ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (346-350), Month: April - June 2015, Available at: www.researchpublish.com

Dependable Privacy Protection for End To End Gesture Recognition Based On Dynamic Key Changes

[1]M.Pradeepa, [2]J.Sangeethaguil, [3]P.Nivetha, [4]R.Karthika

Abstract: **A suitable key agreement protocol plays an essential role in protecting the communications over open channels among users using voice over Internet protocol (VoIP). This study presents a robust and flexible password authenticated key agreement protocol with user anonymity for session initiation protocol (SIP) used by VoIP communications. Security analysis demonstrates that the proposed protocol enjoys many unique properties, such as user anonymity, no password table, session key agreement, mutual authentication, password updating freely, conveniently revoking lost smartcards and so on. Furthermore, the proposed protocol can resist the replay attack, the impersonation attack, the stolen-verifier attack, the man-in-middle attack, the Denning-Sacco attack and the offline dictionary attack with or without smartcards. Finally, the performance analysis shows that the protocol is more suitable for practical application in comparison with other related protocols.**

Keywords: **Antennas, elliptic single complementary split-ring Resonator (ESCSRR), rectangular split-ring resonator (RSRR), ultra Wideband (UWB).**

I. INTRODUCTION

Voice over Internet protocol (VoIP)-based communication systems are undergoing rapid development and attract a great deal of attention. Protection of personal communication information is one of the most important issues in VoIP communications over public channels. But the designers of VoIP communications systems mainly focus on a good level of quality of service and pay little attention to security problems. Owing to these reasons, exposed to the unsecured Internet,which incurs various possible attacks. Long distance calling with Skype is one of the most popular applications of VoIP communications, and VoIP calls are more likely to be threatened by attacks compared with conventional telephone calls with public switched telephone network.

With the widespread applications of VoIP, session initiation protocol (SIP) is receiving a lot of attention. SIP was proposed by Internet Engineering Task Force Network Working Group in 1999 [1]. Now, it is widely used as a text based signalling protocol for VoIP. The architecture of SIP contains five main components: proxy server, redirect server, user agent, register server and location server.

Compared with other signalling protocols such as H.323, SIP is more flexible and lightweight. However, the authentication of SIP is vulnerable to several types of security threats and attacks since it is inherited from HTTP Digest authentication. Most security requirements, such as confidentiality, integrity, authenticity and privacy, can be addressed by building an authentication key agreement protocol. In order to achieve a comparable level of network security with PSTN, an efficient authentication key agreement should be provided to realise the security requirements mentioned above.

The security requirements of an authentication protocol for SIP can be summarised as follows: (i) resistance to password guessing attacks, stolen-verifier attacks and server-spoofing attacks; (ii) mutual authentication and session key(iii) providing user anonymity, that is, the real identity of the user should be kept anonymity from any third party to protect the privacy of the user; (iv) security in updating passwords; (v) perfect forward secrecy and known-key security; (vi) resistance to replay attacks, man-in-middle attacks, modification attacks and Denning-Sacco attacks and (vii) resistance to offline dictionary attacks with/without smartcards.

Since original SIP authentication mechanisms could not protect privacy and valuable information over voice communications, several new authentication key agreement protocols have been proposed to provide strong security protection for prevalent VoIP services. As VoIP communication is more sensitive to transmission latency, providing a suitable key agreement protocol for SIP should not only meet security demands but also satisfy the requirement of transmission latency. The main objective of our study is to address these problems by constructing a robust and efficient authenticated key agreement protocol that provides strong security protection for SIP without sacrificing the quality of real-time VoIP communication.

The rest of this paper is organised as follows: Section 2 describes related work. Preliminaries are reviewed in Section 3. Section 4 presents our authenticated key agreement protocol.

II. RELATED WORK

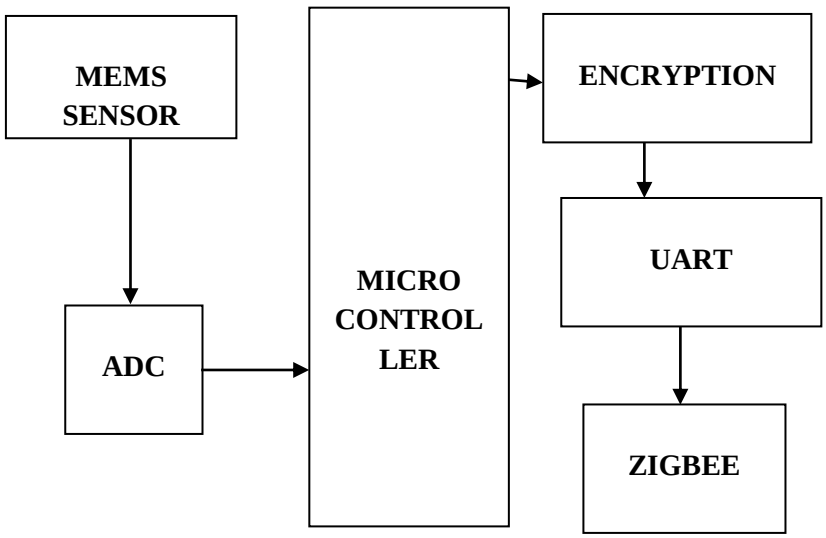
Developing a secure user authentication protocol is a critical issue in SIP-based communication services. To date, several protocols have been suggested to seek ways of strengthening the security of SIP authentication process. The original authentication protocol for SIP was based on hypertext transport protocol (HTTP) digest authentication, which offers one-way authentication, but cannot support integrity and confidentiality protection. So, the original authentication protocol was not good enough for providing acceptable security level in practice.

Several authenticated key agreement protocols have been proposed in order to strengthen the security of SIP. In 2005, Yang et al. [3] found that the original SIP authentication

protocol incurred off-line password guessing attacks and server-spoofing attacks; they constructed a Diffie–Hellman key exchange-based SIP authentication scheme to solve the problems. But their protocol required the server storing apassword table for verification purposes and involved expensive exponential computation which is not practical for SIP. Huang et al. [4] later claimed that Yang's protocol suffered two weaknesses when applied to SIP. One was vulnerable to off-line password-guessing attacks and the other was requiring the execution of expensive exponential operations. So Yang's protocol was not suitable for low computational power devices. With these points in mind, Huang proposed a new authentication scheme for SIP.Unfortunately, in Jo et al. [5] discussed the cryptanalysis Yang's and Huang's authentication protocols and demonstrated that both protocols were vulnerable to off-line password guessing attacks. To avoid the requirement of large public key infrastructure (PKI), identity-based cryptography was employed by Ring et al. [6] to construct an authenticated key agreement for SIP. . In addition, protocol also provides some unique features such as user anonymity, no password table needed, revoking lost smartcard conveniently and password updating freely. Data encryption and data decryption is the process undertaken in this protocol.

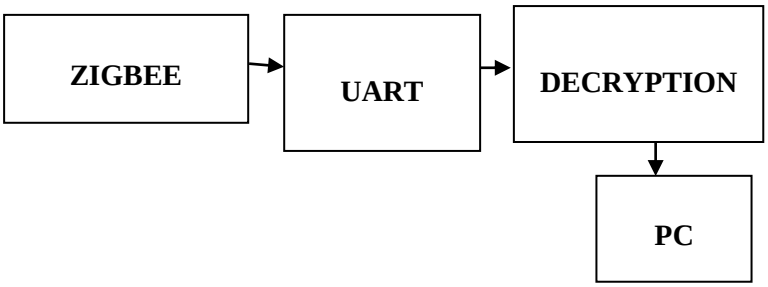
III. BLOCK DIAGRAM

TRANSMITTER DIAGRAM:



ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (346-350), Month: April - June 2015, Available at: www.researchpublish.com

RECEIVER DIAGRAM:



IV. BLOCK DIAGRAM DESCRIPTION

AT89S52:

The AT89S52 is a low-power, high-performance CMOS 8-bit microcontroller with 8K bytes of in-system programmable Flash memory. The device is manufactured using Atmel's high-density non volatile memory technology and is compatible with the standard 80C51 instruction set and pin out. The on- hip Flash allows the program memory to be reprogrammed c in-system or by a conventional non volati**le** memory pro-grammars**.** By coming a versatile 8-bit CPU with in-system programmable Flash on a monolithic chip, the Atmel AT89S52 is a powerful microcontroller which provides a highly-flexible and cost-effective solution to many embedded control applications. The AT89S52 provides the following standard features: 8K bytes of Flash, 256 bytes of RAM, 32 I/O lines, Watchdog timer, two data pointers, three 16-bit timer/counters, a six-vector two-level interrupt architecture, a full duplex serial port, on-chip oscillator, and clock circuitry. In addition, the AT89S52 is designed with static logic for operation down to zero frequency and supports two software selectable power saving modes. The Idle Mode stops the CPU while allowing the RAM, timer/counters, serial port, and interrupt system to continue functioning.

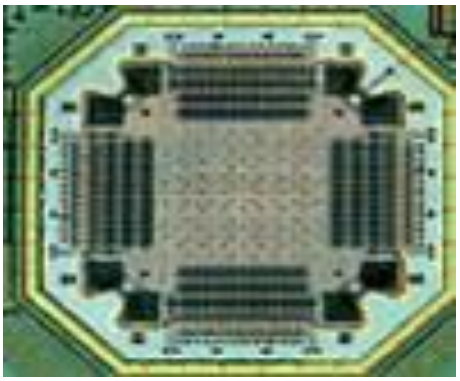
The Power-down mode saves the RAM con-tents but freezes the oscillator, disabling all other chip functions until the next interrupt or hardware reset.

ADC DESCRIPTION:

The ADC0809 data acquisition component is a monolithic CMOS device with an 8-bit analog-to-digital converter, 8-channel multiplexer and microprocessor compatible control logic. The 8-bit A/D converter uses successive approximation as the conversion technique**.**

The converter features a high impedance chopper stabilized comparator, a 256R voltage divider with analog switch tree and a successive approximation register. The 8-channel multiplexer can directly access any of 8-single-ended analog signals**.** The device eliminates the need for external zero and full-scale adjustments. Easy interfacing to microprocessors is provided by the latched and decoded multiplexer address inputs and latched TTL TRI-STATE® outputs. The design of the ADC0808, ADC0809 has been optimized by incorporating the most desirable aspects of several A/D conversion techniques. The ADC0808, ADC0809 offers high speed, high accuracy, minimal temperature dependence, excellent long-term accuracy and repeatability, and consumes minimal power**.** These features make this device ideally suited to applications from process and machine control to consumer and automotive applications. For 16-channel multiplexer with common output (sample/hold port) see ADC0816 data sheet.

MEMS SENSOR:



Micro-electromechanical systems (MEMS) incorporate miniature electro-mechanical components fabricated with processing techniques and equipment originally developed in the semiconductor industry.

Combining traditional silicon processing techniques, bonding technologies and a number of non-traditional processing techniques, MEMS are being developed for a variety of applications.

While existing MEMS sensors and actuators have enabled automotive crash sensors, ink jet printer nozzles and catheter tip pressure sensors, new market opportunities for MEMS technology abound in the telecommunication, biomedical, semiconductor, and aerospace industries.

URAT:

An UART, universal asynchronous receiver / transmitter is responsible for performing the main task in serial communications with computers.

The device changes incoming parallel information to serial data which can be sent on a communication line. A second UART can be used to receive the information. The UART performs all the tasks, timing, parity checking, etc. needed for the communication. The only extra devices attached are line driver chips capable of transforming the TTL level signals to line voltages and vice versa. Basically uart contributes of two components viz

- Max232 ic.
- Rs232 serial cable**.**

WSN:

WSN is the set of specs built around the IEEE 802.15.4 wireless protocol. The IEEE is the *Institute of Electrical and Electronics Engineers*, a non-profit organization dedicated to furthering technology involving electronics and electronic

The 802 group is the section of the IEEE involved in network operations andtechnologies, including mid-sized networks and local networks. Group 15 deals specifically with wireless networking technologies, and includes the now ubiquitous 802.15.1 working group, which is also known as Bluetooth®. The standard itself is regulated by a group known as the WSN Alliance, with over 150 members worldwide .One WSN network can contain more than 65,000 nodes (active devices). The network they form in cooperation with each other may take the shape of a star, a branching tree or a net (mesh). What's more, each device can operate for years off of a AA cell. That means that each nodes little power.

V. REQUIREMENTS

Hardware Requirements:

- MICROCONTROLLER
- MEMS SENSOR
- UART
- WSN
- ADC
- LCD

Software Requirements:

- KEIL COMPLIER
- EMBEDDED C

VI. ADVANTAGES

This Protocol can resist offline dictionary attacks without smartcards

This protocol can resist replay attacks

Advantage of Encryption is that it keeps data from snoopers without compromising systems or storage devices

This protocol can resist stolen-verifier attacks

VII. FUTURE ENHANCEMENT

- The vast growths in mobile and wireless applications would contain lacks of using suitable security concepts during the development process which worries the information security research community.
- This paper reviews most of the encryption techniques which adopt chaos based cryptography, and illustrates the used of chaos based voice encryption techniques in wireless communication as well.
- The review in this paper summarized the traditional and modern techniques of voice/speech encryption and demonstrated the feasibility of adopting chaos based cryptography for in wireless communications

VIII. CONCLUSION

A new password authenticated key agreement protocol with user anonymity for SIP has been proposed in this paper. In our protocol, the user and the server can achieve mutual authentication and key agreement by using passwords and smartcards. Meanwhile, our protocol can withstand replay attacks, impersonation attacks, stolen-verifier attacks, man-in-middle attacks, Denning-Sacco attacks and offline dictionary attacks with or without smartcard. In addition, our protocol also provides some unique features such as user anonymity, no password table needed, revoking lost smartcard conveniently and password updating freely. These new features have not been considered in other related work, but they are very important in implementing a practical and universal authenticated key agreement for SIP.

REFERENCES

[1] Rosenberg, J., Schulzrinne, H., Camarillo, G.: 'SIP: session initiation protocol'. RFC 3261, June 2002

[2] Wang, C.-H., Liu, Y.-S.: 'A dependable privacy protection for end-to-end VoIP via elliptic-curve Diffie-Hellan and dynamic key changes', J. Netw. Comput. Appl., 2011, 34, pp. 1545–1556

[3] Yang, C., Wang, R., Liu, W.: 'Secure authentication scheme for session initiation protocol', Comput. Secur., 2005, 24, pp. 381–386

[4] Huang, H., Wei, W., Brown, G.: 'A new efficient authentication scheme for session initiation protocol'. Proc. JCIS 06, Kaohsiung, Taiwan, ROC, October 2006

[5] Jo, H., Lee, Y., Kim, M., Kim, S.,Won, D.: 'Off-line password-guessing attack to Yang's and Huang's authentication schemes for session initiation protocol'. Proc. INC, IMS and IDC, Seoul, Korea, August 2009, pp. 618–621

[6] Ring, J., Choo, K.-K.R., Foo, E., Looi, M.: 'A new authentication mechanism and key agreement protocol for sip using identity-based cryptography'. Proc. AusCERT R&D Stream, Gold Coast, Australia, May 2006, pp. 61–72

Details About Authors: We are studying final year

ECE in Ponnaiyah Ramajayam College of Engg.& Tech, Vallam, Thanjavur.