Securing Communication in Ambient Networks for Speech Therapy Systems

Mihai Horia ZAHARIA
Technical University "Gh. Asachi" Iasi
Bd-ul D. Mangeron, no. 53 A, RO-700050, Iasi
mike@cs.tuiasi.ro

***Abstract*—In this paper the problem of securing mobile devices used in ambient networks for speech therapy is presented. The main target consists in making various mobile devices involved in speech therapy to maintain both the confidentiality of personal data of the patient and also to avoid interference when simultaneous communicate with the control center. Due to non-technical type of user all password management will be made automatic by the control system. As result the mobile device will have a user transparent security layer added. The problem of people from isolated community treatment is also solved by this approach.**

***Index Terms*—communication system security, distributed computing, microcontrollers**

I. INTRODUCTION

Usually the transient nature of device-interaction in pervasive or mobile systems leads to a series of problem like establishing the target system into a noisy environment. The noisy term refers both to natural and artificial electrical noise and also to the other devices that simultaneous transmits and receives information.

As we know privacy-sensitive information in the context of mobile devices computing environment falls into two categories each of which require qualitatively different approaches to deal with the privacy problem.

There is privacy of personal data that originates in digital form and is explicitly exchanged: this applies to sensitive, personal, digital information owned by the user (credentials, personal data, voice-transcripts, etc.) and is exchanged with the infrastructure based on informed consent and a mutually agreed upon, privacy policy. Typical solutions require decentralized architectures based upon privacy tags that are carried along with sensitive data.

Also we have privacy of sensed information: e.g. sensitive, personal information that is user transparent retrieved by the surrounding infrastructure. Here, the user has no opportunity to conditionally release information based upon an agreed-upon privacy policy. Information gathered by any surveillance technologies and sensor networks are from this category. Such information can also be gathered by exploiting covert channels in the computing device or communication channel (especially wireless) that leak information.

This category includes other types of profiling information that is also retrieved by the infrastructure, e.g. buying patterns, mobility patterns, etc. Preserving the privacy of this type of information requires that safeguards be built into the computing, communications and storage infrastructure.

In this particular case we do not use internet enabled device for handling the patient treatment but this devices will have a wireless based connection with the main centre located at the speech therapist base. As result the patient identification data and the status of their progress and new treatment schemes will be exchanged on the link. So it will be very easy for a hacker with an adequate wireless receptor and a sniffer base application to intercept and even worst to emulate the patient terminal. As result a minimal security layer is required for the mobile device.

II. AMBIENT NETWORKS

In the rapidly evolving communications market a new challenging problem named fixed–mobile convergence appears. This refers at the trend in convergence of services and networks. This term is used by the telecommunications industry to describe the integration of wire line and wireless access technologies in a common services world.

Although this convergence can be viewed from different points of view like:

- user services convergence,
- device convergence,
- network convergence
- and business convergence.

In Figure 1 the industry way of seeing convergence is presented.

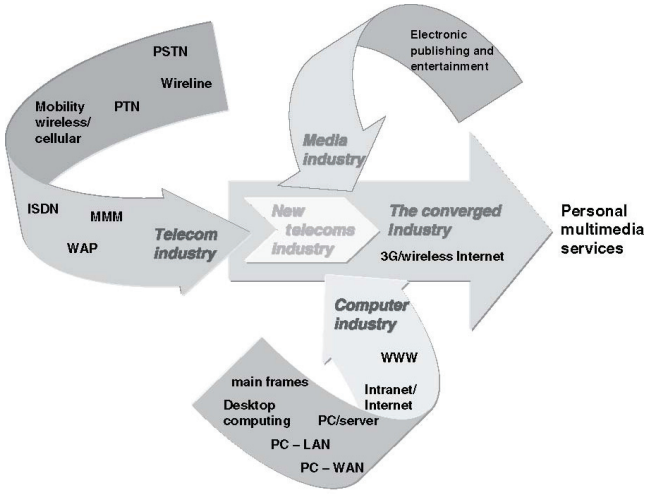

Figure 1. Industry transformation and convergence

Digital Object Identifier 10.4316/AECE.2007.02010

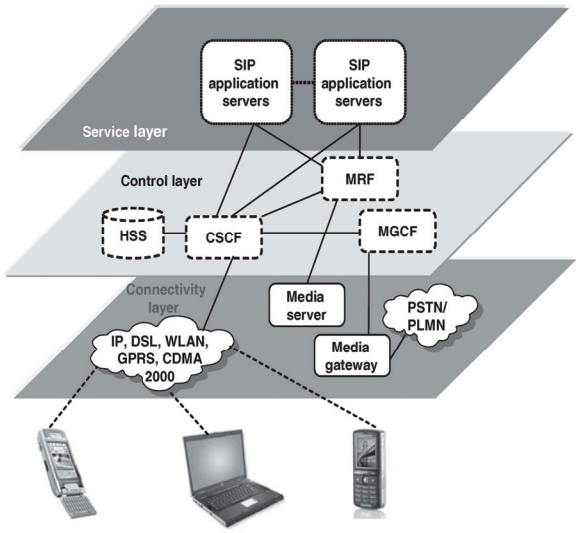

Figure 2. Simplified view of the layered architecture in IMS

As can be seen from Figure 2, IP Multimedia Subsystem (IMS) provides an open, standardized way of using horizontal, layered network architecture.

The application layer comprises application and content servers to execute value-added services for the user.

The control layer comprises network control servers for managing call or session set-up, modification and release.

The connectivity layer comprises routers and switches, both for the backbone and for the access network.

The horizontal architecture in IMS also specifies interoperability and roaming, and provides bearer control, charging and security.

III. THE SPEECH THERAPY SYSTEM

This consists from a combination from an artificial intelligent module, a typical data base system, a 3D graphic interface and a mobile device as is presented in Figure 3.

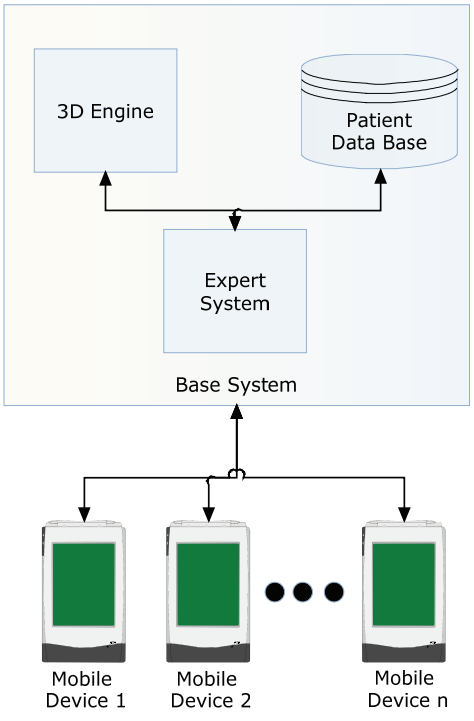

Figure 3. Speech Therapy system

The expert system is based on CLIPS inference engine libraries. In this case the system must implement a series of exercises based on speech therapist specifications. Because there are some similitudes between rules the resulted structure was relatively simple. There are 9 types of generic exercises that can be particularized for each 34 exercises corresponding to each sound. As result there are 748 combinations that will lead to the same number of distinct exercises. The associated texts are stored in .RTF format in order to preserve Romanian language diacritics specification and at the program level from the same reason the Unicode string types are used.

The 3D Graphic interface is very complex and has the role of teaching the patient how to move their muscles at the laryngeal levels in order to begin to correct articulate the words with problem. Those movements are synchronized with sound based stimulus. The database system helps the therapist to maintain order into patients' treatment schemes. The data base will store the already done treatments and in combinations with the expert system will propose some variants of exercises to be done at home by the patient. This type of therapy is mainly based by home working exercises. As result the mobile device became very important.

To maintain link with any mobile device an ad-hoc network will be created between the main system and the mobile device.

The design of this device must have low costs lower that a usual PDA to be used by any social classes but also to have enough complexity to store the weekly exercise parameters and sound, to control the patient evolution by making real time speech recognition and demand continuous repetitions of involved words as the therapeutic schemes desire.

At the end of the week cycle the patient come back at the main center where his results are automatically download into the main system and with help of specialist and of the expert system a new treatment scheme will be selected and will replace the older one. As result at the moment at the therapist base can be as many child come back as many mobile devices that try to find the main system and to communicate with him.

Now became clear that some measure of unique identification of the mobile device, secure communication problems must be taking into account.

This system must be designed to have an adapter layer in order to be integrated into the ambient networks. As result the child mobility will be increased. A typical mobile client for this type of network has enough power to run all needed applications.

Perhaps the most important advantage driven by this approach will be the on line diagnoses of the child using videoconference and on line upload a download results and the new battery of tests. This will be especially for the isolated community that can not afford to make all day long trips to the near city.

IV. SECURITY LAYER

The real time speech recognition will require a powerful microcontroller to be installed in the mobile device. As result there is enough available computing power to use any type of security is required.

The problem of unique identifier is implicit solved by MAC existence at the wireless adapter level. So the system will associate the patient data with the assigned mobile device. When main database is initialized, a pair of keys public and private will be generate and a password too. When a new patient is added he will receive a personal password for securing the communication. In fact we construct a digital passport for the device. This is needed because the communication will be secured using a Feistel based cipher. Because the information not require higher levels of protection even a DES or XDES system can be used to encrypt communication.

DES is a Feistel cipher algorithm that uses a 56-bit key to code a 64-bit information block. Usual key length is 64 bits because of supplementary checksum bits. From mathematical analyze result that this algorithm have space keys dimension at 2^{64}.

Encryption proceeds in 16 stages or rounds. From the input key K sixteen 48-bit subkeys K_i are generated, one for each round. Within each round, 8 fixed, carefully selected 6-to-4 substitution mappings (S-boxes) S_i are used. The 64 plain text is divided in 32-bits halves L_0 and R_0. Each round is functionally equivalent, taking 32-bit inputs L_{i-1} and R_{i-1} from the previous round and producing 32-bit outputs L_i and R_i for $1 \le i \le 16$ as follows:

$$L_i = R_{i-1};$$
$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i), \quad (1)$$
where $f(R_{i-1}, K_i) = P(S(E(R_{i-1}) \oplus K_i))$;

A form of function *f* is presented in Figure 4. Here E is a fixed expansion permutation mapping R_{i-1} from 32 to 48 bits and P is another fixed permutation on 32 bits. Decryption process involves the same key and algorithm, but with subkeys applied to the internal rounds in the reverse order.

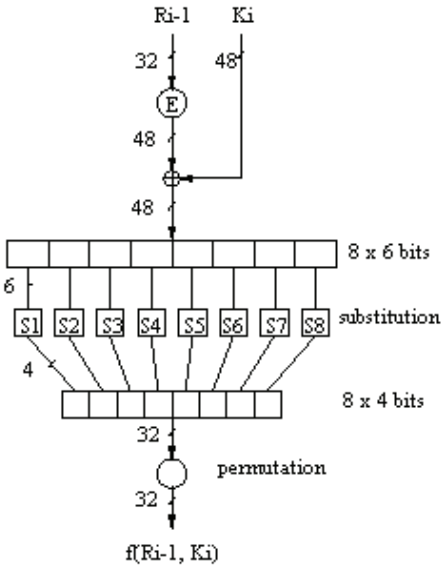

Figure 4. DES function *f*

A simplified view is that right half of each round (after expanding the 32-bit input to 8 characters of 6 bits each) carries out a key-dependent substitution on each of 8 characters, then uses a fixed bit transposition to redistribute the bits of resulting characters to produce 32 output bits.

As result most of the previously mentioned problems will disappear. To strengthen the security each time patient come back to the specialist a new random password will be generated and the undated both in the system data base and in mobile device local storage.

It is clear that all confidential information reside on main system must be stored using an cryptographic algorithm that have as key one derived from the system administrator password. Because that information has not frequently accesses and also little dimensions AES is recommended to be used in the system. We use the Rijndael's key schedule is done as follows:

The first **n** bytes of the expanded key are simply the encryption key.

The rcon iteration value **i** is set to 1

Until we have **b** bytes of expanded key, we do the following to generate **n** more bytes of expanded key:

- do the following to create 4 bytes of expanded key:

create a 4-byte temporary variable, **t**

assign the value of the previous four bytes in the expanded key to **t**

perform the key schedule core (see above) on **t**, with **i** as the rcon iteration value

increment **i** by 1

exclusive-or **t** with the four-byte block **n** bytes before the new expanded key.

- then do the following three times:

assign the value of the previous 4 bytes in the expanded key to t

exclusive-or t with the four-byte block n bytes

- If we are generating a 256-bit key, we do the following to generate the next 4 bytes of expanded key:

assign the value of the previous 4 bytes in the expanded key to t

run each of the 4 bytes in t through Rijndael's S-box

exclusive-or t with the 4-byte block 32 bytes before the new expanded key.

- If we are generating a 128-bit key, we do not perform the following steps. If we are generating a 192-bit key, we run the following steps twice. If we are generating a 256-bit key, we run the following steps three times:

assign the value of the previous 4 bytes in the expanded key to t

exclusive-or t with the four-byte block n bytes before the new expanded key.

Step three is repeated until at least **b** bytes of expanded key are generated

As result the security level is enough to fulfill all the system requirements.

Another possibility to this approach is to use directly the WPA or WPA2 on the chip. This is suitable if the mobile device has own operating system an easy support the load of require drivers, otherwise, which is our case the proposed solution is the cheapest from the implementation point of view.

V. CONCLUSION

The proposed security system solve typical problems related both to trustworthy pervasive and mobile computing. Of course in the analyzed case a very powerful security it is not needed due to the intrinsic system nature. The speech therapy system have many problems concerning the artificial intelligence component involved at the main system level and usually neglect this aspect that can concern at some levels the patient confidentiality. So the proposed system will solve the typical problem for the this type of systems.

REFERENCES

[1] A. Czyzewski, H. Skarzynski Et All, *Therapy System And Device For Speech Articulation*, http://www.wipo.int/pctdb/en/wo.jsp?wo=2002039423.

[2] A. Menzenes, P. van der Orschot and S. Vanstone, "Handbook of Applied Cryptography", CRC Press, 1996

[3] K. Ranganathan (2004), *Trustworthy Pervasive Computing: The Hard Security Problems*, Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops (PERCOMW'04).

[4] N. Niebert, A. Schieder, et all, eds. Ambient Networks, co-operative mobile networking for the wireless world, John Wiley & Sons Ltd, West Sussex, England, 2007

[5] V. Raghunathan, T. Pering, et all (2004), *Experience With A Low Power Wireless Mobile Computing Platform*, in Proceedings of the 2004 International Symposium on Low Power Electronics and Design (ISLPED'04), ppg 363-368.

[6] V. Sacramento, M. Endler, et all (2004), *MoCA: A Middleware for Developing Collaborative Applications for Mobile Users*, IEEE DISTRIBUTED SYSTEMS ONLINE 1541-4922 © 2004 Published by the IEEE Computer Society Vol. 5, No. 10, ppg 1-14.

[7] Z. Wang, S. K. Das, H.Che, and M. Kumar (2004), *A Scalable Asynchronous Cache Consistency Scheme (SACCS) for Mobile Environments*, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 15, NO. 11, ppg. 983 – 995.

[8] ***, http://www.rsasecurity.com/