مرکز خدمات ترجمه تخصصی ترجمه بازار

نام مشتری

نمونه ترجمه مقاله رشته ---

شماره پروژه ترجمه

نمونه ترجمه

ترجمه مقاله ☒

ترجمه کتاب ☐

امضای دیجیتالی غیرقابل جدا شدن مبتنی بر هویت برای عوامل سیار در تجارت الکترونیکی

چکیده

برای فعال کردن عوامل سیار به منظور امضای ایمن از میزبان‌های (هاست) بالقوه مخرب در تجارت الکترونیکی و سایر برنامه‌ها، ما تعریف و مفهوم امنیتی طرح‌های امضای دیجیتال غیرقابل جدا شدن مبتنی بر هویت را پیشنهاد کردیم. از همه مهمتر، ما یک طرح امضای دیجیتال غیرقابل جدا شدن مبتنی بر هویت مشخص با امنیت قابل اثبات ارائه داده‌ایم. در این طرح، عوامل سیار هنگام تولید امضای دیجیتالی از طرف امضا کننده اصلی، نیازی به داشتن کلید خصوصی ندارند، بنابرکلید خصوصی به خطر نمی‌افتد. عملکرد رمزگذاری شده با نیاز امضا کننده اصلی ترکیب شده است، بنابراین می‌توان از استفاده غیر اخلاقی الگوریتم امضا جلوگیری کرد. علاوه بر این، از آنجا که این طرح مبتنی بر هویت است، تأیید امضاهای تولید شده توسط عوامل سیار نیازی به تأیید کل مسیر گواهی یا ارتباط با مرجع صدور گواهی ندارد. بنابراین، در مقایسه با طرح‌های امضای غیر قابل جدا شدن حال حاضر، هزینه تأیید کاهش می‌یابد و حتی وابستگی به اتصال شبکه پایدار کم‌رنگ می‌شود.

متن اصلی (انگلیسی) در صفحه بعدی آمده است ...

METHODOLOGIES AND APPLICATION

Identity-based undetachable digital signature for mobile agents in electronic commerce

Yang Shi[1] · Jingxuan Han[1] · Jiangfeng Li[1] · Guoyue Xiong[1] · Qinpei Zhao[1]

Abstract

To enable mobile agents signing securely on potentially malicious hosts in electronic commerce and other applications, we proposed the definition and security notion of identity-based undetachable digital signature schemes. More importantly, we proposed a concrete identity-based undetachable digital signature scheme with provable security. In the scheme, mobile agents need not carry the private key when they generate digital signatures on behalf of the original signer, so the private key will not be compromised. The encrypted function is combined with the original signer's requirement, so misuse of the signing algorithm can be prevented. Moreover, because the scheme is identity-based, verification of the signatures generated by mobile agents does not require either verification of the entire certificate path or communication with the certification authority. Therefore, compared with existing undetachable signature schemes, the cost of verification is reduced and even the dependence on a stable network connection is weakened.

Keywords Mobile agents · Identity-based · Undetachable digital signatures · Electronic commerce

1 Introduction

With the development in technologies of distributed computing, mobile agent technologies and systems have attracted great interest. Commonly, a mobile agent system comprises platforms and mobile agents. Agents are a type of computer software acting autonomously on behalf of an organization or a person (Object Management Group 1997). Meanwhile, platforms are agent systems that can generate, execute, transfer, and terminate agents. Like an agent, an agent system is associated with an authority identifying the organization or person for which the agent system acts. Moreover, agent systems operate on computers connected by networks and can exchange information with each other via a communication infrastructure. While static agents may reside on hosting platform or an immobile system, mobile agents can transport themselves easily from one platform in a network to another. They can also automatically suspend execution on one platform and migrate to another to restart their computations. The capability of them to travel enables a mobile agent to migrate to a destination agent system that contains an entity in which the agent wishes to interact. Furthermore, the mobile agent may utilize the destination agent platform's services.

The advent of electronic business practices has significantly increased the demand for flexibility in distributed computing environments and interoperability to enable real-time exchange of data across enterprise borders, across applications, and across IT platforms. Compared with traditional computing models (e.g., client/server), mobile agent technology has several significant advantages in electronic commerce applications (Busch et al. 1998; Singh and Dave 2013). First, autonomous mobile agents strive to achieve a given goal without continuous supervision by the owner of the agent. Second, when a host is shut down, all mobile agents running on that machine are warned and given time to dispatch; they then continue their operation on another host in the network. Third, users may dispatch agents to a target host via a temporary network connection. After the agent is dispatched, the temporary network connection can be brought down until a later time.

In electronic commerce, an intelligent mobile agent that roams the Internet to purchase services or goods on behalf of its owner usually has many advantages. It can specifically allow businesses to respond rapidly to market opportunities

Communicated by V. Loia.

✉ Qinpei Zhao
qinpeizhao@tongji.edu.cn

[1] Tongji University, Shanghai 201804, People's Republic of China