سه شنبه 07 شهريور 1391 - 07:29

روش‌هاي رمزنگاري

يكي از مهم‌ترين مباحث در امنيت شبكه و رايانه رمزنگاري است. رمز نگاري دانشي است كه به بررسي و شناخت اصول و روش‌هاي انتقال يا ذخيره اطلاعات به صورت امن (حتي اگر مسير انتقال اطلاعات و كانال‌هاي ارتباطي يا محل ذخيره اطلاعات ناامن باشند) مي‌پردازد

برقراري امنيت در دنيايي نا امن
روش‌هاي رمزنگاري
جام جم آنلاين: يكي از مهم‌ترين مباحث در امنيت شبكه و رايانه رمزنگاري است. رمز نگاري دانشي است كه به بررسي و شناخت اصول و روش‌هاي انتقال يا ذخيره اطلاعات به صورت امن (حتي اگر مسير انتقال اطلاعات و كانال‌هاي ارتباطي يا محل ذخيره اطلاعات ناامن باشند) مي‌پردازد.

رمزنگاري از زمان‌هاي قديم براي حفظ اطلاعات، همخواني اطلاعات فرستاده شده و دريافت شده، تصديق هويت و سنديت استفاده مي‌شد و اين اصول بايد در هر نوع از رمزنگاري رعايت شود.

حفظ اطلاعات و رازداري به اين معني است كه فقط فرستنده و گيرنده محتواي پيغام را بفهمند. ممكن است افراد ديگر بتوانند محتواي آن را ببينند، اما از ديد آنها محتواي آن بايد كاملا نامفهوم باشد.

تصديق هويت به اين معني است كه هم فرستنده و هم گيرنده از هويت واقعي يكديگر مطلع باشند. همخواني پيغام به اين معني است كه فرستنده و گيرنده مطمئن باشند اطلاعات فرستاده شده، بعد از ارسال تغييري نكرده است و اگر اين اتفاق افتاده باشد از اين موضوع با خبر شوند.

اين اصل شامل تغييرات محتواي پيغام، تغيير اسم فرستنده و يا گيرنده، تأخير در ارسال پيغام و ترتيب پيغام‌ها مي‌شود.

رمزنگاري به سه نوع متقارن (symmetric encryption)، نامتقارن (asymmetric encryption) و تابع درهم (hash function) تقسيم مي‌شود.

رمزنگاري متقارن

رمزنگاري متقارن به هر نوع رمزنگاري گفته مي‌شود كه در آن يك كليد براي رمزنگاري و رمزگشايي پيغام استفاده مي‌شود. در اين نوع رمزنگاري، كليد بايد فقط بين فرستنده و گيرنده به اشتراك گذاشته شود.

رمزنگاري متقارن به دو روش جرياني (stream cipher) و بلوكي (block cipher) پياده‌سازي مي‌شود. در روش بلوكي اطلاعات به قسمت‌هاي كوچك تر تقسيم مي‌شود و هر قسمت رمزنگاري مي‌شود در حالي كه در روش جرياني هر كاراكتر به تنهايي رمزنگاري مي‌شود.

One Time Pad، SEAL، Fish، RC4 الگوريتم‌هايي هستند كه از روش جرياني استفاده مي‌كنند كه RC4 يكي از محبوب ترين آنهاست و در رمزنگاري WEP در استاندارد 802.11 استفاده مي‌شود. رمزنگاري متقارن انواعي دارد از جمله:

الف: رمزنگاري سزار

اين رمزنگاري يكي از قديمي ترين و ساده ترين انواع رمزنگاري است كه براي اولين بار توسط ژوليوس سزار در جنگ‌ها براي حفاظت از محتواي پيغام‌ها استفاده مي‌شد.

در اين روش، هر حرف از حروف الفبا به اندازه مشخصي جابه‌جا مي‌شوند. مثلا اگر جابه‌جايي سه خانه است، به جاي حرف A حرف D قرار مي‌گيرد و براي رمزگشايي، بايد به همين مقدار حزوف را در جهت عكس جابجا كنيد. همانطور كه الگوريتم اين روش بسيار ساده است، حمله براي رمزگشايي آن نيز ساده است.

براي رمزگشايي، كافي است (با استفاده از روش brute force) كليدهاي يك تا 25 را امتحان كنيم تا يكي از آنها متن رمزنگاري شده

را به كلمات با معني تبديل كند.

الگوريتم سزار در واقع يك نوع الگوريتم جايگزيني نيز به حساب مي‌آيد. به طور كلي در الگوريتم‌هاي جايگزيني هر حرف الفبا با يك حرف ديگر جايگزين مي‌شود و گيرنده متن رمزنگاري شده بايد عكس اين عمل را انجام دهد و از اين روش بيش از 2000 سال است كه استفاده مي‌شود.

در اين روش كليد، جدولي از حروف خواهد بود. در اين روش، حمله با روش brute force سخت تر است؛ چراكه در اين روش تعداد كليدها 26! است و محاسبه و تحليل آنها عملا زمان بسيار زيادي مي‌برد و غير ممكن است.

براي مثال اگر در هر ثانيه 100 ميليارد كليد را امتحان كنيم، 100 ميليارد سال طول مي‌كشد! براي حمله و رمزگشايي آن از روشي به اسم آناليز تكرار استفاده مي‌كنند.

در اين نوع حمله، تعداد تكرار حروف رمزنگاري شده، با تعداد تكرار حروف در متن‌هاي عادي انگليسي مقايسه مي‌شود و از اين طريق ممكن است كليد رمزنگاري را بدست آورند و هر چقدر متن طولاني‌تر باشد، رمزگشايي آن ساده‌تر مي‌شود.

ب: رمزنگاري بلوكي

در اين روش، اطلاعات با گروه‌هاي مختلف با طول معين تقسيم مي‌شوند و هر گروه يا بلوك به صورت جداگانه رمزنگاري مي‌شود.

الگوريتم‌هاي معروفي كه از اين روش استفاده مي‌كنند شامل 3DES ،DES و AES هستند.

Data Encryption Standard:

اين الگوريتم از سوي سازمان ملي استانداردهاي آمريكا (NBS) به عنوان الگوريتم رسمي براي استاندارد پردازش اطلاعات فدرال (FIPS) انتخاب شد و با اين‌كه اين الگوريتم در بسياري از كشورها استفاده مي‌شود، الگوريتمي نا امن براي بسياري از كاربردها به حساب مي‌آيد و اين صرفا به علت طول كليد 56 بيتي استفاده شده در آن است. در سال 1999 اين الگوريتم در كمتر از 23 ساعت با حمله brute force رمزگشايي شد. به همين دليل الگوريتم 3DES طراحي شد كه به نوعي همان الگوريتم DES است كه با 3 كليد متفاوت هر بلوك را 3 بار رمزنگاري مي‌كند.

Advanced Encryption Standard:

از سوي ديگر به جاي DES الگوريتم‌هاي متعددي طراحي شدند كه در طي يك رقابت جايگزين آن شوند. در سال 1997 براي اين رقابت معيارهايي از سوي مؤسسه ملي استاندارد و تكنولوژي آمريكا (NIST) تعيين شد كه به شرح زير است:

• اين الگوريتم بايد بدون محدوديت در دنيا استفاده شود

• جزئيات اين الگوريتم بايد با زبان ANSI C و JAVA قابل پياده سازي باشد.

• بايد در مقابل حملات مستحكم باشد

• وقتي الگوريتم براي عموم باز و قابل دسترس بود بايد قدرت خود را حفظ كند.

• امنيت به وسيله ابهام ممنوع است.

• درست كردن كليد بايد سريع باشد.

• سادگي الگوريتم

• قابل پياده‌سازي براي پلت فرم‌هاي كوچك مانند كارت‌هاي هوشمند و پلت فرم‌هاي بزرگ مانند سرور ها.

در واقع الگوريتم AES از سوي دنيا مورد آزمايش قرار گرفت نه فقط NIST. در طي اين فرآيند، الگوريتم‌هاي ضعيف از دور رقابت خارج شدند. و در سال 2000 الگوريتم Rijndael كه توسط Vincent Rijmen و Joan Daemen از كشور بلژيك نوشته شده بود برنده اين رقابت اعلام شد.

رمزنگاري نامتقارن

يكي از مشكلات رمزنگاري به شيوه متقارن، ارسال و توزيع كليد است؛ اگر هكري كه مي‌خواهد محتواي پيغام‌هاي رد و بدل شده را بداند، با داشتن كليد به راحتي به هدف خود مي‌رسد و رمزنگاري اثر خود را از دست مي‌دهد. گيرنده براي رمزگشايي به كليد نياز دارد و همچنين كليد نبايد به دست كسي جز او برسد.

براي حل اين مشكل راه حل‌هايي پيش نهاد شده است كه به آنها مي‌پردازيم.مي‌توانيم كليد را قبل از شروع ارتباط توزيع كنيم. اين روش فوايدي دارد اما بسيار محدود اگر به گيرنده دسترسي فيزيكي داريم مي‌توانيم كليد را از طريق يك كارت حافظه به او برسانيم اما اين كار براي كسي كه به او دسترسي فيزيكي نداريم تقريبا عملي نيست. در ضمن اگر تعداد گيرنده‌ها زياد باشند از اين روش نمي‌توان استفاده كرد.

رمزنگاري تابع در هم

راه‌حل ديگر استفاده از يك مركز توزيع كليد است كه گيرنده براي دريافت كليد به آن مراجعه كند.اين روش نيز محدوديت‌هايي دارد. فرآيند توليد كليد به سادگي روش‌هاي ديگر نيست.

در ضمن در اين روش اگر مركز توزيع كليد از كار بيفتد همه ارتباطات رمزنگاري شده متوقف مي‌شود و اگر يك هكر بتواند به اين مركز نفوذ كند، روزنگاري اثر خود را از دست مي‌دهد.

روشي كه كاربرد بيشتري دارد استفاده از كليد عمومي است. در اين روش كليدي به عنوان كليد عمومي در دسترس عموم قرار مي‌گيرد و اين به معني آن است كه هر كس مي‌تواند با استفاده از اين كليد پيغام‌ها را رمزنگاري كند ولي نمي‌تواند از آن براي رمزگشايي استفاده كند.

از سوي ديگر كليدي كه براي رمزگشايي استفاده مي‌شود خصوصي است و نبايد در دسترس كسي جز گيرنده قرار گيرد. در اين روش گيرنده دو كليد خصوصي و عمومي را مي‌سازد و اين دو كليد جفت يكديگر هستند.

كليد عمومي را براي فرستنده مي‌فرستد و فرستنده با استفاده از آن مي‌تواند اطلاعات را رمزنگاري كند و اين اطلاعات فقط با استفاده از كليد خصوصي گيرنده قابل رمزگشايي هستند.

در اين روش مهم نيست اگر شخص ديگري به كليد عمومي دسترسي پيدا كند، مهم اين است كه كليد خصوصي فاش نشود.

با استفاده از اين روش مشكل توزيع كليد حل مي‌شود اما اين روش نسبت به رمزنگاري متقارن زمان بيشتري مي‌برد.

محمدعلي زارعي‌فر