ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

Implementation of NTRU in Mobile Phones

S.Esther Sukila

Department of Mathematics, Bharath University, Chennai, Tamil Nadu, India

ABSTRACT: The recent implementation of NTRU in mobile phones [1] is highlighted in this paper.

I. INTRODUCTION

Security continues to be one of the biggest challenges facing developers. The need to build secure applications with secure information is critical for many businesses today. As applications once again evolve to smaller platforms that are constrained in regard to resources, consideration must be given to the robustness of the application - including its security - versus being too large or too bulky[2].

NTRU cryptosystem founded in 1996 by four mathematicians and cryptographers at Brown University provides security products for consumer, enterprise and embedded system markets. The company's public key cryptography technologies can be used to secure anything from a corporate network to digital content, from a wireless phone to a TV set. NTRU sells its technology to electronics, semi-conductor and wireless networking companies[5].

Today, NTRU announces NTRU Neo for Java, a developer toolkit - the first public-key security system designed for all wireless devices and applications. According to NTRU, up until now it has been impossible to secure Java-enabled wireless devices and applications in a practical manner, due to size and speed constraints[7].

NTRU states that Neo for Java is the smallest and fastest public key-based Java security product in the world. NTRU states that it is possible to running at speeds 100 times faster than legacy security systems. Additionally, they require only 1/50th of the footprint at roughly 5k. NTRU technology enables security on all Java-enabled wireless devices and applications. It is small enough to fit in space-constrained wireless environments like mobile phones and handhelds, yet as powerful as enterprise class security[1].

With many of the major handset manufactures having announced support for Java, a small-scale, robust security system is needed.

"With its new Neo Java offering, NTRU addresses two of the most important requirements for mass adoption of wireless applications and services --strong security and platform portability," said Warren Wilson, Wireless Practice director at Boston-based Summit Strategies. "Java specifically J2ME -- is rapidly becoming the de facto platform for mobile and wireless devices from smart phones to PDAs, and NTRU's high-performance, small-footprint encryption technology is well-suited to protect even the most sensitive information on these resource-constrained devices. Wireless carriers, device makers and application developers will all appreciate this combination of capabilities[2]. "

II. BENEFITS FROM NEO FOR JAVA

- Elimination of the historic trade-offs between performance and security, making it possible to deliver wireless applications and services that are both secure and fast.
- Practical and powerful public-key security never before possible in space-constrained wireless devices and applications. Brings powerful security for the first time to wireless devices and applications.
- Ability to develop secure, Java-based business and financial wireless applications such as wireless banking, payment and trading.
- Increased flexibility in their wireless designs. Service providers and operating system providers are enabled to deliver secure business and financial applications to their customers.

Neo for Java offers a fast, small public key cryptographic system the smallest in the world. Depending on the security, size and speed requirements, the implementation of the Neo for Java API into the wireless applications can be relatively easy.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

Today, mobile phones are considered to be the most common communication devices in history. The demand for such device is tremendous, as in, the second quarter of 2009, there were more than 4.3 billion mobile subscribers worldwide compared to 3 billion mobile subscribers in 2008 and 2.5 billion mobile subscribers in 2007 [1]. The majority of them are sending and receiving SMS texts, or making calls, it is sometimes used to exchange sensitive information between communicating parties[4]. In some cases however, this data may also include very private information reserved for the personal viewing of the legal recipient. Some mobile networks such as GSM networks use different security algorithms called A3, A5 and A8. An A3/A8 algorithm is implemented in the Subscriber Identity Module (SIM) cards and in the GSM network authentication centers[6]. The A5 encryption algorithm scrambles the user's voice and data traffic between the handset and the base station to provide privacy; the algorithm is implemented in both the handset and the base station subsystem (BSS). In September 2003, a group of researchers introduced a practical ciphertext-only cryptanalysis for GSM encrypted communication, and launched active attacks on the GSM protocols. They describe a ciphertext-only attack on A5/2 that merely requires a few dozen milliseconds of encrypted off-the-air cellular conversation to find the correct key in less than a second on a personal computer. It is clear that the transmitted data through the mobile networks is unsecured. GSM networks were not designed to transmit sensitive information. Therefore, security was not considered in its implementation. As the amount of products and services offered via the Internet grows rapidly, privacy, copyright and security are very important issues.

Nowadays, the visibility of security applications is wide; the term security, is presented in the scholar papers, side by side, with terms confidentiality, integrity, authenticity, non-repudiation, privacy and data protection. Researcher state many words on the role played by security on the life. They say "only protected transaction, have significant impact on consumers' perception about e-banking security. "Privacy and security are very important issues being discussed in the literature, on the current use of ICT". Public key cryptography is a proven solution, which can be used to secure mobile communications. The usage of public key cryptography can provide the confidentiality, authentication, integrity and non-repudiation security services needed to secure mobile communications. Due to the limitation of the mobile devices resources, implementing a public key cryptography solution to secure peer to peer communication has become a challenge.

In 2009, made an experiment on the performance of enhanced NTRU-251 and compared it with RSA-1024 in the mobile java emulator. The results of their experiment are shown in Table 1. The results that they got show that the time of key generation for NTRU is less 200 times that the time of key generation for RSA, and the time of encryption is almost 3 times less, and the time of decryption is about 30 times less. Thus NTRU is more reasonable for public key cryptography implementation on the mobile phone devices.

III. NTRU EXPERIMENT ON THE REAL MOBILE PHONE DEVICE

Unlike the papers reported in the literature, they used java emulator to test the performance of the algorithms; NTRU in the real mobile devices was tested. To test the NTRU speed four of the Nokia devices were selected; Nokia N70, N73, N93 and Nokia 5800 Xpress Music. The Nokia N70 belongs to the second generation (2G) of Nokia mobile devices and it operates with symbian operating system. It has ARM9 CPU with a 220 MHz clock rate. In addition, it has 22MB internal memory and supports extension memory from MMC type. Nokia N73 is from the third generation (3G) and operates with the developed version of symbian operating system, which is Symbian OS. This model has Dual ARM 9 CPU with 220 MHz clock rate. N73 has 42 MB internal memory and 2 GB Mini SD, as extended memory. Nokia N93 which belongs to the third generation (3G, has Dual ARM 11 CPU with 332 MHz clock rate. It also operates with the symbian operating system. This model has 50MB internal memory and 2 GB Mini SD as extended memory[9]. Finally, Nokia 5800 Xpress Music which is the most modern among them, belongs to the fifth generation (5G), and operates with the Symbian OS. This model has ARM 11 CPU with 434 MHz clock rate. It also has 81MB internal memory with 16GB Mini SD as extended memory.

We performed tests on key generation, encryption and decryption, as well as signing and verifying operations for one hundred times and then calculated the average of time required for each operation. The NTRU key strength is NTRU 251 which is equivalent to RSA 1024. Table 2 shows the key generation operation elapsed time on the real equipment. From the results, it is noticed that NTRU algorithm performed very well on the mobile devices and there were no negative effects on the mobile device's performance due to the small time required for the key generation[8].

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2015

The tests results of NTRU on real equipment such as Nokia N70, N73, N93 and Nokia 5800 Xpress Music showed that the mobile device was able to achieve this operation in less than one second. This is in comparison with one of the best SMS security solutions, who applied the PKI on the mobile phone environment by using the RSA algorithm. The solution tests were carried out on the mobile phone Nokia N95 (ARM 11 Dual CPU with 332MHz CPU Clock Rate) to generate RSA pair keys with 1024 bit key length. The elapsed time was around eighteen seconds[1]. In the test, Nokia N93, which has the same computing ability to Nokia N95, was used (that is, ARM 11 Dual CPU with 332MHz CPU Clock Rate). But the operation, generating NTRUEncrypt pair keys with length 251, which is equivalent in security level to RSA 1024, is done within 53 ms. This means that, the proposed solution is faster by about 340 times than Kuen's solution.

From the results above, note that NTRU does not require high computing ability, which makes it the best alternatives for mobile devices.

Table 1. Preliminary experimental results

Operation	NTRU-251 (ms)	RSA-1024 (ms)
Key generation	9617	2090509
Encryption	515	1505
Decryption	1132	35102

Table 2. NTRU pair keys generation operation test

Nokia N70 (ms)	Nokia N73 (ms)	Nokia N93 (ms)	Nokia 5800 Xpress Music (ms)
142	77	53	29

REFERENCES

(1). Zionts, S 1965, "Size reduction techniques of linear programming and their applications", Ph.D. Thesis, Carnegie Institute of Technology.
(2).Umanath K., Palanikumar K., Selvamani S.T., "Analysis of dry sliding wear behaviour of Al6061/SiC/Al2O 3 hybrid metal matrix composites", Composites Part B: Engineering, ISSN : 1359-8368, 53() (2013) pp. 159-168.
(3).Taha, HA 2006, Operations Research, An Introduction, 8th Edition, Pearson Prentice Hall, New Jersey.
(4)Tamilselvi N., Krishnamoorthy P., Dhamotharan R., Arumugam P., Sagadevan E., "Analysis of total phenols,total tannins and screening of phytocomponents in Indigoferaaspalathoides (ShivanarVembu) Vahl EX DC", Journal of Chemical and Pharmaceutical Research, ISSN : 0975 – 7384, 4(6) (2012) pp.3259-3262.
(5).Tomlin, LA and Welch, JS 1986, "Finding duplicate rows in a linear programming model", Operations Research Letters, vol. 5, no. 1, pp. 7-11.
(6)Rajasulochana P., Dhamotharan R., Murugakoothan P., Murugesan S., Krishnamoorthy P., "Biosynthesis and characterization of gold nanoparticles using the alga kappaphycusalvarezii", International Journal of Nanoscience, ISSN : 1793-5350, 9(5) (2010) pp.511-516.
(7)Sharmila S., Jeyanthi Rebecca L., Das M.P., Saduzzaman M., "Isolation and partial purification of protease from plant leaves", Journal of Chemical and Pharmaceutical Research, ISSN : 0975 – 7384, 4(8) (2012) PP. 3808-3812.
(8)Serane T.V., Zengeya S., Penford G., Cooke J., Khanna G., McGregor-Colman E., "Once daily dose gentamicin in neonates - Is our dosing correct?", ActaPaediatrica, International Journal of Paediatrics, ISSN : 0803-5326, 98(7) (2009) PP.110-1105
(9)S.H.Al-Bakri,SecuringPeer-to-Peer Mobile Communication Using Public Key Cryptosystem: New Security Strategy, International Journal of the Physical Sciences Vol. 6(4), February 2011, pp. 930-938