ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

RFID and Finger Print Based Security System

K.Syam Prasad
M.Tech Student
Department of Electronics & Communication Engineering,
Priyadarshini Institute of Technology & Sciences, Tenali.

SK.Sahir
Associate Professor,
Department of Electronics & Communication Engineering,
Priyadarshini Institute of Technology & Sciences, Tenali.

Abstract

Recently, in 2014, He and Wang proposed a robust and efficient multi-server authentication scheme using biometrics-based smart card and elliptic curve cryptography(ECC). In this paper, we first analyze He–Wang's scheme and show that their scheme is vulnerable to a known session specific temporary information attack and impersonation attack. In addition, we show that their scheme does not provide strong user's anonymity. Furthermore, He–Wang's scheme cannot provide the user revocation facility when the smart card is lost/stolen or user's authentication parameter is revealed. Apart from these, He–Wang's scheme has some design flaws, such as wrong password login and its consequences, and wrong password update during password change phase. We then propose a new secure multi-server authentication protocol using biometric-based smart card and ECC with more security functionalities. Using the Burrows Abadi Needham logic, we show that our scheme provides secure authentication.

In addition, we simulate our scheme for the formal security verification using the widely accepted and used automated validation of Internet security protocols and applications tool, and show that our scheme is secure against passive and active attacks. Our scheme provides high security along with low communication cost, computational cost, and variety of security features. As a result, our scheme is very suitable for battery-limited mobile devices as compared with He–Wang's scheme.

Keywords—components; Zigbee, Max232, keypad, Arm board, finger print ,smartcard reader.

Introduction

Embedded systems are electronic devices that incorporate microprocessors with in Their implementations. The main purposes of the microprocessors are to simplify the system design and provide flexibility. Having a microprocessor in the device means that removing the bugs, making modifications, or adding new features are only matters of rewriting the software that controls the device. Or in other words embedded computer systems are electronic systems that include a microcomputer to perform a specific dedicated application. The computer is hidden inside these products. Embedded systems are ubiquitous. Every week millions of tiny computer chips come pouring out of factories finding their way into our everyday products.

Embedded systems are self-contained programs that are embedded within a piece of hardware. Whereas a regular computer has many different applications and software that can be applied to various tasks, embedded systems are usually set to a specific task that cannot be altered without physically manipulating the circuitry. Another way to think of an embedded system is as a computer system that is created with optimal efficiency, thereby allowing it to complete specific functions as quickly as possible. Embedded systems designers usually have a significant grasp of hardware technologies. They used specific programming languages and software to develop embedded systems and manipulate the equipment. When searching online, companies offer embedded systems development kits and other embedded systems tools for use by engineers and businesses.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Embedded systems technologies are usually fairly expensive due to the necessary development time and built in efficiencies, but they are also highly valued in specific industries. Smaller businesses may wish to hire a consultant to determine what sort of embedded systems will add value to your organization. An embedded system is a system which is going to do a predefined specified task is the embedded system and is even defined as combination of both software and hardware. A general-purpose definition of embedded systems is that they are devices used to control, monitor or assist the operation of equipment, machinery or plant. "Embedded" reflects the fact that they are an integral part of the system. At the other extreme a general-purpose computer may be used to control the operation of a large complex processing plant, and its presence will be obvious.

The enlargement of micro technology has many Features like size, efficiency and capital. For a large scale device micro fabrication is used because of its smallness, applicability and lessening of material utilization. Micro technology and electronics have great scope of innovation. MEMS can be mounted on the ARM Lpc microcontroller wirelessly. A is the microcontroller proposed in this methodology which has inbuilt ADC conversion. By using MEMS many succession of external components can be eliminated. “Gaining data, storage of data, data filtering, statement interfacing and networking ”are included hence it is called elegant included MEMS. MEMS equipment not only makes the utensils much lesser but also makes them much improved. The chief inspiration for this investigation is to make the human-robot interface more flexible and simpler for the user. static and of low fidelity, with accommodation solely the result of the form and placement of furniture and fixtures. Smart homes aim to extend awareness, increase control over systems, and enhance the security, healthfulness, and safety of the environment through sensing, inference, communication technologies, decision-making algorithms, and appliance control.

However, the real-time processing of occupant activity has historically been costly in terms of computing and Memory requirements and often relies on technologies considered intrusive of people’s privacy (e.g., cameras). As a result, these efforts have focused on systems associated with the built environment such as the design and placement of furniture and fixtures. Practical occupant sensing in smart homes remains of low fidelity including such ON/OFF sensor activations as room changes, door openings/closings, appliance actuations, etc.

A logical progression for the use of high fidelity sensing maybe seen in its central importance to assistive robotics. As Green and Walker describe , the notion of assistive robotics frequently conjures images of a self-contained *humanoid servant* in which all robotic and intelligence challenges have been addressed. Finding this to be an unlikely possibility in the near term and seeking to move beyond the conventional *static* smart home, we envision an environment containing robotic components that take advantage of the capabilities and higher level thinking of the user to operate in a collaborative manner; working *with* rather than *for* the user.

The authors’ past investigations into possible forms and use models for assistive robotics have considered appliances such as a hospital over-the-bed table, continuum surfaces, and intelligent storage for personal items.

Ease of use

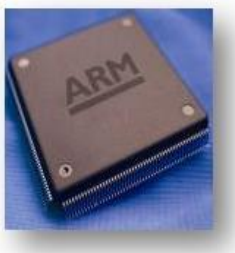
An embedded system is a system which is going to do a predefined specified task is the embedded system and is even defined as combination of both software and hardware. A general-purpose definition of embedded systems is that they are devices used to control, monitor or assist the operation of equipment, machinery or plant. "Embedded" reflects the fact that they are an integral part of the system. At the other extreme a general-purpose computer may be used to control the operation of a large complex processing plant, and its presence will be obvious. All embedded systems are including computers or microprocessors. Some of these computers

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

are however very simple systems as compared with a personal computer. The very simplest embedded systems are capable of performing only a single function or set of functions to meet a single predetermined purpose. In more complex systems an application program that enables the embedded system to be used for a particular purpose in a specific application determines the functioning of the embedded system. The ability to have programs means that the same embedded system can be used for a variety of different purposes. In some cases a microprocessor may be designed in such a way that application software for a particular purpose can be added to the basic software in a second process, after which it is not possible to make further changes. The applications software on such processors is sometimes referred to as firmware.

Arm processor review:

ARM stands for Advanced RISC Machines. It is a 32 bit processor core, used for high end application. It is widely used in Advanced Robotic Applications. It performs number of instruction in a single cycle compare with other controllers it have advanced features. The Arm CPU with real-time emulation and embedded trace support, that combine microcontroller with embedded high speed flash memory ranging from 32 kB to 512 kB. A 128-bit wide memory interface and a unique accelerator architecture enable 32-bit code execution at the maximum clock rate. For critical code size applications, the alternative 16-bit Thumb mode reduces code by more than 30 % with minimal performance penalty. Due to their tiny size and low power consumption, LPC2141/42/44/46/48 are ideal for applications where miniaturization is a key requirement, such as access control and point-of-sale. Serial communications interfaces ranging from a USB 2.0 Full-speed device, multiple UARTs, SPI, SSP to I2C-bus and on-chip SRAM of 8 kB up to 40 kB, make these devices very well suited for communication gateways and protocol converters, soft modems, voice recognition and low end imaging, providing both large buffer size and high processing power.



History and Development:

- ARM was developed at Acron Computers ltd of Cambridge, England between 1983 and 1985.
- RISC concept was introduced in 1980 at Stanford and Berkley.
- ARM ltd was found in 1990.
- ARM cores are licensed to partners so as to develop and fabricate new microcontrollers around same processor cores.

Key features:

1. 16-bit/32-bit ARM7TDMI-S microcontroller in a tiny LQFP64 package.
2. 8 kB to 40 kB of on-chip static RAM and 32 kB to 512 kB of on-chip flash memory.
   128-bit wide interface/accelerator enables high-speed 60 MHz operation.
3. In- System Programming/In-Application programming (ISP/IAP) via on-chip boot loader software. Single flash sector or full chip erase in 400 ms and programming of
   256 bytes in 1 ms.

Historical Background

The invention of the transistor at Bell Telephone Laboratories in 1947 sparked a fast-growing microelectronic technology. Jack Kilby of Texas Instruments built the first integrated circuit (IC) in 1958 using germanium (Ge) devices. It consisted of one transistor, three resistors, and one capacitor. The IC was implemented on a sliver of Ge that was glued on a glass slide. Later that same year Robert Noyce of Fairchild Semiconductor announced the development of a planar double-diffused Si IC. The complete transition

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

from the original Ge transistors with grown and alloyed junctions to silicon (Si) planar double-diffused devices took about 10 years. The success of Si as an electronic material was due partly to its wide availability from silicon dioxide (SiO2) (sand), resulting in potentially lower material costs relative to other semiconductors.

Zigbee

ZigBee is a specification for a suite of high level communication protocols using small, low-power digital radios based on the IEEE 802.15.4-2003 standard for wireless personal area networks (WPANs), such as wireless headphones connecting with cell phones via short-range radio. The technology defined by the ZigBee specification is intended to be simpler and less expensive than other WPANs, such as Bluetooth. ZigBee is targeted at radio-frequency (RF) applications that require a low data rate, long battery life, and secure networking.

A. Overview

ZigBee is a low-cost, low-power, wireless mesh networking proprietary standard. The low cost allows the technology to be widely deployed in wireless control and monitoring applications, the low power-usage allows longer life with smaller batteries, and the mesh networking provides high reliability and larger range.

ZigBee is a low-cost, low-power, wireless mesh networking proprietary standard. The low cost allows the technology to be widely deployed in wireless control and monitoring applications, the low power-usage allows longer life with smaller batteries, and the mesh networking provides high reliability and larger range

The ZigBee Alliance, the standards body that defines ZigBee, also publishes application profiles that allow multiple OEM vendors to create interoperable products. The current list of application profiles either published or in the works are:

- Home Automation
- ZigBee Smart Energy
- Commercial Building Automation
- Telecommunication Applications
- Personal, Home, and Hospital Care
- Toys

The relationship between IEEE 802.15.4 and ZigBee is similar to that between IEEE 802.11 and the Wi-Fi Alliance. The ZigBee 1.0 specification was ratified on 14 December 2004 and is available to members of the ZigBee Alliance. Most recently, the ZigBee 2007 specification was posted on 30 October 2007. The first ZigBee Application Profile, Home Automation, was announced 2 November 2007.

ZigBee operates in the industrial, scientific and medical (ISM) radio bands; 868 MHz in Europe, 915 MHz in the USA and Australia, and 2.4 GHz in most jurisdictions worldwide. The technology is intended to be simpler and less expensive than other WPANs such as Bluetooth. ZigBee chip vendors typically sell integrated radios and microcontrollers with between 60K and 128K flash memory, such as the Jennic JN5148, the Freescale MC13213, the Ember EM250, the Texas Instruments CC2430 and the Atmel ATmega128RFA1. Radios are also available stand-alone to be used with any processor or microcontroller. Generally, the chip vendors also offer the ZigBee software stack, although independent ones are also available.

Because ZigBee can activate (go from sleep to active mode) in 15 msec or less, the latency can be very low and devices can be very responsive — particularly compared to Bluetooth wake-up delays, which are typically around three seconds. Because ZigBees can sleep most of the time, average power consumption can be very low, resulting in long battery life.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The first stack release is now called ZigBee 2004. The second stack release is called ZigBee 2006, and mainly replaces the MSG/KVP structure used in 2004 with a "cluster library". The 2004 stack is now more or less obsolete.

ZigBee 2007, now the current stack release, contains two stack profiles, stack profile 1 (simply called ZigBee), for home and light commercial use, and stack profile 2 (called ZigBee Pro). ZigBee Pro offers more features, such as multi-casting, many-to-one routing and high security with Symmetric-Key Key Exchange (SKKE), while ZigBee (stack profile 1) offers a smaller footprint in RAM and flash. Both offer full mesh networking and work with all ZigBee application profiles.

Zig Bee 2007 is fully backward compatible with ZigBee 2006 devices: A Zig Bee 2007 device may join and operate on a ZigBee 2006 network and vice versa. Due to differences in routing options, ZigBee Pro devices must become non-routing ZigBee End-Devices (ZEDs) on a ZigBee 2006 or ZigBee 2007 network, the same as ZigBee 2006 or ZigBee 2007 devices must become ZEDs on a ZigBee Pro network energy systems Today, an electricity disruption such as a blackout can have a domino effect—a series of failures that can affect banking, communications, traffic, and security. This is a particular threat in the winter, when homeowners can be left without heat.

A smarter grid will add resiliency to our electric power System and make it better prepared to address emergencies such as severe storms, earthquakes, large solar flares, and terrorist attacks. Because of its two-way interactive capacity, the Smart Grid will allow for automatic rerouting when equipment fails or outages occur. This will minimize outages and minimize the effects when they do happen. When a power outage occurs, Smart Grid technologies will detect and isolate the outages, containing them before they become large-scale blackouts. The new technologies will also help ensure that electricity recovery resumes quickly and strategically after an emergency—routing electricity to emergency services first, for example.

In addition, the Smart Grid will take greater advantage of customer-owned power generators to produce power when it is not available from utilities. By combining these "distributed generation" resources, a community could keep its health center, police department, traffic lights, phone System, and grocery store operating during emergencies. In addition, the Smart Grid is a way to address an aging energy infrastructure that needs to be upgraded or replaced. It's a way to address energy efficiency, to bring increased awareness to consumers about the connection between electricity use and the environment. And it's a way to bring increased national security to our energy System—drawing on greater amounts of home-grown electricity that is more resistant to natural disasters and attack.

Finger print module

Fingerprint Sensor Module is able to conduct fingerprint image processing, template generation, template matching, fingerprint searching, template storage, etc. Compared with similar products from other suppliers, KY-M6 proudly boasts of following features:

Proprietary Intellectual Property

Optic fingerprint enrollment device, KY-M6 hardware as well as fingerprint algorithm are all developed by Key Power Security.

Wide Application Range of Fingerprints with Different Quality

Self-adaptive parameter adjustment mechanism is used in the course of fingerprint enrollment. This ensures good image quality for even dry or wet fingers, thus it has wider application range.

Immense Improved Algorithm

KY-M6 Fingerprint algorithm is specially written according to optic imaging theory. The algorithm is good for low-quality fingers due to its excellent correction and tolerance features.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Flexible Application

User can easily set KY-M6 Module to different working modes depending on complexity of application systems. User can conduct secondary development with high efficiency and reliability.

Easy to Use and Expand

It is not necessary for user to have professional knowledge in the field of fingerprint verification. User can develop powerful fingerprint verification application systems with the command set provided by KY-M6.

Low Power Consumption

Sleep/awake control interface makes KY-M6 suitable for occasions that require low power consumption.

Different Security Levels

User can set different security level according to different application environment.

Application

KY-M6 can be used on all fingerprint verification systems, such as Safety cabinet, door lock, Complicated door-guard system, Fingerprint IC card Identification Terminal, Fingerprint identification and verification system associated with PC.

Keypad

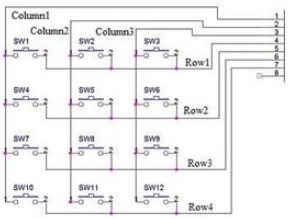
If the application is so time sensitive that the delays associated with de bouncing and awaiting an all up cannot be tolerated then some form of interrupt must be used so that the main program can run unhindered. A compromise may be made by polling the keyboard as the main program loops, but all time delays are don using timers so that the main program does not wait for a software delay.

The get key program can be modified to use a timer to generate the delays associated with the key down de bounce time and the all up delay. The challenge associated with this approach is to have the program remember which delay is being timed out. Remembering which delay is in progress can be handled using a flag bit or one timer can be used to generate the key down de bounce delay and another timer to generate the key up delay. The two timer approach is examined in the example given in this section.

The important feature of this approach is that the main program will check a flag to see whether there is any Keyboard activity. If the flag is set then the program finds the key stored in a ram location and resets the flag. The getting of the key is transparent to the main program it is done in the interrupt program.

As you have seen interfacing switches to microcontroller normally the port pin is high but when a switch is pressed the controller pin gets a Low signal and we come to know that a switch has been pressed. One end of switch is connected to the port pin whereas the other end is connected to the Ground.

In case of matrix Keypad both the ends of switches are connected to the port Pin. Over here we have considered a 4x3 matrix keypad i.e. four rows and three columns. So in all twelve switches have been interfaced using just seven lines. The adjoining figure shows the diagram of a matrix keypad and how it is interfaced with the controller.



As you can see no pin is connected to ground, over here the controller pin itself provides the ground. We pull one of the Column Pins low & check the row pins if any of

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

the Pin is low then we come to know which switch is pressed.

Suppose we make column 1 pin low and while checking the rows we get Row 3 is low then we come to know switch 7 has been pressed.

keil software

It is possible to create the source files in a text editor such as Notepad, run the Compiler on each C source file, specifying a list of controls, run the Assembler on each Assembler source file, specifying another list of controls, run either the Library Manager or Linker (again specifying a list of controls) and finally running the Object-HEX Converter to convert the Linker output file to an Intel Hex File. Once that has been completed the Hex File can be downloaded to the target hardware and debugged. Alternatively KEIL can be used to create source files; automatically compile, link and covert using options set with an easy to use user interface and finally simulate or perform debugging on the hardware with access to C variables and memory. Unless you have to use the tolls on the command line, the choice is clear. KEIL Greatly simplifies the process of creating and testing an embedded application.

Projects

The user of KEIL centers on "projects". A project is a list of all the source files required to build a single application, all the tool options which specify exactly how to build the application, and – if required – how the application should be simulated. A project contains enough information to take a set of source files and generate exactly the binary code required for the application. Because of the high degree of flexibility required from the tools, there are many options that can be set to configure the tools to operate in a specific manner. It would be tedious to have to set these options up every time the application is being built; therefore they are stored in a project file. Loading the project file into KEIL informs KEIL which source files are required, where they are, and how to configure the tools in the correct way.

KEIL can then execute each tool with the correct options. It is also possible to create new projects in KEIL. Source files are added to the project and the tool options are set as required. The project can then be saved to preserve the settings. The project is reloaded and the simulator or debugger started, all the desired windows are opened. KEIL project files have the extension

Simulator/Debugger

The simulator/ debugger in KEIL can perform a very detailed simulation of a micro controller along with external signals. It is possible to view the precise execution time of a single assembly instruction, or a single line of C code, all the way up to the entire application, simply by entering the crystal frequency. A window can be opened for each peripheral on the device, showing the state of the peripheral. This enables quick trouble shooting of mis-configured peripherals. Breakpoints may be set on either assembly instructions or lines of C code, and execution may be stepped through one instruction or C line at a time. The contents of all the memory areas may be viewed along with ability to find specific variables. In addition the registers may be viewed allowing a detailed view of what the microcontroller is doing at any point in time. The Keil Software 8051 development tools listed below are the programs you use to compile your C code, assemble your assembler source files, link your program together, create HEX files, and debug your target program. µVision2 for Windows™ Integrated

Development Environment: combines Project Management, Source Code Editing, and Program Debugging in one powerful environment.

- C51 ANSI Optimizing C Cross Compiler: creates relocatable object modules from your C source code,
- A51 Macro Assembler: creates relocatable object modules from your 8051 assembler source code,
- BL51 Linker/Locator: combines relocatable object modules created by the compiler and assembler into the final absolute object module,
- LIB51 Library Manager: combines object modules into a library, which may be used by the linker,

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

- OH51 Object-HEX Converter: creates Intel HEX files from absolute object modules.

What's New in µVision3?

µVision3 adds many new features to the Editor like Text Templates, Quick Function Navigation, and Syntax Coloring with brace high lighting Configuration Wizard for dialog based startup and debugger setup. µVision3 is fully compatible to µVision2 and can be used in parallel with µVision2.

Advantages

The proposed algorithm almost outperforms other algorithms in each category from Z Tables except for the path length.
In order to locate the Fermat point of a triangle, the largest angle of the triangle must be less than or equal to 120◦.

- Ease of controlling.
- Fast response.
- The module can be made into various forms as per the area of application.
- User friendly- One need not to know about the robot, as they can control by hand movement.

Conclusion and future scope

In this paper, we have presented a new approach toward the development of a gesture-based human–machine interface. An end-to-end approach is presented which maps arm-scale gesture by a human user to a learned response by a robotic agent through repeated applications of user-provided reward. Between these two end points, the constituent challenges are addressed in the areas of sensor selection, data representation, pattern recognition, and machine learning. As a composite approach, the proposed system overcomes many of the shortcomings of previous efforts.

However, it is foreseen that this process would be difficult for an actual human trainer to entertain, since visualization of a robot's configuration as a Cartesian space may be difficult, if not impossible, for higher dimensions. Certainly, a path-planning component would be called for which considers the robot's configuration in light of the geometry of the environment and the social sensibilities of the user (speed, angle of approach, visibility, etc.). As it is implemented here, the proposed approach is seen as practical for mapping of a robot's end effector and, thus, useful for common applications. Segmentation of gestures (*gesture spotting*) is a typical problem in gesture recognition. Although our future work will address spotting, our focus here has been on validation of a real time learning technique that produces desirable outcomes using a human teacher and a simple, binary reward signal.

Result

The project "A Secure Biometrics-Based Multi-Server Authentication Protocol Using Smart Cards" been successfully designed and tested**.** Integrating features of all the hardware components used have developed it. Presence of every module has been reasoned out and placed carefully thus contributing to the best working of the unit. Secondly, using highly advanced IC's and with the help of growing technology the project has been successfully implemented.

Reference

[1] A. El-Sawah, N. Georganas, and E. Petriu, "A prototype for 3-D handtracking and gesture estimation," IEEE Trans. Instrum. Meas., vol. 57,no. 8, pp. 1627–1636, Aug. 2008.

[2] D. G. Lowe, "Distinctive image features from scale-invariant keypoints,"
Int. J. Comput. Vis., vol. 60, no. 2, pp. 91–110, Nov. 2004

[3] A. Bosch, X. Munoz, and R. Marti, "Which is the best way to organize/ classify images by content?" Image Vis. Comput., vol. 25, no. 6, pp. 778–791, Jun. 2007.

[4] H. Zhou and T. Huang, "Tracking articulated hand motion with Eigen dynamics analysis," in Proc. Int. Conf. Comput. Vis., 2003, vol. 2, pp. 1102–1109.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[5] B. Stenger, "Template based hand pose recognition using multiple cues," in Proc. 7th ACCV, 2006, pp. 551–560.

[6] L. Bretzner, I. Laptev, and T. Lindeberg, "Hand gesture recognition using multiscale color features, hieracrchichal models and particle filtering," in Proc. Int. Conf. Autom. Face Gesture Recog., Washington, DC, May 2002.

[7] A. Argyros and M. Lourakis, "Vision-based interpretation of hand gestures for remote control of a computer mouse," in Proc. Workshop Comput.Human Interact., 2006, pp. 40–51.