical layer	Scrambling, Hopping, Quantum Communications

پروتکل های امنیت وآلگوریتم های رمزنگاری

انواع آلگوریتم های رمزنگاری

- MD : Message Digest
- SHA : Secure Hash Algorithm
- DES : Data Encryption Standard
- 3DES: Triple-DES
- AES : Advanced Encryption Standard
- Blowfish/Twofish
- CAST : Carlisle Adams & Stanford Tavares
- RC : Ron's Code & Riverst Cipher
- IDEA :International Data Encryption Algorithm

پروتکل های امنیت وآلگوریتم های رمزنگاری

انواع آلگوریتم های رمزنگاری

- **RSA :** Ron Riverst & Adi Shamir & Leonard Adleman
- **Diffie-Hellman(DH)**
- **ECC :** Elliptic Curve Cryptosystem
- **E1 Gamal (DSA)**

پروتکل های امنیت وآلگوریتم های رمزنگاری

پروتکل	آلگوریتم
1) CDPD /GPRS	(DH , RC4)
2) DNSSEC	(RSA , MD5 , DSA , AES , Blowfish)
3) DOCSIS	(RSA , DES , HMAC , SHA1)
4) WEP - WAP	(RC4 , MD5)
5) IPSec	(DH , RSA , MD5 , DES , SHA1 , 3DES)
6) PPTP /L2F/L2TP	(RSA , DES)
7) SET	(RSA , DES , HMAC-SHA1 , SHA1)
8) S/MIME –PGP	(RSA , AES , 3DES , MD5 , SHA1 , RC2, twofish,IDEA)
9) SSH	(RSA , DES , 3DES , RC2 , RC4 , RC5, twofish ,blowfish)
10) SSL / TLS	(RSA , DES , 3DES ,MD5,RC4,DH ,SHA1)

پروتکل های امنیت وآلگوریتم های رمزنگاری

دسته بندی آلگوریتم های رمزنگاری

پروتکل های امنیت از آلگوریتم های رمزنگاری (Ciphers) گوناگون استفاده می کنند وهر نسخه از پروتکل ها ضرورتا آلگوریتم های رمز نگاری سایر نسخه ها را حمایت نمی کند.

آلگوریتم های رمز نگاری بطور کلی در دو دسته قرار می گیرند:

- آلگوریتم های متقارن (symmetric)

یا secret-key cryptography یا shared secret

از قبیل DES، 3DES، AES، CAST ، RC5&6، Blowfish، IDEA

- آلگوریتم های نا متقارن (Asymmetric)

یا public – key cryptography

از قبیل RSA، Diffie-Hellman ، ECC ، E1 Gamal

پروتکل های امنیت وآلگوریتم های رمزنگاری

نکات مهم در بکارگیری آلگوریتم های رمزنگاری در پروتکل های امنیتی

۱. قویترین آلگوریتم همیشه بهترین انتخاب نیست زیرا حجم داده ها را افزایش می دهد.

۲. ارزش زمانی داده : هرچه این زمان کوتاهتر باشد بایستی از آلگوریتم ضعیف تری استفاده کرد.

۳. برای افزایش performance مورد نیاز بایستی از آلگوریتم ضعیفتر استفاده کرد.

۴. سرعت پردازشگر و اندازه حافظه در انتخاب موثر است.

۵. ممکن است برخی از انواع رمزنگاری توسط برنامه های نرم افزاری کاربردی ویا سیستم عامل صورت پذیرد.

پروتکل های امنیت وآلگوریتم های رمزنگاری

نکات مهم در بکارگیری آلگوریتم های رمزنگاری در پروتکل های امنیتی

۶. در برخی سازمانها ارزش امنیتی داده های ورودی و خروجی یکسان نیست مانند سرویس e-mail .

۷. پارامترها ئی ازجمله استفاده از خطوط اختصاصی بجای اینترنت نیز در انتخاب موثرند.

۸. با انتخاب پروتکل ها واستانداردهای خاصی جهت رمزنگاری ممکن است به استفاده از آلگوریتم های خاصی محدود شویم بطورمثال در email که به آلگوریتم هائی مانند PGP ، S/MIME وغیره محدود میشویم.

۹. برخی آلگوریتم ها ارزش امنیتی خود را از دست داده اند.

پروتکل های امنیت وآلگوریتم های رمزنگاری

نکات مهم در بکارگیری آلگوریتم های رمزنگاری در پروتکل های امنیتی

در سال ۱۹۹۸ ، EFF(Electronic Frontier Foundation)
توانست با استفاده ازbreaking DES آلگوریتم DESRSA DES
ChallengeII-2 را در کمتر از ۳روز بشکند.

در فاصله زمانی تا ۱۹۹۹ ، EFF توانست DES Cracker را با هزینه ای بیش از۲۵۰،۰۰۰ دلاربسازد که قادر بود ۸۸ میلیارد کلید را دریک ثانیه پردازش وتست کند.

در سال ۱۹۹۹ ، Distributed. Net با استفاده از DES Cracker و۱۰۰،۰۰۰ رایانه شخصی در شبکه جهانی به مصاف RSA DES Challenge III رفت وتوانست پس از ۲۲ساعت و۱۵دقیقه آنرا در هم بشکند.(برای یافتن کلید صحیح ۲۴۵میلیاردکلیددر ثانیه تست شد!)

پروتکل های امنیت وآلگوریتم های رمزنگاری

نکات مهم در بکارگیری آلگوریتم های رمزنگاری در پروتکل های امنیتی

- انتخاب یک پروتکل مناسب امنیتی بستگی به آلگوریتم های رمزنگاری بکار رفته دارد .مثال :

اگر سازمانی پروتکل S/MIME را برای ایجاد امنیت در پست الکترونیکی انتخاب نماید

نباید RC2 40 (ضعیف ترین آلگوریتم رمزنگاری) یا DES (آلگوریتم ضعیف رمزنگاری) را برای Mail های حساس خود انتخاب نماید.

RC2 64 قویتر از DES یا RC2 40 وسریعتر از DES و3DES عمل می کند ولی برای امنیت بهتر، 3DES مناسبتراست .

پروتکل های امنیت وآلگوریتم های رمزنگاری

کاربرد آلگوریتم های رمزنگاری در پروتکل های امنیتی

- برخی آلگوریتم ها وجود دارند که برای hashing یعنی تبدیل پیام یا داده به مقادیر عددی بکار می روند.ازقبیل MD و SHA وDH

MD5 و SHA-1 جدیدترین نسخه ها هستند که بترتیب Hash های ۱۲۸ و ۱۶۰ بیتی تولید می کنند.

- از Diffie-Hellman بهمراه SHA1 برای مبادله کلید

RC4- ، DES ، 3DES ، AES ، twofish و blowfish برای رمزنگاری ورمزگشائی داده ها.

- RSA و DSA برای امنیت امضاها وenveloping رقمی

- از HMAC بهمراه MD5 یا SHA1 برای یکپارچگی ورمز متون

پروتکل های امنیت وآلگوریتم های رمزنگاری

کاربرد آلگوریتم ها درپروتکل PGP

FUNCTION	ALGORITHM	DESCRIPTION
Digital Signature (Authentication)	SHA-1 or RIPEMD-160 along with either DSS or RSA	A hash code of a message is created using SHA-1 or RIPEMD-160. This message digest is encrypted using DSS or RSA with the sender's private key, and included with the message
Message Encryption (Confidentiality)	CAST or IDEA or Three-key Triple DES or Blowfish with Diffie-Hellman or RSA (Version 7.0.3 adds Twofish, AES, and RSA 4096)	A message is encrypted using CAST-128 or IDEA or 3DES or Blowfish with a one-time, one-message session key generated by the sender. The session key is encrypted using DH or RSA with the recipient's public key

پروتکل های امنیت وآلگوریتم های رمزنگاری

کاربرد آلگوریتم ها در پروتکل IPSec

Encryption	Integrity/Authentication	Modes
Data Privacy	Data Exchange Verification	Transport Format
DES *Data Encryption Standard*	**IKE** Diffie-Hellman •• RSA *Internet Key Exchange*	**AH / ESP** *Authentication Header / Encapsulating Security Payload*
3DES *Triple Data Encryption Standard*	**RSA / DSS** *Rivest, Shamir, Adelman / Digital Signature Standard*	**Tunnel / Transport** *Network to Network / Host to Host*
symmetric encryption	**X.509v3** *Digital Certificates*	
	MD5 / SHA for HASHING *Message Digest 5 / Secure Hash Algorithm*	

پروتکل های امنیت وآلگوریتم های رمزنگاری

```
Spiritwrack root #openssl speed
```

The 'numbers' are in 1000s of bytes per second processed.

Type	16 bytes	64 bytes	256 bytes	1024 bytes	8192 bytes
md2	781.82k	1658.54k	2302.72k	2551.81k	2646.65k
mdc2	2303.33k	2601.19k	2691.07k	2713.26k	2722.47k
md4	8088.59k	28497.81k	81425.75k	152377.69k	204186.28k
md5	6658.93k	23101.61k	64989.44k	119329.11k	154162.52k
hmac(md5)	7759.01k	26624.06k	72236.29k	125175.13k	156237.06k
sha1	6341.00k	19797.27k	46929.07k	71337.98k	84077.23k
rmd160	5810.05k	16892.76k	36562.60k	51938.65k	59072.51k
rc4	90142.04k	103726.75k	109965.65k	111563.43k	112017.41k
des cbc	20494.70k	21585.24k	21716.22k	21814.97k	21749.76k
des ede3	7474.74k	7685.31k	7816.62k	7852.37k	7858.86k
idea cbc	15655.19k	16604.78k	16738.56k	16802.47k	16826.37k
rc2 cbc	8038.72k	8356.65k	8447.32k	8468.48k	8467.80k
rc5-32/12 cbc	57561.14k	64905.50k	66914.74k	67767.64k	68263.94k
blowfish cbc	32069.08k	34651.74k	34664.70k	34956.07k	35124.57k
cast cbc	22870.35k	24536.13k	25176.06k	25432.19k	25384.28k
aes-128 cbc	20298.75k	20858.41k	21088.09k	21236.53k	21181.78k
aes-192 cbc	17338.95k	17913.43k	18051.93k	18111.83k	18128.90k
aes-256 cbc	15485.55k	15934.95k	16042.58k	16142.21k	16100.01k

پروتکل های امنیت وآلگوریتم های رمزنگاری

برخی نکات مهم در نحوه بکارگیری انواع آلگوریتم ها

در جدولی که مطابق دستور openSSL speed روی سیستم عامل لینوکس و رایانه ای با مشخصات ذیل اجرا شده است به نکـات قابل توجهـــــی برمی خوریم که عدم توجه به آنها مشکلاتی رابدنبال خواهد داشت ،

- Dell P III 1GHz RAM:512K OS: Gentoo Linux

۱) DES در فضای بلوک ۶۴بایتی (با کلید ۵۶بیتی)در مقایسه با سایر آلگوریتم ها از سرعت رمزنگاری و رمزگشائی خوبی برخوردار است (حدود 22Mps) ولی بمنزله تائید آن نیست .

۲) 3DES (درجدول بانام DES-ede3 آمده است) نیز برای سه بار اجرای آلگوریتم DES به پردازش بیشتری نیاز دارد (حدود7.5Mps)

پروتکل های امنیت وآلگوریتم های رمزنگاری

برخی نکات مهم در نحوه بکارگیری انواع آلگوریتم ها

۳) Blowfish با کلید ۱۲۸بیتی و قدرت وسرعتی که دارد بلوک ۶۴بایتی را با حدود 35Mps رمزنگاری می کند.

۴) AES با کلید های ۱۲۸ ، ۱۹۲ و ۲۵۶ بیتی خود این بلوک ۶۴ بیتی را بترتیب با سرعت 21Mps ، 17Mps و 15Mps رمزنگاری می کند.

۵) RC4 با وجود سرعت بالا (حدود 104Mps) برای صرفا جریان داده ها با سری طولانی مانند صدا و ویدئو مناسب است وبرای راه حل های تونل مناسب نیست .

پروتکل های امنیت وآلگوریتم های رمزنگاری

بکارگیری آلگوریتم ها بصورت تلفیقی در پروتکل های امنیتی

WAP با ترکیب دو مولفه ، امنیت را تامین می کند:

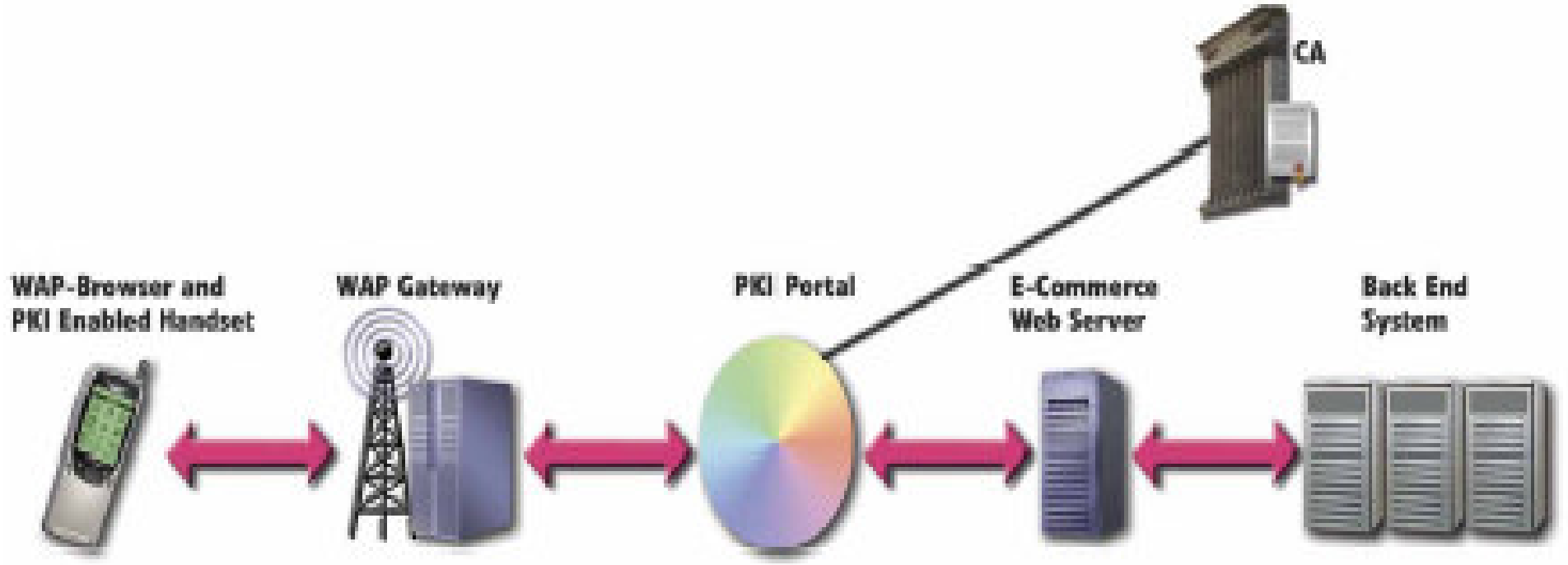
۱) امنیت درسطح لایه Transport که امنیت کانال نامیده می شود و با استفاده از پروتکل های SSL ، TLS ، SSL plus (ترکیب پروتکل های SSL و TLS) و WTLS تامین می شود.

WTLS : Wireless Transport Layer Security

پروتکل های امنیت وآلگوریتم های رمزنگاری

بکارگیری آلگوریتم ها بصورت تلفیقی در پروتکل های امنیتی

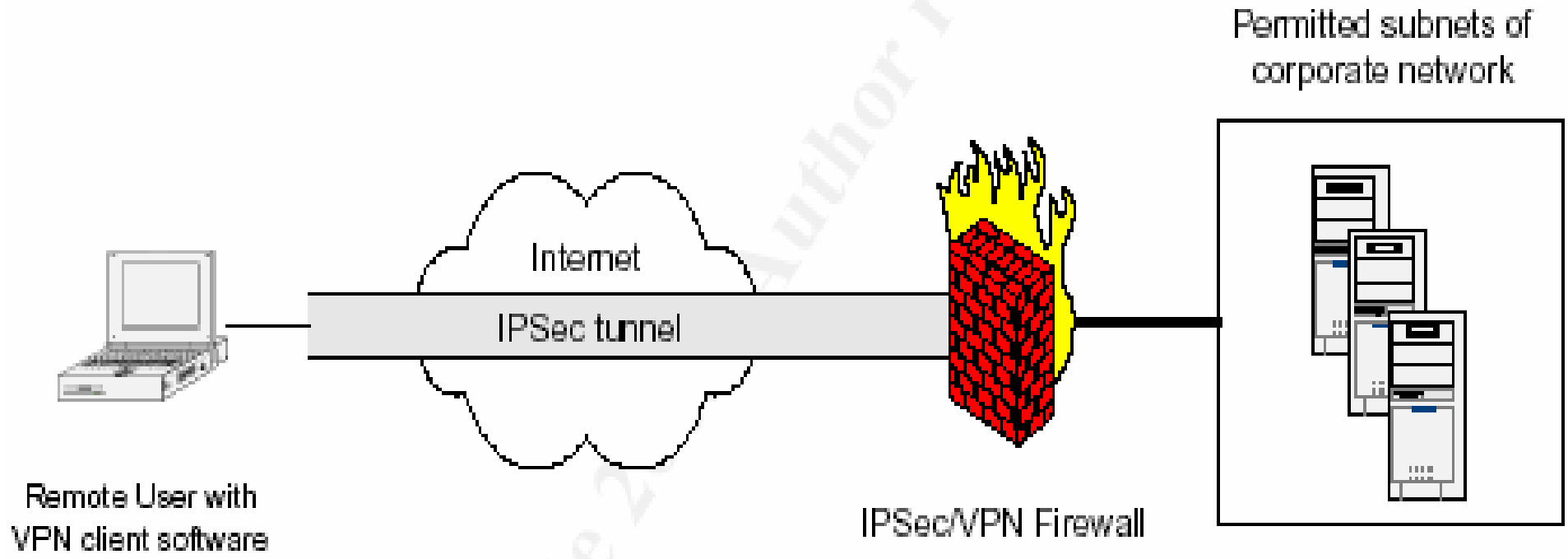
۲) امنیت تبادلات داده end-to-end که بااستفاده از توابع امنیتی در سطح لایه Application مانند امضای رقمی و PKI تامین می شود.



پروتکل های امنیت وآلگوریتم های رمزنگاری

IPSec VPN

برای کاربرانی که نیاز به دسترسی سطح پائین دارند ورایانه آنها همواره کنترل می شود.



پروتکل های امنیت وآلگوریتم های رمزنگاری

بکارگیری پروتکل های امنیتی بصورت تلفیقی (۱)

مزایای IPSec VPN :

۱) نظر به اینکه VPN یک تونل site-to-site است ، IPSec هنوزانتخاب اول محسوب می شود

۲) عملکرد IPSec در لایه IP موجب انعطاف پذیری آن درتنظیمات شبکه و برنامه های کاربردی می شود، بطوریکه تقریبا همه برنامه های کاربردی Mainframe از IPSec VPN استفاده می کنند.

۳) محیط IPSec VPN بدون وجود اینترنت نیز کار می کند.

۴) بعلت کپسوله کردن وپنهان سازی کل پکتها می تواند پروتکل های non-routable مانند VoIP ، NetBeui وSNA را قابل مسیردهی کند.

پروتکل های امنیت وآلگوریتم های رمزنگاری

بکارگیری پروتکل های امنیتی بصورت تلفیقی (۱)

۵) همینکه تونل IPSec از طریق مبادله کلید ایجاد شود ، برای ارتباطات بعدی نیازی به مبادله کلید اضافی نخواهد بود.

۶) نرم افزار VPN client آن می تواند نیاز به آنتی ویروس و فایروال شخصی را وآخرین نسخه سیستم عامل به لحاظ patch را تشخیص دهد تا مانع از ورود نفوذگران ، ویروسها ، کرم ها و اسب های تراوا شود.

پروتکل های امنیت وآلگوریتم های رمزنگاری

بکارگیری پروتکل های امنیتی بصورت تلفیقی (۱)

معایب IPSec VPN :

۱) نیاز دارد نرم افزار VPN client روی رایانه شخصی راه دور یا notebook نصب شود و این برای برای شرکتها وکاربرانی که نیاز به دسترسی درهرکجا و درهرزمان دارند مطلوب نیست وحتی در برخی از سیستم عامل ها مانند یونیکس ولینوکس قابل اجرا نیست.

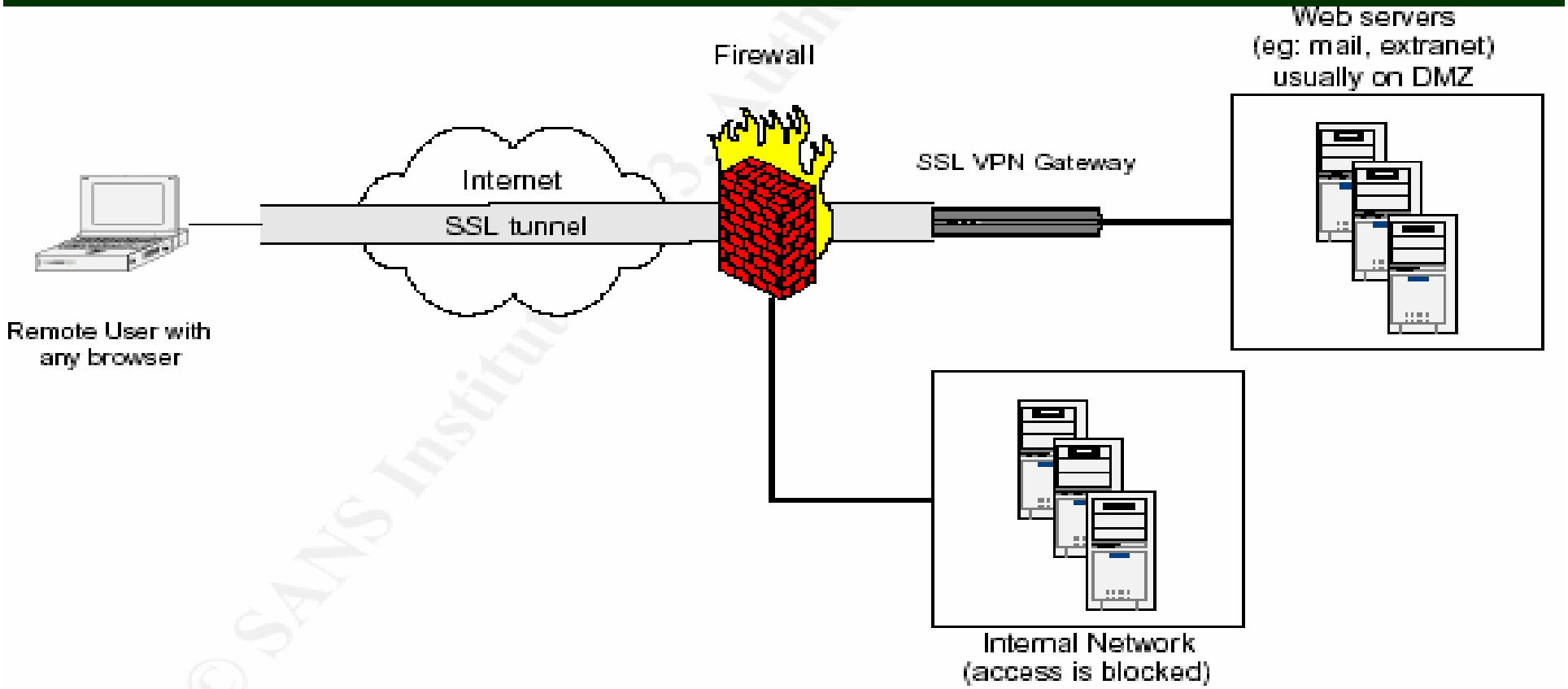
۱) از آنجائی که دسترسی به کل subnet دریک شبکه را فراهم می آورد ، client PC می تواند بعنوان وسیله ای حامل برای نفوذگران به شبکه مورد استفاده قرار گیرد یعنی حتی با آلوده شدن آن کل شبکه به مخاطره می افتد.

۱) از آنجائی که اتصال آن از طریق فایروال برقرار می شود باز گذاشتن برخی از پورتهای فایروال وبالا رفتن ریسک امنیتی اجتناب ناپذیراست.

پروتکل های امنیت وآلگوریتم های رمزنگاری

SSL VPN

برای دسترسی به پست الکترونیکی ودسترسی مبتنی بر وب .



پروتکل های امنیت وآلگوریتم های رمزنگاری

بکارگیری پروتکل های امنیتی بصورت تلفیقی (۲)

مزایای SSL VPN :

۱) SSL به نرم افزار client PC نیاز ندارد.

۲) SSL به سیستم عامل وابسته نیست.

۳) SSL درهمه مرورگرها از قبیل Mozilla وInternet Explorer تعبیه شده است وبرنامه هائی مانند outlook ، Exchange و Lotus Notes آنرا پشتیبانی می کنند.

۴) بدلایل فوق در کیوسک های فرودگاه و کافه های اینترنتی برای دسترسی به VPN های متصله قابل استفاده است.

۵) هزینه اجرائی و پشتیبانی آن بدلایل فوق ، پائین است.

۶) SSL اجازه دسترسی به subnet شبکه را نمی دهد.

پروتکل های امنیت وآلگوریتم های رمزنگاری

بکارگیری پروتکل های امنیتی بصورت تلفیقی (۲)

۷) SSL از پورت TCP/443 که قبلا روی فایروال به سمت DMZ باز می باشد ، استفاده می کند.

۸) به محض قطع session ، کلیه cookie ها از بین می روند ، trace ها حذف می شوند و هر نوع cache برداشته می شود لذا اطلاعات یک کاربر روی کیوسک یا کافه های اینترنتی توسط کاربر بعدی قابل استفاده نخواهد بود.

پروتکل های امنیت وآلگوریتم های رمزنگاری

بکارگیری پروتکل های امنیتی بصورت تلفیقی (۲)

معایب SSL VPN :

۱) دسترسی VPN فقط به برنامه های کاربردی تحت وب امکان پذیر است واگر کاربری به اینترنت دسترسی نداشته باشد ، کارکردن بصورت offline ممکن نیست.

۲) اجرای دستوراتی از قبیل Telnet (دسترسی سطح پائین) برخلاف IPSec VPN ممکن نیست وبارگیری برنامه های کوچک برای بهبود کارائی برنامه کاربردی وب توسط Java یا Active X وبارگذاری آن روی مرورگر ، اجتناب ناپذیر است . وکافه های اینترنتی وکیوسک ها جهت جلوگیری از نفوذهای ناخواسته ، مانع از اینکار می شوند.

پروتکل های امنیت وآلگوریتم های رمزنگاری

بکارگیری پروتکل های امنیتی بصورت تلفیقی (۲)

۳) از پیامدهای دیگر مبادله چندباره کلید است که می تواند طی یک session رخ دهد وباعث کاهش کارائی وب سرور گردد. این مشکل از طریق SSL gateway یا شتاب دهنده های نرم افزاری قابل رفع است ولی هزینه اجرا را بالا می برد.

۴) وقتی چند سرور SSL پیغامی مانند No Cache meta tags را به یک client بفرستند وبه هر دلیل توسط client پذیرفته نشوند ، اطلاعات مربوط به session را می توان trace کرد ومورد استفاده قرار داد.

پروتکل های امنیت وآلگوریتم های رمزنگاری

بکارگیری پروتکل های امنیتی بصورت تلفیقی (۲)

هم اکنون شرکتهای سخت افزاری ونرم افزاری مانند Cisco ، Checkpoint و Nortel عرضه راه حل های ترکیبی از پروتکل های IPSec و SSL در VPN آغاز کرده اند لذا در انتخاب راه حل های ملی توجه به ماتریس آلگوریتم ها ی رمزنگاری و پروتکل های امنیتی از اهمیت ویژه ای برخوردار است.