Asain Journal of Information Technology 5 (3) : 321-323, 2006

Impact of Elliptic Curve Cryptosystem in the Mobile Communication

[1]P.Balasubramaniam and [2]E.Karthikeyan
[1]Department of Mathematics, [2]Department of Computer Science
Gandhigram Rural Institute-Deemed University, Gandhigram - 624 302, Tamil Nadu, India

Abstract: Commercial transactions conducted over the Internet, known as electronic commerce (E-commerce), play an important role in the global economy and the rapid growth of mobile devices providing more opportunities for doing mobile E-commerce (M-commerce). Due to the constraints of the resources in the mobile device, we have to increase the transactions between the mobile device and web server. Though many cryptosystems and protocols are there, they are not suitable for mobile environment. ECC is an emerging cryptosystem, which is more suitable for handheld devices like PDA, mobile phones etc. Though various means are available to speeding web transaction, we are presenting the impact of ECC, a new public-key cryptosystem in mobile commerce / environment from the hand held device to the web server. The conventional public-key cryptosystem have been replaced by ECC and found that ECC is good one for the web transaction.

Key words: M-Commerce, cryptography, elliptic curve, digital signature

INTRODUCTION

Commercial transactions conducted over the Internet, known as electronic commerce (E-commerce), play an important role in the global economy. In recent years the areas of mobile computing and wireless networks have seen an explosive growth both in terms of the number of services provided and the types of technologies that have become available, provides more opportunities to do E-business transactions, which is called as mobile E-commerce (M-commerce). So the consumers will be able to access desired products anytime and anywhere. The continued growth in wireless voice and data communications has opened up a broad new frontier for mobile E-commerce applications
and services.

The world is forecasting that M-commerce service will be one of the next biggest growths in the area of information and communication technology market. According to Telecom Trends International, the volume of business using M-commerce would be from $6.8 billion in 2003 to more than $554 billion in 2008[1]. The following graph illustrates the growth of fixed E-commerce and mobile E-commerce (Fig. 1) .

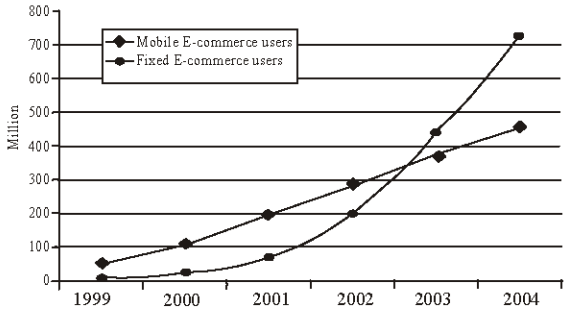

Fig. 1: Predicted reach for fixed and mobile E-commerce (source: ARC Group, Intelligence)

SECURITY ISSUES IN MOBILE COMMUNICATION

Network remains the backbone of any external data communication and it may be wire or wireless. As mobile networks expand their bandwidth, mobile phones, as with any other Internet device becomes substantially exposed to Internet security vulnerabilities. The hackers will actively target all M-commerce services, service providers and the underlying infrastructure. Since transactions eventually get routed over a public network, security must be maintained not only by the mobile carriers but also all the way through to the M-commerce server. Protecting critical information and infrastructure has become imperative in this emerging, always connected, always networked in everywhere environment. As web services move into complex business transactions, security will play a major role. Sensitive information, like credit card number, order details, etc which is transmitted across the Internet from the browser to the server. The third party could hack this information at some point on the network between the browser and the server.

International Data Corporation (IDC) predicted that the worldwide information security market would increase from roughly $6.7 billion in 2000 to $21 billion by 2005.

Corresponding Author: P. Balasubramaniam, Department of Mathematics, Gandhigram Rural Institute-Deemed University, Gandhigram-624 302, Tamil Nadu, India

Security over the mobile platform is more critical due to the open nature of wireless networking and implement on a mobile platform because of the resource limitation of the mobile hand held devices.

Cryptography, a fascinating scientific mathematics can be used to provides secure communication for which the two types of cryptosystems Symmetric-key cryptography and Asymmetric-key cryptography can be used. The basic cryptographic services are data integrity, confidentiality, authentication and non-repudiation[2]. The various cryptography algorithms are to be implemented in various network security protocols.

SECURITY PROTOCOLS FOR MOBILE COMMUNICATION

WAP (Wireless Application Protocol) is the *de facto* world standard for wireless information and telephony services. SSL (Secure Socket Layer) is the most popular, widely used trusted security protocol on the web[3]. SSL offers all the security services like encryption, source authentication and integrity for data exchanged over insecure public network. It operates above a reliable transport service and has the flexibility to accommodate different cryptographic algorithms for hashing (SHA), key agreement (Diffie-Hellman), digital signature (DSA), and public-key algorithm (RSA) and bulk encryption (RC4) are called cipher-suite.

Secure Electronic Transaction (SET) is an open protocol standard for the commerce industry developed by Visa and MasterCard as a way to facilitate secure payment card transactions over the Internet[4]. SET doesn't really compete with SSL since SSL is focused on encrypting information communicated between two trusted parties. SET, on the other hand, uses digital certificates to help identify and establish trust between parties involved in a financial transaction as well as providing digital signatures for documentation. SET uses encryption and certification to help protect, identify and verify the parties involved in an online transaction: customers, merchants, processors and acquirers (banks).

The connection between the mobile device and gateway server is typically protected by Transport Layer Security (TLS) / Wireless TLS (WTLS). TLS is a IETF version of SSL, WTLS is a wireless version of TLS. Usually the mobile device connects to Internet through a gateway that translates between Internet and WAP gateway. Secure channels between the client and WAP gateway are supported by WTLS, while the channel between the WAP gateway and Internet server is supported by TLS.

NEED TO SPEEDING UP THE WEB TRANSACTION

Slow download times, the bane of an online shopper's existence, may be costing E-commerce merchants more than $4 billion in sales each year, according to a report by Zona Research[5] . The report The Need for Speed" found that more than one-third of web users may simply give up trying to buy an item over the Internet when frustrated with an online shopping experience. These frustrations could result in as much as $4.35 billion in US E-commerce sales being put at risk each year, the report found.

There are many ways to speedup the web transactions by introducing new technology, new algorithm, optimising the existing one etc. We have chosen to optimize the existing cryptography algorithm to increase speed. In this paper we have chosen to optimize the conventional algorithms by introducing the applications of elliptic curve.

CRYPTOGRAPHY FOR MOBILE COMMUNICATION

The security in mobile communications can be further enhanced using a variety of methods. Public-key cryptosystem implemented in traditional computer platform, however secure they are and good for fixed E-commerce, may not be suitable for mobile communication. Due to the resource constraints of mobile computing platforms, lightweight security mechanisms are needed for protecting M-commerce transactions.

Elliptic curve based cryptosystem (ECC)[6] is emerging as an attractive alternative to traditional public-key cryptosystems like RSA[10], DSA[7] and Diffie-Hellman[8].

ECC offers the same level of security with smaller key sizes resulting in faster computations, low power consumption, as well as memory and bandwidth savings which are very much suitable for constrained devices. For example, ECC uses just 160-bits to provide the same level of security where RSA / DSA uses 1024-bits.

Elliptic curves are used for several kind cryptosystems including key exchange protocols and digital signature algorithms[9]. The key exchange algorithm, Diffie-Hellman based on integer modulo is unpalatable for machines that need to participate in many keyed conversations with a large set of peers like mobile commerce transaction.

Elliptic curve version of this algorithm (ECDH) is more efficient than the integer modulo one. Integer

modulo DH takes 2674 msec and elliptic curve version takes only 372 msec for exchanging keys[10].

As we know that ECC, a next generation cryptosystem and is very much suitable for constrained devices. Bonesh has tested the effect of ECC in a Palm device[11], a hand held device to perform business transaction and the result is given here.

Algorithm	Time
512-bit RSA key generation	3.4 minutes
512-bit RSA sig. generation	7028 ms
512-bit RSA sig. verification	1376 ms (e=65535)
163-bit EC - DSA key generation	597 ms
163-bit EC – DSA sig. generation	776 ms
163-bit EC - DSA sig. verification	2448 ms

As the processor speeds increases and the number of Internet connected devices grows, potential attackers will hack more resources by attacking the cryptography algorithm used in secure communication. So to provide good security the key size has to be increased. Already 512-bit RSA is considered as insecure one and 1024-bit keys are used for general communication. (It requires approximately 20 minutes to generate keys on the Palm Pilot).

The TLS / SSL designers knew that RSA is computationally expensive and that web browsers tend to re connect many times to the web server. Speeding up the public-key operation in SSL still remains a very active area for research and development.

	ECC-160	RSA-1024	ECC-224	RSA-2048
Operations / Sec	271.3	114.3	195.5	17.8
Speedup	2. 4:1		11.1	

Measurements show that RSA computation consumes 20% to 58% of the time spent in web server[12]. Vipul gupta study says that using ECC reduces overall processing time at the server by 29% to 86%. Replacing RSA with ECC reduces the server's processing time for new SSL connection across the network[13].

The authority for ECC, Certicom, OpenSSL and Sun microsystem are actively participating in promoting the adoption of ECC into IETF standards[14]. Integrating ECC technology into OpenSSL, Apache, Netscape Security Service (NSS) and Mozilla. OpenSSL is used by Apache, the most widely used web server and other application including Lynx, Apple's Safety etc.

CONCLUSION

The areas of mobile computing and wireless networks have seen an explosive growth both in terms of the number of services provided and the types of technologies that have become available, provides more opportunities for doing business transactions, which is called as mobile E-commerce (M-commerce). The growth of M-commerce depends upon the way in which we provide the secure communication between the entities.

Though many cryptosystems and protocols are available, they are not suitable for constrained devices. Replacing the conventional public-key cryptosystem by ECC will increase the speed of web transactions from mobile device to the web server.

REFERENCES

1. www.wirelessweek.com - M-commerce Keeps On Growing,
2. Bruce Schneier, 1996. Applied Cryptography. John Wiley and Sons, Canada.
3. Frier, P.Karlton and P.Kocher, 1996. The SSL3.0 Protocol Version 3.0.
4. www.software.ibm.com/commerce/set/overview.html, June 1998
5. George DiGiacomo, 1999. E-commerce Sales At Risk Over Download Times Study.
6. ANSI X 9.62, 1999. Public Key cryptography fir the financial services industry–the Elliptic Curve Digital Signature Algorithm (ECDSA).
7. ElGamal, T., 1985. Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. IEEE Transactions on Information Theory, pp: 469-472.
8. Diffie, W., M. E. Hellman, 1976. New Directions in Cryptography. IEEE Transactions on Information Theory, 22: 644-654.
9. IEEE Standard specifications for Public-key cryptography, IEEE Standards 1363, IEEE Computer Society, 29, August 2000.
10. Richard Schroeppel, Hilarie Orman, Sean W. O'Malley and Oliver Spatscheck, 1995. Fast Key Exchange with Elliptic Curve Systems, LNCS. 963: 43-56.
11. Boneh, D. and N. Daswani, 1999. Elliptic Curve Cryptography and financial application using PalmPilot. Proceedings of Financial Cryptography '99, LNCS, Vol. 1648, Springer-Verlag, pp: 1-16
12. Vipul Gupta, Douglas Stebila, Sheueling Chang Shantz, 2004. Integrating Elliptic Curve Cryptography into the Web's Security Infrastructure. WWW 2004, pp: 402-403.
13. Vipul Gupta, Sumit Gupta Sheueling Chang and Douglas Stebila, 2002. Performance Analysis of Elliptic Curve Cryptography for SSL", Proceedings of the ACM workshop on Wireless security, pp: 87-94.
14. Gupta, V., S. Blake-Wilson, B. Moeller, C. Hawk and N. Bolyard, 2004. ECC Cipher suites for TLS. IETF Internet draft < draft-ietf-tls-ecc-07.txt>.