مقدمه رمزنگاری شناسه مبنا

علی محمودی

مقدمه

IBC[1] یا همان رمزنگاری شناسه مبنا، زیرمجموعه از رمزنگاری کلید عمومی است که در آن از مشخصات فردی از قبیل رایانامه، آدرس IP و ... به‌عنوان کلید عمومی در رمزگذاری و تائید امضا به جای استفاده از گواهی و زیرساخت کلید عمومی (PKI) بهره می‌گیرد که به طور قابل ملاحظه‌ای پیچیدگی و هزینه ایجاد زیر ساخت کلید عمومی را کاهش می‌دهد. دراین روش نیاز به یک عامل سوم مورد اعتماد به نام PKG[2] داریم که به‌طور عمده وظیفه تولید کلید خصوصی کاربران را بر عهده دارد. این ایده اولین بار توسط شامیر[3] در سال 1984مطرح شد. شامیر توانست طرحی برای امضا، مبتنی بر رمزنگاری شناسه مبنا (IBS[4]) با استفاده از توابع RSA ارائه کند اما نتوانست طرحی برای رمزگذاری بر این مبنا (IBE[5]) معرفی کند و این موضوع مدت‌ها به‌عنوان یک مسئله حل نشده باقی ماند تا سال 2001 که این مسئله حل شد و تاکنون طرح‌های رمزگذاری بی‌شماری مبتنی بر این زیرساخت مطرح شده است.

بررسی اجمالی مزایا و معایب IBC و مقایسه آن با PKI

همان‌طور که می‌دانیم در الگوریتم‌های رمزنگاری ما با دو نوع الگوریتم مواجه هستیم، الگوریتم‌های متقارن و نامتقارن (کلید عمومی). در الگوریتم‌های کلید عمومی مسئله‌ای که مطرح می‌شود، بحث صحت و اعتبار کلیدهای عمومی است که در روش سنتی از زیرساخت کلید عمومی استفاده می‌شود، اما این زیر ساخت مشکلاتی را به همراه دارد که با ظهور IBC این مشکلات از بین می‌رود ولی در عوض مسائل جدیدی مطرح خواهد شد. در ادامه به بیان این معایب و همچنین محاسن این دو نوع زیرساخت و مقایسه آنها می‌پردازیم:

1- معایب PKI

- در این زیرساخت، به‌نحوی تمامی کاربران به‌طور متوالی با PKI در ارتباط هستند و نظم بخشیدن به روال‌ها و سلسله‌مراتب با مسائل و پیچیدگی‌هایی همراه است.
- هزینه زیاد زیر ساخت
- چگونگی طراحی و راه‌اندازی CA
- نحوه مدیریت کلیدها و الگوریتم‌ها
- نحوه ابطال کلیدها و تولید لیست گواهی‌های باطل شده (CRL) و مدیریت آن.
- در واقع بحث گواهی‌ها و مدیریت آن‌ها مسئله اصلی PKI است.

2- مزایای IBC

الف) Certificate-Free : مسائل مربوط به تولید و بررسی و مدیریت و توزیع گواهی در اینجا مطرح نیست.

ب) Directory-Less :

- گیرنده پیام (باب)، بدون اینکه بخواهد ابتدا کلید عمومی فرستنده پیام (آلیس) را جستجو کند می‌تواند پیام را رمز و ارسال کند.

1- Id-based Cryptography
2- Private Key Generator
3- Shamir
4 -ID-Based Signature
5- ID-Based Encryption

- آلیس لازم نیست وقتی پیام رمز شده باب را دریافت می‌کند کلید خصوصی خود را در اختیار داشته باشد و پس از دریافت، آن را به‌دست می‌آورد.

الف) Automatic Revocation : دیگر نیازی به CRLs[6] یا OCSP[7] نیست و با اعمال برچسب زمانی در انتهای شناسه مورد استفاده به‌عنوان کلید عمومی، در انتهای هر ارتباط کلید خصوصی باطل می‌شود و در هر ارتباط آلیس کلید خصوصی جدید خود را از PKG دریافت می‌کند.

ب) Support for Key Recovery : PKG قادر به تولید کلید خصوصی برای تمامی کاربران است و در صورت نیاز، مانند از یاد بردن و یا مسائل حقوقی (درمواقعی که بحث محدودکردن امنیت برای کاربران مطرح است) می‌تواند از این قدرت استفاده کند.

3- معایب IBC

- **Effect of Catastrophic Compromise**: امنیت تمامی کلیدهای خصوصی در گرو امنیت کلید خصوصی PKG است و چنانچه این کلید فاش شود تمامی پیام‌های رمزشده قبلی فاش خواهد شد و تمامی امضاها نامعتبر می‌شوند.
- **Key Escrow**: PKG قادر به تولید کلید خصوصی برای تمامی کاربران است و این، خطر هرگونه سوء استفاده را فراهم می‌کند چرا که وی هر پیامی را می‌تواند رمزگشایی کند و به جای هر کسی امضا تولید کند. (البته راه‌هایی برای جلوگیری از این موضوع وجود دارد از قبیل اینکه از چند PKG استفاده کرد و هرکدام قسمتی از کلید خصوصی را تولید کنند و هرکسی برای به‌دست آوردن کلید خصوصی، ابتدا خود را به تمامی این PKGها احراز اصالت کرده و سپس کلید خود را با استفاده از روش تسهیم راز[8] به‌دست آورد.)
- **Inability to Provide Non-repudiation**: این مورد نمونه‌ای از همان Key Escrow است که امکان انکار امضا پیش می‌آید در صورتی که PKG مورد تایید همگان نباشد.

استانداردهای مکانیزم رمزنگاری شناسه مبنا

استانداردهای مکانیزم رمزنگاری شناسه مبنا عبارتند از :

- ISO/IEC 11770-3, key management mechanisms usingasymmetric techniques
- ISO/IEC 14888-2, digital signatures with appendix integer factorization based mechanisms
- ISO/IEC 14888-3, digital signatures with appendix discrete logarithm based mechanisms
- IEEE P1363.3, identity-based public key cryptographyusing pairings

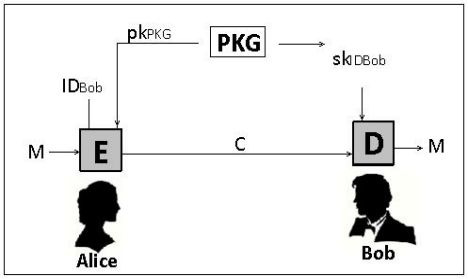
مفاهیم اولیه در مورد امضا و رمزگذاری

مفاهیم اولیه رمزگذاری شناسه مبنا (IBE)

در طرح IBE، فرستنده (آلیس) می‌تواند از مشخصات فردی گیرنده (باب) که می‌تواند دنباله‌ای از آدرس IP، رایانامه یا حتی عکس دیجیتال (به‌عنوان کلید عمومی) باشد، استفاده کند. در مقابل باب می‌تواند کلید خصوصی متناظر با این اطلاعات شخصی را از مرجع مورد اعتماد به نام تولیدکننده کلید خصوصی (PKG) دریافت کند و عمل رمزگشایی را انجام دهد.

مراحل طرح IBE عبارت است از:

1. آماده‌سازی: ابتدا PKG جفت کلید عمومی و خصوصی خود را تولید می‌کند (pk_{PKG},sk_{PKG}) و کلید عمومی خود (pk_{PKG}) را در اختیار همگان قرار می‌دهد. این پارامتر، پارامتر ثابت طرح برای مدت طولانی خواهد بود.



7- Online certificate status checking

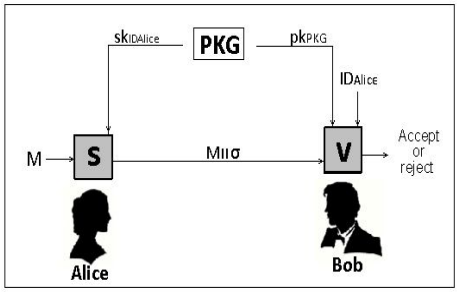
8 -Secret sharing

2. دست‌یابی کلید خصوصی: گیرنده (باب) مرحله احراز اصالت خود را برای PKG انجام می‌دهد و کلید خصوصی خود (sk_{IDBob}) که متناظر با اطلاعات شخصی (ID_{Bob}) وی هست را دریافت می‌کند.
3. رمزگذاری: با استفاده از مشخصات باب (ID_{Bob}) و کلید عمومی PKG (pk_{PKG}) آلیس پیام (M) خود را رمز می‌کند و پیام رمزشده C را به‌دست می‌آورد.
4. رمزگشایی: باب با دریافتC و با استفاده ازکلید خصوصی خود، C را رمزگشایی می‌کند و M را به‌دست می‌آورد.

مفاهیم اولیه امضا شناسه مبنا(IBS)

در امضا دقیقا برعکس رمزگذاری عمل می‌کنیم به‌صورت مراحل زیر:

1. آماده‌سازی: ابتدا PKG جفت کلید عمومی و خصوصی خود را تولید می‌کند (pk_{PKG},sk_{PKG}) و کلید عمومی خود (pk_{PKG}) را در اختیار همگان قرار می‌دهد.
2. دستیابی کلید خصوصی: امضاکننده (آلیس) ابتدا خود را برای PKG احراز اصالت می‌کند، سپس کلید امضا (خصوصی) خود ($sk_{IDAlice}$) متناظر با شناسه‌اش (ID_{Alice}) را دریافت می‌کند.
3. تولید امضا: آلیس با استفاده از کلید $sk_{IDAlice}$ امضای σ را روی پیام M اعمال می‌کند.
4. بررسی امضا: باب پس از دریافت پیام M و امضای σ و با در اختیار داشتن کلید عمومی PKG (pk_{PKG}) و مشخصات آلیس (ID_{Alice}) صحت امضا را بررسی می‌کند و امضا را قبول یا رد می‌کند.



نتیجه گیری

در این مقاله، ابتدا توضیح مختصری در مورد IBC داده شد. سپس در ادامه به مقایسه این زیرساخت با زیرساخت کلید عمومی و استانداردهای این سیستم پرداخته و در انتها مفاهیم اولیه در مورد امضا و رمزگذاری به‌صورت مختصر معرفی شد.

منابع

[1]. Baek, Joonsang, et al. "A survey of identity-based cryptography." *Proc. of Australian Unix Users Group Annual Conference*. 2004.

[2]. Boneh, Dan, and Matt Franklin. "Identity-based encryption from the Weil pairing." *Advances in Cryptology—CRYPTO 2001*. Springer Berlin Heidelberg, 2001.

[3]. Shamir, Adi. "Identity-based cryptosystems and signature schemes."*Advances in cryptology*.Springer Berlin Heidelberg, 1985.

[4].Stinson, Douglas R. *Cryptography: theory and practice*. CRC press, 2005.