اصول امنیت براساس زیرساخت کلید عمومی

از مجموعه سمینارهای آشنایی کمیسیون افتا - کارگروه آموزش و پژوهش

ارائه دهنده: **رامبد راستی**

مدیر راه‌حل های امنیتی در شرکت گام الکترونیک

1

عناوین قابل بحث در این سمینار

- مبانی امنیت اطلاعات
- مبانی رمز
- زیرساخت کلید عمومی (PKI)
- کاربرد PKI
- ادوات رمز - توکن
- ادوات رمز – ماژول امن سخت‌افزاری

2

"تعریف اطلاعات"

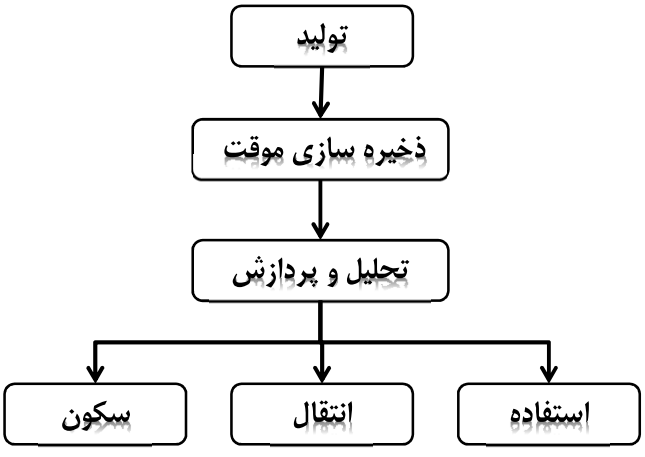
از مهمترین و حیاتی ترین منابع هر سازمانی اطلاعات آن سازمان می باشد

اطلاعات یک دارایی همانند سایر دارایی ها سازمان می باشد. بنابراین...؟

تعریف امنیت اطلاعات از دیدگاه جین اسپافورد

3

"مفهموم اطلاعات"



4

تقسیم‌بندی کلان امنیتی

- ✓ **امنیت رایانه شخصی**
- ✓ **امنیت در شبکه‌های خصوصی**
- ✓ **امنیت برروی کانال‌های ارتباطی**

5

امنیت رایانه شخصی

که بشکل معمول شامل استفاده از:

- ضد ویروس
- دیوار آتش
- کپی پشتیبان
- پنهان سازها و رمزکننده ها بصورت شخصی و یا سازمانی
- نرم افزار ها بوسیله قفل های نرم افزاری و یا سخت افزاری

6

امنیت در شبکه‌های خصوصی

✓ **که بشکل معمول شامل استفاده از:**

- امنیت فیزیکی
- ضد ویروس و دیوار آتش سخت افزاری در محیط سرور
- ضد ویروس و دیوار آتش نرم افزاری برروی سیستم کاربران با کنترل مرکزی
- کپی پشتیبان دوره‌ای
- ارزیابی های امنیتی توسط CSEM و تصحیح پویای سیاست های امنیتی
- استفاده از عامل دوم احراز هویت کاربران
- آموزش های دوره ای کاربران و مدیران در خصوص مخاطرات و تهدیدات امنیتی

7

امنیت کانال‌های ارتباطی

✓**استفاده از انواع روش های:**

- پنهان سازی اطلاعات
- رمزنگاری اطلاعات
- امضای دیجیتال
- و استفاده از زیرساخت کلید عمومی (PKI)

8

دیدگاه‌های امنیتی موجود

امنیت محیط محور (Perimeter-Centric)

✓ **فلسفه:**

- تمامی افراد غیرقابل اعتماد از داخل سازمان دور شده اند.
- تمامی پرسنل داخل سازمان مورد اعتماد هستند
- اطلاعات حساس هیچگاه و بهیچ عنوان از محیط سازمان خارج نخواهند شد.

✓ **تهدیدات شناسایی شده:**

- Denial of Service, Malware, Hacking

✓ **راه حل های ارائه شده:**

- حراست و حفاظت فیزیکی از اطلاعات
- استفاده از Firewall, IDS/IPS, Anti-Virus

✓ **مشکلات این دیدگاه:**

- اطلاعات می تواند سازمان را ترک کند.
- اطلاعات داخل سازمان به هیچ عنوان محافظت نمی شود.
- دائما باید نسبت به تهدیدات جدید امنیتی آگاه و بروز بود.
- دیدگاه این طراحی در حفاظت از سیستم مناسبتر است تا اطلاعات
- افشای کل اطلاعات درصورت هرگونه دسترسی غیرمجاز به اطلاعات

9

دیدگاه‌های امنیتی موجود

امنیت اطلاعات محور (Data-Centric)

– **فلسفه:**

- هیچ شخصی مورد اعتماد نیست
- درحال حاضر افراد غیرقابل اعتماد در سازمان حاضر هستند.
- فرض براین است که هیچ کنترلی برروی محل و چگونگی استفاده از اطلاعات وجود ندارد.

– **تهدیدات شناسایی شده:**

- Privacy breach, data leakage, IP theft,
- identity theft, insider attacks

– **راه حل های ارائه شده:**

- حفاظت از کلیه اطلاعات حساس براساس اهمیت آنها
- رمزنگاری اطلاعات، تشخیص هویت و مدیریت سطح دسترسی و کلید

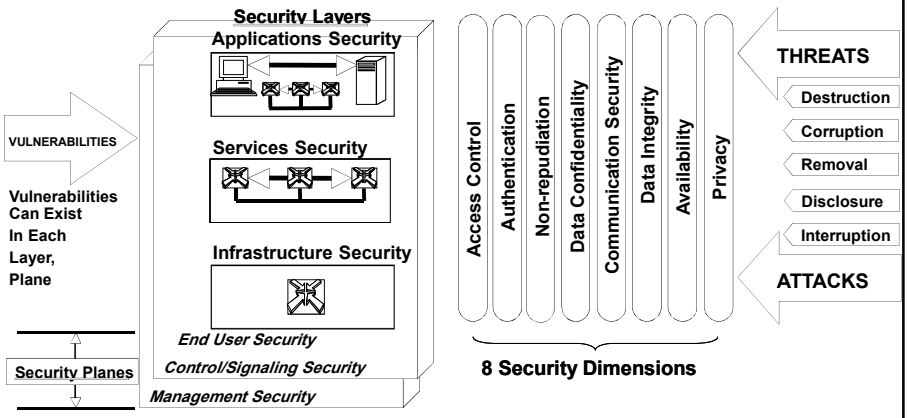
– **مزایای استفاده از این دیدگاه:**

- مخفی ماندن اطلاعات، متمرکز بودن و احرازهویت
- دسترسی به اطلاعات فقط برای کاربران مجاز میسر خواهد بود.
- قابلیت انتقال ایمن اطلاعات از طریق ادوات نامطمئن
- یک دفاع مطمئن در برابر ازبین رفتن هریک از لایه های امنیتی

10

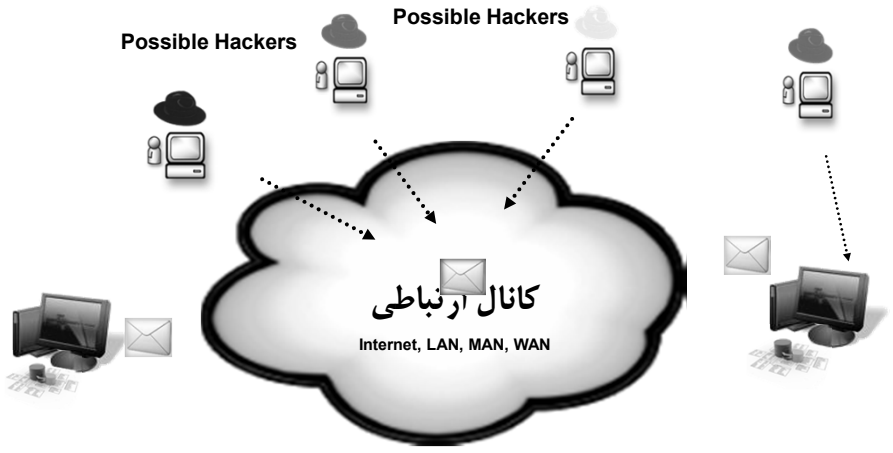
ابعاد امنیتی ۸ گانه (ویژگی امنیتی درفتا)

ابعاد امنیتی ۸ گانه در معماری امنیت شبکه که توسط ITU-T و در استاندارد X.805 ارائه شده است عبارتند از:



11

پیام، ارتباط، اطلاعات وکانال ارتباطی



12

حمله یا فضولی!!

معمولا پس از فضولی که توسط یک آماتور صورت می پذیرد:
تعیین قوانین جدید
ایجاد وقفه کوتاه مدت و ادامه کار

و زمانیکه یک حمله توسط یک گروه حرفه ای اتفاق می افتد:
از دست دادن مالکیت معنوی یک تجارت
از دست دادن اعتبار در پرداخت های احتمالی
سرقت هویت در ابعاد وسیع
از دست دادن تجارت بخاطر اطلاعات سرقت شده

13

حمله‌های قابل پیش‌بینی

حمله به رایانه گیرنده و فرستنده

Backdoor – Trojan – Virus - Worms
Key logger
Shoulder Phishing
Social Engineering

حمله به کانال ارتباطی

Packet-Monitor (Sniffing)
Spoofing attack (IP (man-in-the-middle), URL (Phishing), Caller ID, Ref-tar)
MAC & ARP flooding

حمله به اطلاعات

14

حمله‌های امنیتی به اطلاعات

روش های مرسوم در حمله به اطلاعات در حال حرکت عبارتند از:

- **Interruption (قطع)**
- **Fabrication (ایجاد پیام)**
- **Interception (دسترسی غیرمجاز)**
- **Modification (دستکاری داده)**

15

ساز و کارهای حرفه‌ای برای جلوگیری از حملات امنیتی

برای جلوگیری از حملات امنیتی به یک پیام معمولا از یک و یا تمام مکانیسم های زیر استفاده می‌شود:

Authentication (احراز هویت)

مسیری که هویت یک کاربر بررسی و ارزیابی می گردد.

Authorization (مجوز دسترسی)

مسیری که باعث عطای سطح دسترسی به کاربر برای استفاده از نرم افزارها، فایل ها، اطلاعات و منابع شبکه می گردد

Auditing (ممیزی)

عدم انکار در اطلاعات تغییر یافته توسط کاربر

Data Privacy and Integrity (اختفای اطلاعات و یکپارچگی آنها)

برای اطمینان از عدم تغییر اطلاعات بخصوص در هنگام انتقال

16

احرازهویت

آیا کاربران واقعا کسانی هستند که ادعا می کنند؟
کاربران برای چه کارهای مجوز دارند؟
آیا نام کاربری و رمزعبور برای کاری که آنها قرار به انجام آن را دارند کفایت می کند؟

مجوز دسترسی

چه کسی وارد محیط ما شده است؟
چه حق و مجوزی را می بایستی به کاربران بدهیم؟
کاربر به چه فایلها و اطلاعاتی را می تواند رویت کند؟
تامین امنیت اطلاعات چگونه باشد تا تعهدی بر مخفی ماندن اطلاعات بوجود بیاید؟

17

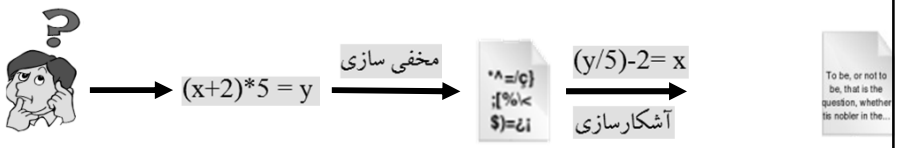
ممیزی

واقعا چه کارهایی را کاربران انجام می دهند؟
آیا آن فرد بخصوص مجوز عملی را که انجام می دهند را دارد؟
آیا ما بدرستی با مفهمومی مثل عدم انکار آشنا شده ایم؟
آیا می توانید فعالیت هایی که ویژه یک شخص، شرکت، سازمان و وابسته به زمان خاصی است را تصدیق کنید؟
آیا گزارشی دال بر کنترل فعالیت صحیح افراد وجود دارد؟
آیا برای کاری که انجام می شود نام کاربری و رمزعبور کفایت می کند؟

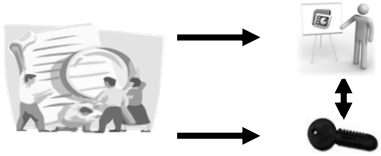
18

اختفای اطلاعات و یکپارچگی آنها

۱- مخفی سازی توسط الگوریتم



۲- مخفی سازی توسط کلید (رمزنگاری)



رمـزنگاری متقارن

رمزنگاری نامتقارن

تعاریف و اصطلاحات رمزنگاری

- **کلید (Key)**

XCBhGyhuhgH89YH8piu08if-09FGo78dvs9e4310

XCBhGyhuhgH89YH8piu08if

09FGo78dvs9e4310

- کلید عمومی(Public Key)
- کلید خصوصی(Private Key)

- **گواهینامه دیجیتال (Digital Certificate)**

X.509 v3

- **بهم ریختگی (HASH)**

MD5, SHA1, SHA3

تعاریف و اصطلاحات رمزنگاری

PKCS (Public-Key Cryptography Standards) -

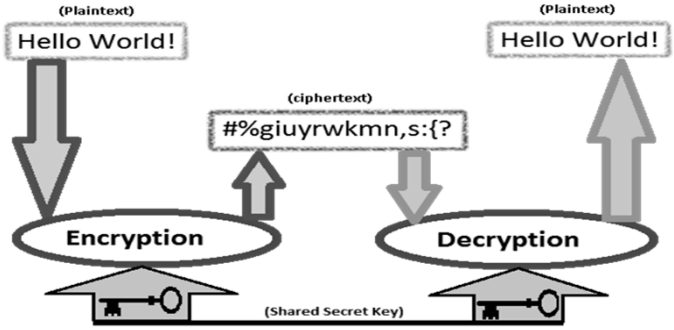
MS-CAPI (Microsoft Cryptography API)-

CNG (Cryptography API: Next Generation) -

تعاریف و اصطلاحات رمزنگاری

	Version	Name
PKCS #1	2.1	RSA Cryptography Standard
PKCS #3	1.4	Diffie–Hellman Key Agreement Standard
PKCS #5	2.0	Password-based Encryption Standard
PKCS #6	1.5	Extended-Certificate Syntax Standard
PKCS #7	1.5	Cryptographic Message Syntax Standard
PKCS #8	1.2	Private-Key Information Syntax Standard
PKCS #9	2.0	Selected Attribute Types
PKCS #10	1.7	Certification Request Standard
PKCS #11	2.2	Cryptographic Token Interface
PKCS #12	1.0	Personal Information Exchange Syntax Standard
PKCS #13	-	Elliptic Curve Cryptography Standard
PKCS #14	-	Pseudo-random Number Generation
PKCS #15	1.1	Cryptographic Token Information Format Standard

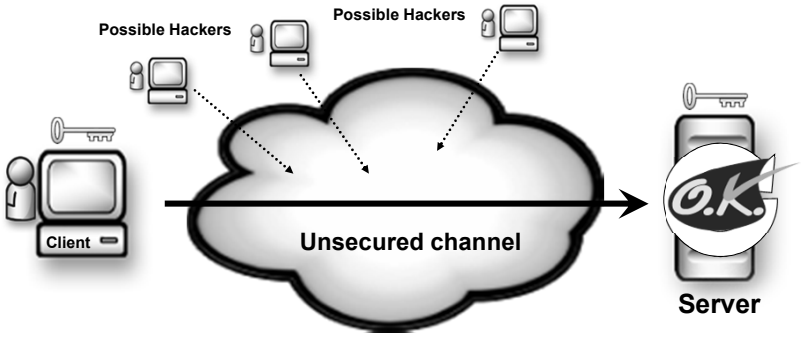
رمزنگاری متقارن



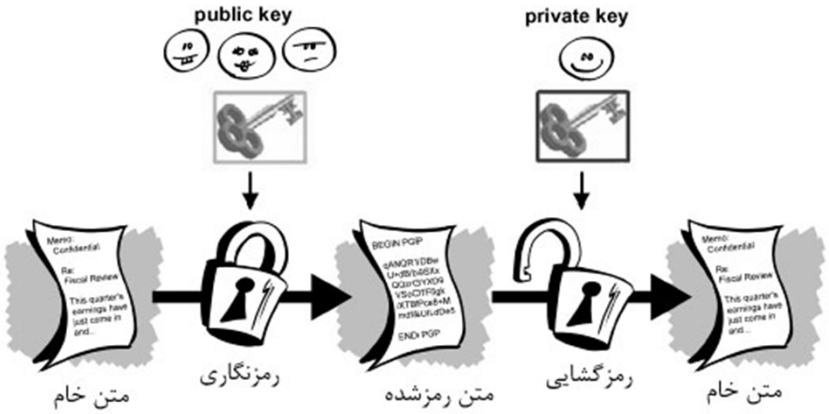
- **DES/3DES**
- **RC4/AES**

احراز هویت براساس روش
Shared Secret / Challenge response

– ارسال مشخصات کاربر بشکل رمز
– رمزگشایی و بررسی مشخصات کاربر
– درصورت تایید هویت کاربر، تهیه پاسخ و ارسال آن

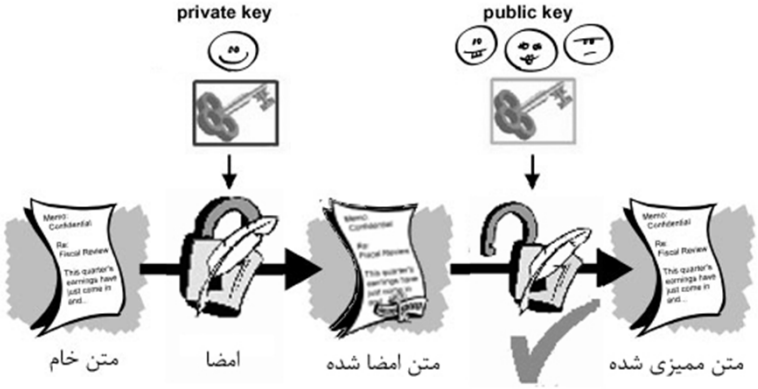


رمزنگاری نامتقارن



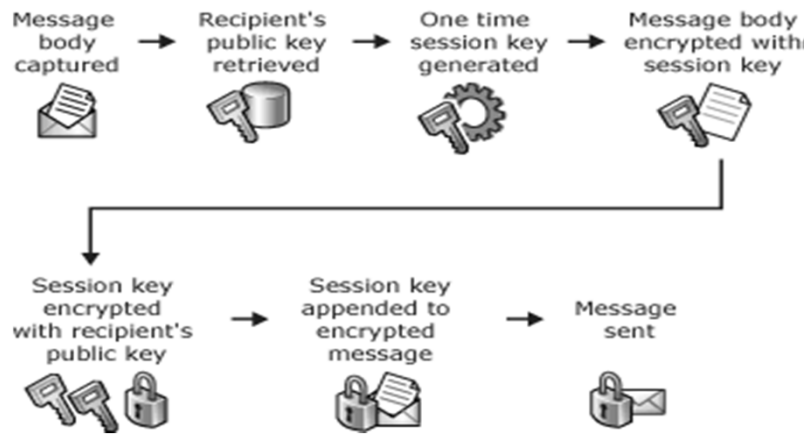
- **RSA**

امضای دیجیتال

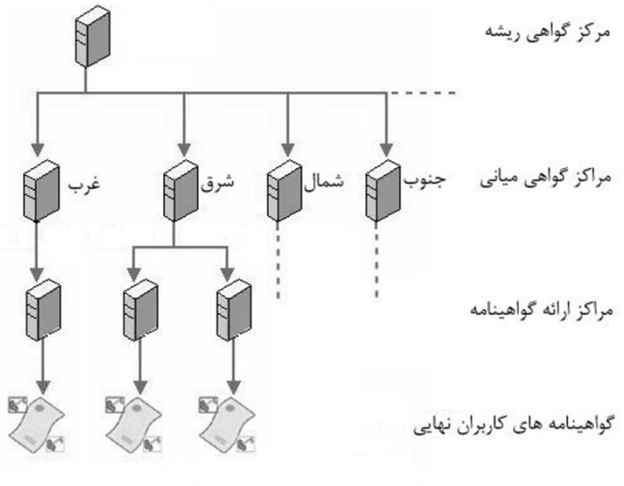


- **DSA**

رمزنگاری در دنیای واقعی



مرکز گواهی یا طرف سوم مورد اعتماد



28

وظایف اصلی مرکز صدور گواهی

- ✓ تولید گواهی
- ✓ انتشار گواهی
- ✓ ابطال گواهی
- ✓ تجدید گواهی
- ✓ مدیریت بانک‌های اطلاعاتی
- ✓ تدوین سیاست‌های امنیتی

29

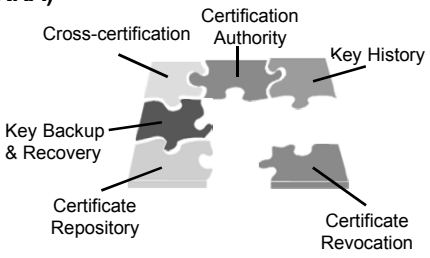
بخش‌های اصلی در PKI

- **عملکردهای مرکز گواهی**
  در این قسمت تعاریف اصلی فعالیت های یک مرکز گواهی انجام می شود.
- **مدیریت چرخه زمانی کلید/گواهینامه**
  مدیریت تولید، طول عمر و بازیابی کلیدها و گواهینامه را عهده دار است.
- **پشتیبانی از مبحث عدم انکار**
  ثبت احوال مرکز گواهی .عملیات مربوط به ثبت نام و درخواست گواهی را عهده دار می باشد.
- **پایدارسازی و کنترل صحت**
  مجموعه مواردی که اصالت و صحت عملکرد یک مرکز گواهی را تضمین می کند.

30

فعالیت‌های اصلی در یک مرکز گواهی

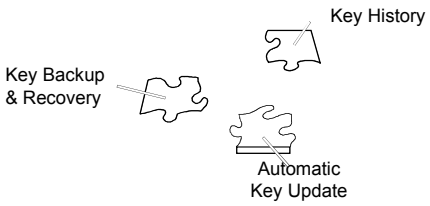
1. **Certificate Authority**
(Key Generation System, Certificate signing, Issue, Suspend, Publishing)
2. **Certificate Repository**
3. **Certificate Revocation**
4. **Cross Certification**
5. **Key Backup and Recovery (KMI / KRA)**
6. **Key History(Certificate Archive)**



31

مدیریت چرخه زمانی کلید / گواهینامه در یک مرکز گواهی

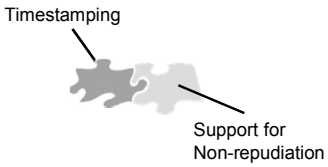
1. **Automatic Certificate/Key update (Recertification - Renew)**
2. **Key backup and recovery**
3. **Certificate/Key History**



32

عدم انکار در مرکز گواهی

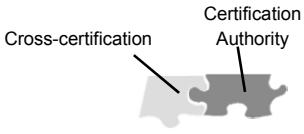
1. Two key pair system
2. Notary services (Registry Authority)
3. Secure long term storage
4. Timestamping services



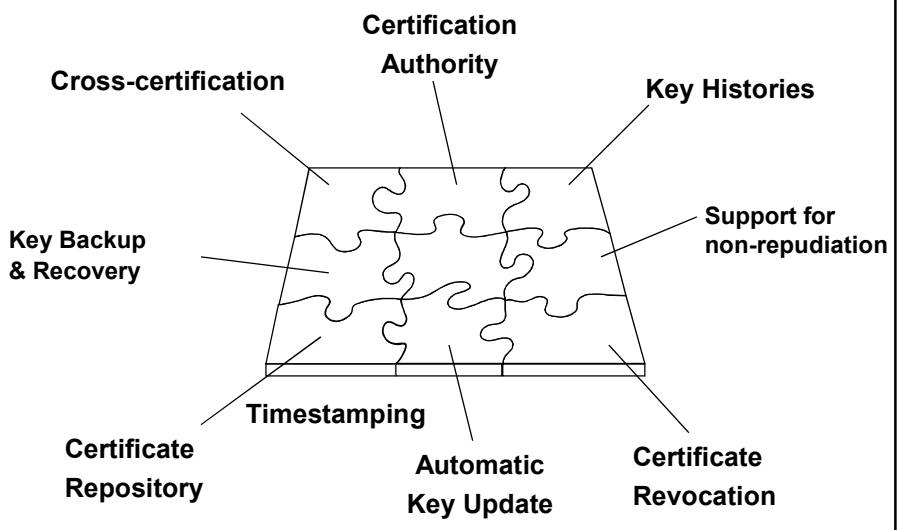
33

کنترل صحت و اطمینان به مرکز گواهی

1. Certification Authority
2. Cross-certification



34



35

مزایای استفاده از PKI

آنچه‌که بعد از پیاده سازی PKI بدست خواهیم آورد:

- امنیت پایدار و مورد اعتماد
- به حداقل رسانیدن اشتباهات امنیتی پرمخاطره کاربران
- ایمن سازی نرم افزارها توسط کلیدهای رمز و فقط با استفاده از یک رمزعبور
- وجود سیاست متمرکز امنیتی در سازمان در
- جلوگیری از تنوع در تعریف امنیت نرم افزارهای موجود
- جلوگیری از وجود رمزعبورهای متنوع و احتمال شکستن آنها برای نفوذ
- پایین آوردن هزینه های سازمانی در امنیت اطلاعات

36

اصطلاحات متداول در فضای PKI

RA - Registry Authority	مرکز مجاز ثبت نام گواهی
Extended Validation (EV) Certification	اعتبارسنجی توسعه یافته
CP - Certificate Policy	سیاست گواهی
CSP - Certification Practice Statements	تعاریف ساختارهای تولید، ارائه، مدیریت و استفاده گواهی
CIP - Certificate Insurance Plan	سیاست بیمه گواهی
CRL - Certificate Revocation List	لسیت گواهی های باطل شده
CTL - Certificate Trust List	لسیت گواهی های ریشه
LDAP - Lightweight Directory Access Protocol	پروتکل انتشار گواهی
OCSP - Online Certificate Status Protocol	پروتکل مشخص کننده وضعیت گواهی بشکل لحظه ای
SCEP - Simple Certificate Enrollment Protocol	پروتکل دریافت گواهی توسط اداوات شبکه
CSR - Certificate Signing Request	درخواست امضای گواهی

37

اصطلاحات متداول در فضای PKI

CVC - Content Verification Certificate	امضای محتوای صفحات وب سایت
TSA - Time Stamp Authority	مرکز مجاز صدور مهرزمانی
KMI - Key Management Infrastructure	زیرساخت مدیریت کلید
KRA - Key Recovery Authority	مرکز مجاز بازیابی کلید
KGS - Key Generation System	سیستم تولید کلید

38

آنچه که از PKI نباید انتظار داشت!!

- عملیات مربوط به کنترل مجوز (Authorization)
  - این عملیات عمدتا از طریق سیستم PMI (Privilege Management Infrastructure)صورت می پذیرد.
- امنیت خودکار یک سیستم
  - عواملی همچون خطاهای انسانی، اشکالات نرم افزاری، یا امضای یک برنامه اجرایی مخرب و یا . . .

39

کاربردهای گواهی دیجیتال

- امنیت کانال های ارتباطی
- امنیت داده های ذخیره شده
- امنیت کد اجرائی
- امنیت پست الکترونیک
- احراز هویت افراد
- هویت شناسی رایانه کاربر
- هویت شناسی رایانه سرویس دهنده
- کنترل مجوز نرم افزار
- کنترل دسترسی به اطلاعات
- برقراری ارتباط امن بین سرویس دهنده وب و مرورگر اینترنتی(SSL)

گواهینامه دیجیتال

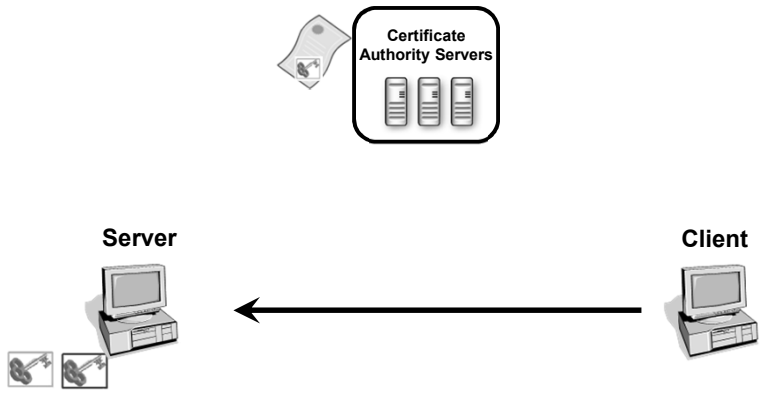
گواهینامه بهمراه کلید خصوصی

CRL

CTL

40

ارتباط امن در حوزه PKI



41

امضای دیجیتال در حوزه PKI

42

تشریح کاربرد گواهینامه در SSL

- **هدف:**
  - برقراری ارتباطی امن بین سرویس دهنـده وب و مرورگـر اینترنتـی بـا استفاده از پروتکل امنیتی
    Secure Socket Layer (SSL)
- **ابداع کننده :**
  - شرکت Netscape

43

تشریح کاربرد گواهینامه در SSL

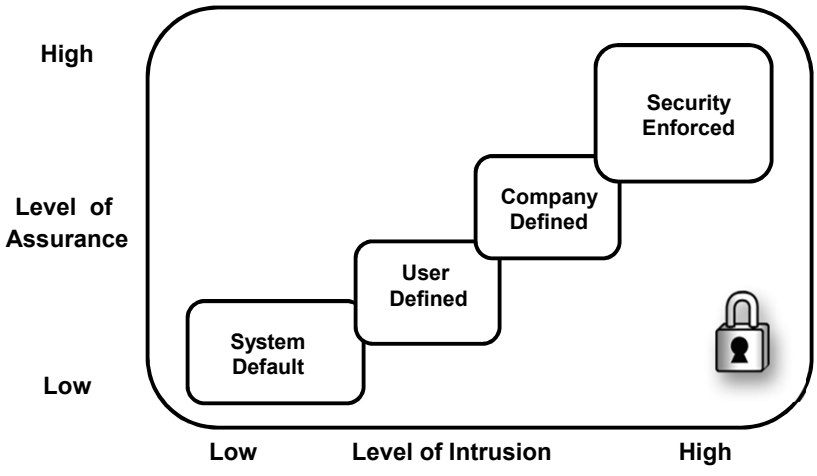
- **نیازمندیها:**
  - **گواهی دیجیتال سرویس دهنده**
  - **گواهی دیجیتال سرویس گیرنده**
  - **مرکز CA**
- **مکانیسم و روند ارتباط:**
  - **تایید هویت سرویس دهنده**
  - **توافق سرویس دهنده و گیرنده در نوع الگوریتم رمزنگاری**
  - **تایید هویت سرویس گیرنده**
  - **تهیه کلید متقارن و برقراری ارتباط بشکل رمز**

44

احراز هویت

- انتخابهای اصلی در احراز هویت:
  - نام کاربری و رمز عبور
  - توکن
  - کارت های هوشمند
  - اداوت زیست سنجی
  - ترکیبی از انتخاب های بالا
- کنترل مدیریت در احراز هویت:
  - قوانین تعریف شده توسط کاربر
  - قوانین اعلام شده توسط سیاست های گروهی

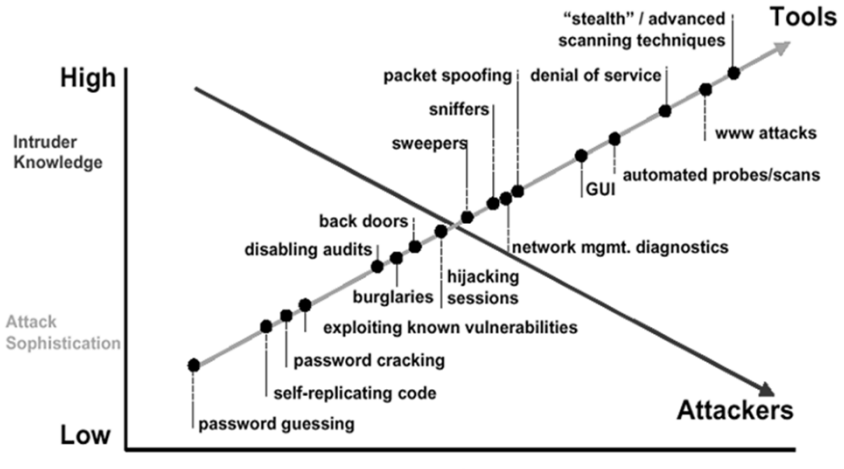
تئوری رمزعبور



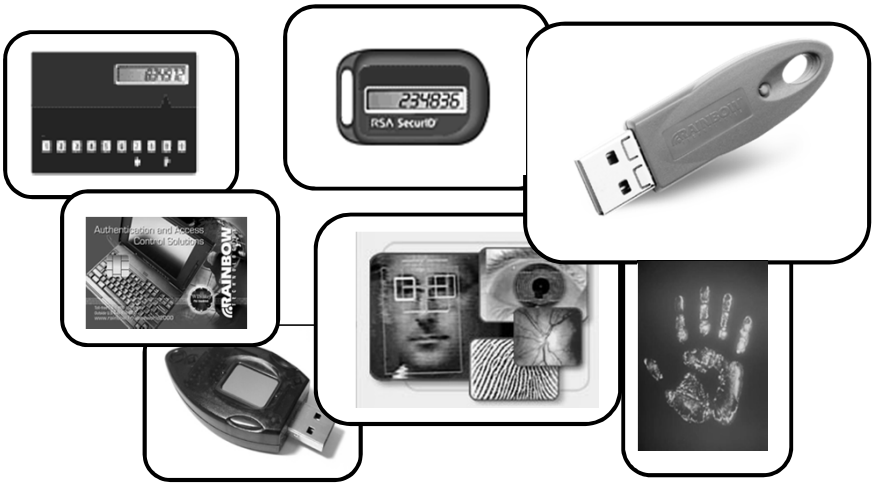
سیاست های رمزعبور

- **استفاده از روشهایی که مغز قادر به نگهداری اطلاعات و حدس آن نباشد:**
  - گروه های منطقی (ترکیب اعدد با کلمات)
  - وابستگی تصویری (پیوند کلمات با تصاویر)
- **استفاده از حروف غیر معمول**
  - مشکل در بخاطر سپردن آن که عمده مردم بصورت ناخودآگاه آن را روی کاغذ می نویسند.
- **رمزعبورهای تولید شده توسط رایانه**
  - مشکل در بخاطر سپردن آن که عمده مردم بصورت ناخودآگاه آن را روی کاغذ می نویسند.
- **رمزعبورهای وابسته به زمان**
  - مشکل در بخاطر سپردن آن که عمده مردم بصورت ناخودآگاه آن را روی کاغذ می نویسند.
- **رمزعبورهای مختلف برای کاربردهای مختلف**
  - مشکل در بخاطر سپردن آن که عمده مردم بصورت ناخودآگاه آن را روی کاغذ می نویسند.

رمزعبور: ضعیفترین نقطه درانجام یک حمله



حرکت بعدی در احرازهویت



انتخاب های اصلی در احرازهویت دوعاملی

نوع	روش	مزایا	مشکلات
OTP		امکان کار در هر محلی	- عدم رضایتمندی ۳۰ ٪از کاربران بدلیل سعی مجدد در احراز هویت - قیمت بالا ی دستگاه و سرور ACE - عمر مفید سه ساله
USB Token		- استفاده آسان - بخاطر سپاری راحت رمز توکن - مدیریت توزیع ساده و کم هزینه	نیازمند پورت USB
Smart Card		-راحتی حمل و نقل -- استفاده راحت -- امکان چاپ تصاویر	-نیاز به کارت خوان -- هزینه های سربار بالا
Biometric		قویترین نوع احرازهویت	-هزینه بر -- ضریب اعتماد پایین

استاندارد FIPS

استاندارد فدرال پردازش اطلاعات یا FIPS استانداردی است که به تشریح ملزومات محصولات فناوری اطلاعات طبقه بندی نشده دولت فدرال آمریکا می پردازد .این استاندارد توسط NIST تهیه شده و توسط CSB و ANSIپذیرفته شده است.

چهار سطح امنیتی برای این استاندارد لحاظ شده :سطح ۱ (ضعیف ترین سطح)تا سطح ۴ (قویترین سطح) .این سطوح برای تحت پوشش قرار دادن تمام محصولات امنیتی در نظر گرفته شده است و شامل موارد زیر می شود :

طرح اصلی و مستندات، واسط ماژول، سرویس ها و خدمات، ایمنی فیزیکی، ایمنی نرم‌افزاری، مدیریت کلید، الگوریتم های رمز نگاری، سازگاری الکترومغناطیسی /تداخل الکترومغناطیسی (EMI/EMC)و خود آزمایی

امنیت توکن براساس .A.A.A

- احرازهویت
  - احرازهویت دوعاملی بسیار قوی براساس آنچه که داریم و آنچکه می دانیم
- مجوز دسترسی
  - اطمینان از اینکه کسی که احرازهویت شده مجوز دسترسی به منابع را دارد.
  - اطمینان از برآورده شدن تمامی مقررات تنظیم شده برای امنیت و حفاظت اطلاعات
- کنترل دسترسی
  - دسترسی از هرکجا – امکان احرازهویت در سرویس های تشکیلاتی بصورت محلی و یا از روی یک شبکه عمومی
  - خاتمه نشست و ارتباط با جدا نمودن توکن
- قابل ممیزی
  - عدم انکار بواسطه امضا توسط گواهینامه های دیجیتالی

کاربرد توکن

- استفاده از امکانات آماده سیستم عامل همچون
  - امضای دیجیتال و رمزنگاری پست الکترونیک
  - احراز هویت در Local LAN، VPN، Terminal Service
- استفاده از توابع رمز در برنامه‌های مبتنی بر PKI
  - MSCAPI
  - PKCS#11
- استفاده در نرم‌افزارهای تحت وب همچون اتوماسیون‌های اداری

خلاصه اینکه ...

جایگزینی را برای رمزهای عبور بخصوص در تشکیلات بزرگ با حساسیت اطلاعاتی خاص پیدا کنید.

- رمزعبور مهم است ولی همانند استفاده از یک قفل قدیمیست
  - احساس امنیت را بشما خواهد داد ولی
  - واقعا راه حل موثری برای امنیت شما نخواهد بود.
- امکان احرازهویت تک عاملی صحیح بدلیل ماهیت رمزعبور وجود ندارد.
- عمدتا تلاش برای بالابردن امنیت براساس رمزعبور نتایج معکوسی خواهد داد .ضمن اینکه باعث افزایش هزینه های پشتیبانی نیز می گردد.
  - ۹۰ ٪افراد باعث لو رفتن رمزعبورهای خود در مکان های عمومی شده اند.
  - ۷۵ ٪افراد رمزعبور همکاران خود را می دانند.
  - ۶۶ ٪افراد از یک رمزعبور برای کاربردهای مختلف استفاده می کنند.
  - ۵۵ ٪افراد رمزعبور خود را براساس اسامی افراد خانواده، شماره تلفن منزل و ..تعیین می نمایند

Hardware security module (HSM)

- ماژول امن سخت افزاری یک ابزار امنیتی است که کلیـد هـای رمـز نگـاری را تولیـد، ذخیـره و محافظـت می‌کند .این ماژول ها به وسیله CPUهای رمز نگار برای انجام عملیات رمز نگاری (متقارن و نا متقـارن) ویژه سازی شده اند و بطور کلی باعث کاهش حجم کاری سرور و افـزایش بـازدهی نـرم افـزار هـای رمـز نگاری می شوند.

- ماژول ها ی امن سخت افزاری زیر بنای یک CAبا سطح بالای امنیتی را ایجاد می کنند .این مـاژول هـا برای محافظت از کلید خصوصی ریشه در ساختار PKI، شتاب دهنده عملیات رمز نگاری و امضـاء دیجیتـال اسـتفاده مـی شـوند و در مـوارد زیـادی مثـل Web Serverهـا ، Application Serverهـا و Stamping Server Timeها ، VPN، Firewallو ASPو ISPها کاربرد دارند.

Hardware security module (HSM)

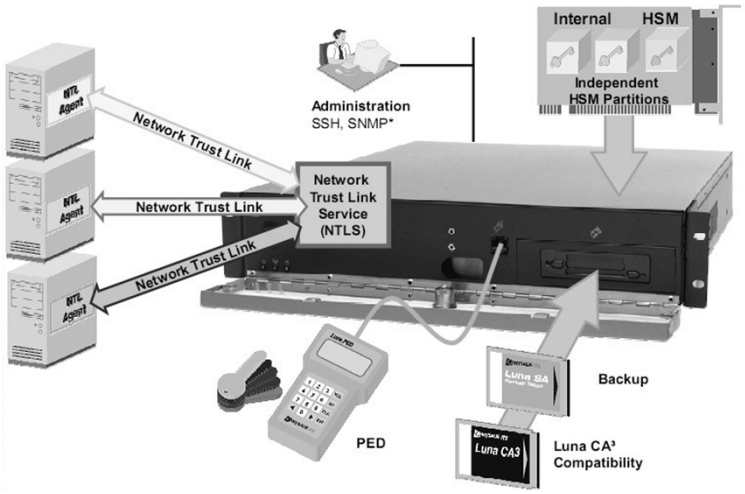
- **انواع کاربردی ماژول‌های امن سخت افزاری**
  - ماژول‌های اختصاصی و تک منظوره
  - ماژول‌های چند کاربردی

- **شکل فیزیکی ماژول‌های امن سخت افزاری**
  - ماژول‌های داخلی (Internal)
  - سخت افزارهای خارجی و یا متصل به شبکه (Network-Attached)

ماژول‌های داخلی (Internal)

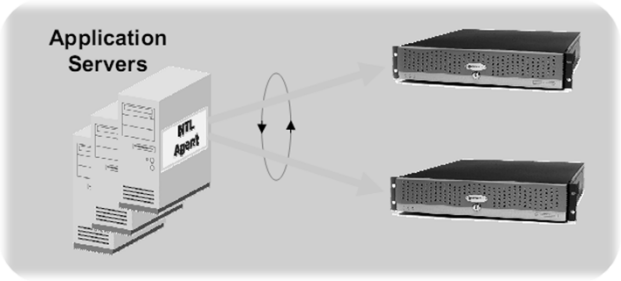
مزیت استفاده از ایـن نـوع مـاژول در قیمـت پـایین آن می‌باشد ولیکن در صورت تعدد سرویس دهندگان و حجم بالای عملیاتی اسـتفاده از ایـن نـوع مقـرون بـه صـرفه نمی‌باشد.

سخت‌افزارهای متصل به شبکه (Network-Attached)



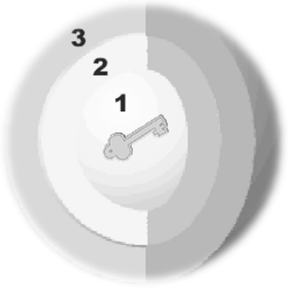
سخت‌افزارهای متصل به شبکه (Network-Attached)

- High Availability & Load Sharing



Hardware security module (HSM)

لایه‌های امنیتی برای دسترسی به کلیدهای رمز:



۱)رمزنگاری متقارن (3DES)

۲)دسترسی بصورت "M of N"

۳)سخت افزار ضد سرقت

Hardware security module (HSM)

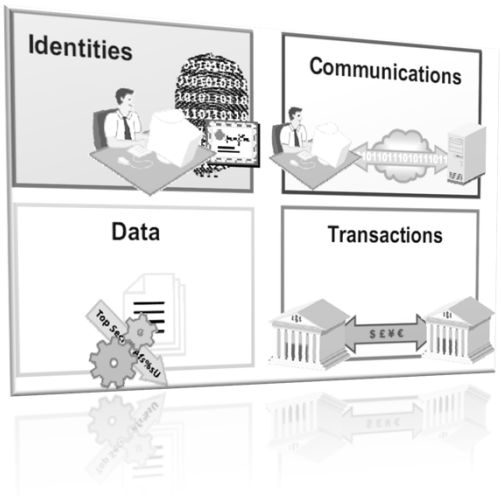
ویژگی‌های ماژول‌های امن سخت‌افزاری

- امنیت
- تفکیک بر حسب کاربرد
- مدیریت سخت‌افزاری کلید
- غیر قابل کپی برداری
- عدم امکان در استفاده غیرمجاز
- کنترل بالای Hardware Failure

Hardware security module (HSM)

کاربردها

عمده‌ترین کاربرد ماژول‌های امن سخت‌افزاری در امن نمودن:



خریداران اینگونه از محصولات

تمامی سازمان‌ها، اداره‌ها و شرکت‌هایی که:

- کاربران آنان از راه دور و یا از طریق سیستم‌های تحت وب نیـاز بـه تغییـر، تصـحیح و یـا مشـاهده اطلاعـات شخصی و یا سازمانی دارند همانند شرکت‌های نفتی، بانکها و مؤسسات مالی اعتباری، وزارتخانه ها و ..
- دارای اطلاعات طبقه‌بندی شده هستند و دسترسی به این دسـته از اطلاعـات نیـاز بـه مجوزهـای خـاص دارد همانند وزارت دفاع و پلیس و ..
- پرسنل امکان دسترسی به اطلاعات شخصی افراد را دارند و احتمال استفاده غیرمجاز از اینگونه اطلاعات وجـود داشته باشد همانند خدمات درمانی، مراکز تحصیلی و ..
- و تمامی کسانی که به امنیت اطلاعات خود، سازمان و کاربرانشان می‌اندیشند.

باتشکر از حسن همراهی شما

پاسخ به سئوالات؟؟

www.gamelectronics.com
Tehran.irannsr.org

64