International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

Design and implementation of enhanced 3factor security protocol

[1]Mekala.Pooja & [2]Ms. N Hima Bindu

[1]**B-Tech (E.C.E) M-Tech (Embedded Systems),** (Persuing) Vignana Bharathi Institute Of Technology (2013-2015) Affiliated To Jntu Hyderabad, mekala.pooja@gmail.com

[2]M.Tech **Assistant Professor B.Tech (JNTUH) M.Tech (JNTUK)**
Himabindu.naineni@gmail.com

Abstract—

With rapid development and usage of technology among people, data migration has become an essential part of our life. Various removable devices like USB flash drives, hard drives, PDAs etc are used to move data. Removable media are widely used for transferring, storing or for backing up data. People often spend considerable amount of time generating data that are confidential even for the organization they work for. Maintaining confidentiality of data has become a great challenge. Any security threat can lead to organization's sensitive data being compromised. Due to this many organizations restricts the usage of removable devices, but restricting usage of these devices is not an optimal solution. In this paper we will review various cryptographic techniques, algorithms and tools available for securing data on major platforms that might help in solving this problem.

Keywords— Data Confidentiality; Information security; USB; encryption; removable media

1.Introduction:

Data confidentiality means that data stored in the system is protected against unintended access. Due to advances in computer science, removable devices are thus preferably used for data storage and transfer due to its convenience, ease of usage and higher transfer speeds. Hence maintaining confidentiality is essential as removable devices are widely used among people for data migration. Due to this, the usage of these devices are tremendously increased resulting in the exposure of confidential data as it is stored in plain text and possess huge risk of data being compromised and being misused. Thus, this has become a major issue in the field of information security. Data theft has now become a growing problem as with the ease in technology like desktop computers, other hand-held devices all the sensitive data is been stored in them and if proper security is not provided or if someone is intercepting or attacking the data it can create huge problems in individual's personal or professional life. Therefore, despite their convenience and ease of usage, removable devices (USB) have been prohibited in most of the institutes/organizations as they are main source of transmitting computer viruses and other harmful software that harms and degrades the performance of machines, but preventing usage of these devices is not an optimal solution. USB memories have become standard components to store data in enterprises and among individuals. However, crucial information can be obtained from these memories when USBs are lost, stolen or hacked because they usually store many different kinds of important data. The loss of this data can result in considerable security vulnerabilities and sometimes can also breach national security [1].

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

Besides, [4] claimed that a security breach exposing the data of over 2595 Michigan resident's personal information was compromised when a laptop and a flash drive was stolen from the employee of State Long Term Care (LTC) Ombudsman's Office on January 30,2014

2 RELATED WORK:

Various tools and software are available that helps us in our study. They are widely used tools or disk encryption software which is computer security software that maintains confidentiality of data that is stored within removable media (such as USB media, hard disks, floppy disk etc.) by using disk encryption. Several types of tools are reviewed, such as BitLocker, TrueCrypt, FileVault, AESCrypt, SecurStick which shows the current trend in disk encryption scenario. BitLocker (BitLocker Drive Encryption) initially released in 2006, is a security feature that provides protection to• data and is available for Windows operating system users running Ultimate or Enterprise version of Windows 7 or the pro and Enterprise version of Windows 8. It is also available for server platforms like Windows server 2008. It is used to provide encryption to data of entire volumes and by default it uses AES encryption algorithm in CBC mode with 256 bit key, combined with Elephant diffuser as it provides additional security which is not provided by AES. But the disadvantage of this is it works only on Windows Platform [10]. TrueCrypt is a software for preserving and implementing an on the fly encryption (OTFE). On the fly encryption• is a method which refers to data being automatically encrypted or decrypted as it is loaded or saved. It creates a virtual encrypted disk within a file, partition or the entire storage device where data cannot be decrypted (read) without using password or encryption keys. TrueCrypt was the only software which was used on Android platform. But on May 2014, TrueCrypt Website announced that the project was no longer available and recommended users to find an alternate solution [9]. FileVault was introduced in Mac OS X Panther, which encrypted user's home directory but not the entire volume.• Now FileVault is available for Mac OS X Lion or later and OS X Recovery installed on the start-up drive. FileVault uses XTS-AES 128 bit encryption for securing data. Only authorized users can lock or unlock the drives. This encrypts whole OS X start-up volumes and includes home directory as well. But the major disadvantage of this is it works only for the Mac OS platform [8]. AESCrypt is open source file encryption software which runs on Windows, Mac, Linux and even Android devices.• It uses 256-bit AES encryption algorithm which can safely secure the user's most sensitive information. On Windows the files are encrypted by only right clicking and choosing aescrypt. On Mac, user can drag a file and provide the required password into the aescrypt program. On Linux, using command line specific syntax is used i.e by using word "aescrypt" encryption or decryption of files can take place. Relies upon having /dev/urandom, This program was deliberately kept extremely simple. It is not intended to be a full encryption solution, it is intended to be used within scripts as part of a complete solution. Keychain management, public key signatures, etc. are all expected to be done external to this program [11]. SecurStick is a portable drive encryption tool which is used to secure data of USB drives and removable media. It• uses AES-256 bit encryption algorithm and works for Windows, Mac, Linux platforms. It consists of WEBDAV which caches the data and passwords so it is more important to remove the cache files before leaving the page. SecurStick does not guarantee data protection as anyone can

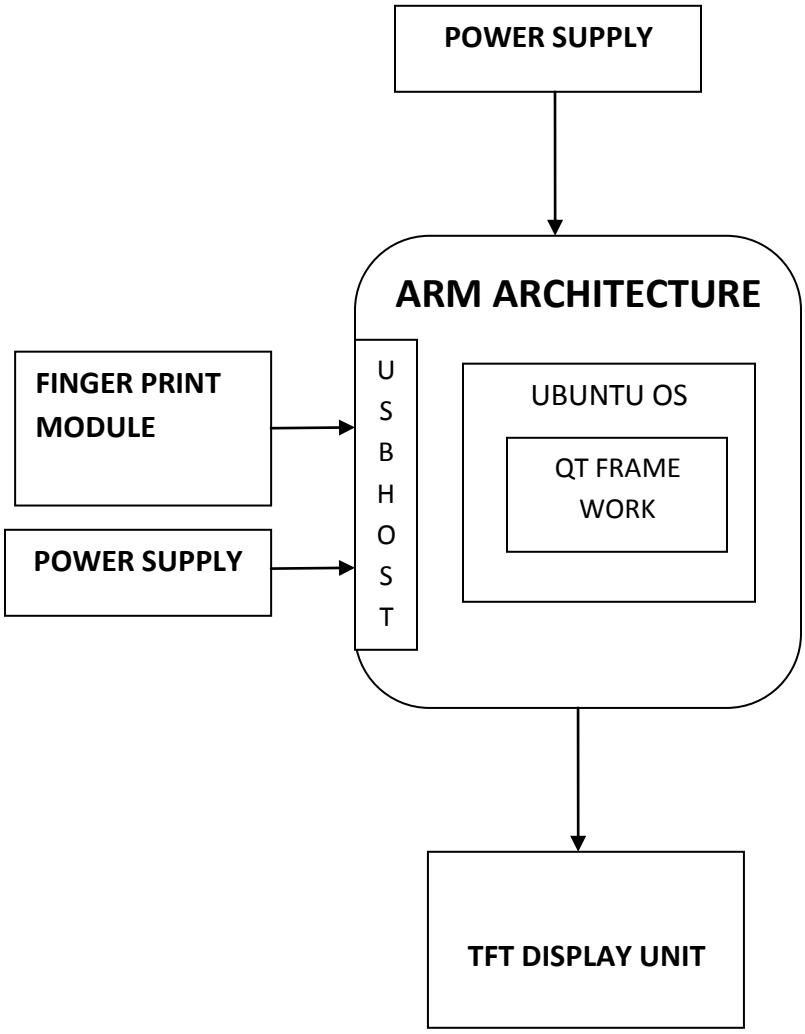
International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

delete the files but it can protect our data from being stolen. It is a German website but its English translation is also available [7].

3. PROPOSED METHOD:

In the proposed method we overcome the drawback present in existing system by using three levels of security. Our system is designed by using ARM 32-bit micro controller which supports different features and algorithms for the development of automotive secure embedded systems. We are using touch pattern, password through keypad, and biometric data like human finger using finger print module. When any file transfer from one usb to another usb then it asked for username/password, it will verify the finger of the person who connected the usb device to system where the usb device is connected. When everything is matched then only usb device start working on the system and data exchange is possible.

BLOCK DIAGRAM:



International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

3.1.Power supply:

Power supply is a reference to a source of electrical power. A device or system that supplies electrical or other types of energy to an output load or group of loads is called a power supply unit or PSU. The term is most commonly applied to electrical energy supplies, less often to mechanical ones, and rarely to otherThis power supply section is required to convert AC signal to DC signal and also to reduce the amplitude of the signal. The available voltage signal from the mains is 230V/50Hz which is an AC voltage, but the required is DC voltage(no frequency) with the amplitude of +5V and +12V for various applications_In this section we have Transformer, Bridge rectifier, are connected serially and voltage regulators for +5V and +12V (7805 and 7812) via a capacitor (1000µF) in parallel are connected parallel as shown in the circuit diagram below. Each voltage regulator output is again is connected to the capacitors of values (100µF, 10µF, 1 µF, 0.1 µF) are connected parallel through which the corresponding output(+5V or +12V) are taken into consideration.

3.2.SMART ARM-based MPU:

SMART SAMA5D3 series is a high-performance, power-efficient®The Atmel -A5 processor, achieving 536 MHz® Cortex®embedded MPU based on the ARM with power consumption levels below 0.5 mW in low-power mode. The device features a floating point unit for high-precision computing and accelerated data processing, and a high data bandwidth architecture. It integrates advanced user interface and connectivity peripherals and security features. The SAMA5D3 series features an internal multi-layer bus architecture associated with 39 DMA channels to sustain the high bandwidth required by the processor and the high-speed peripherals. The device offers support for DDR2/LPDDR/LPDDR2 and MLC NAND Flash memory with 24-bit ECC. The comprehensive peripheral set includes an LCD controller with overlays for hardware-accelerated image composition, a touchscreen interface and a CMOS sensor interface. Connectivity peripherals include Gigabit EMAC with IEEE1588, 10/100 EMAC, multiple CAN, UART, SPI and I2C. With its secure boot mechanism, hardware accelerated engines for encryption (AES, TDES) and hash function (SHA), the SAMA5D3 ensures anti-cloning, code protection and secure external data transfers. The SAMA5D3 series is optimized for control panel/HMI applications and applications that require high levels of connectivity in the industrial and consumer markets. Its low-power consumption levels make the SAMA5D3 particularly suited for battery-powered devices.

3.3.FINGER PRINT MODULE:

The ARA-EM01 is high performance fingerprint module developed by Aratek Biometrics Technology Co, Ltd .it has many features : easy restructure, powerful functions, compatible with PC, and multiple-functions in one module: Fingerprint enrollment, image process, characters acquisition, fingerprint template creation, fingerprint template storage, fingerprint compare (1: 1, 1: N), fingerprint delete. This module can work with different devices based on UAWRT such as PC, SCM and so on. Only easy circuits and fingerprint module can enhance your product into fingerprint authentication power. It is widely used by electronics business, information security, access control, identity authentication and other security industry.

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

3.4. TFT TOUCH SCREEN

A thin-film-transistor liquid-crystal display (TFT LCD) is a variant of a liquid-crystal display (LCD) that uses thin-film transistor (TFT) technology to improve image qualities such as addressability and contrast. A TFT LCD is an active-matrix LCD, in contrast to passive-matrix LCDs or simple, direct-driven LCDs with a few segments. TFT LCDs are used in appliances including television sets, computer monitors, mobile phones, handheld video game systems, personal digital assistants, navigation systems and projectors. TFT LCDs are also used in car instrument clusters because they allow the driver to customize the cluster, as well as being able to provide an analogue-like display with digital elements. The liquid crystal displays used in calculators and other devices with similarly simple displays have direct-driven image elements, and therefore a voltage can be easily applied across just one segment of these types of displays without interfering with the other segments.

3.5.Key pad:

A keypad is a set of buttons arranged in a block which usually bear digits and other symbols but not a complete set of alphabetical letters. If it mostly contains numbers then it can also be called a numeric keypad. Keypads are found on many alphanumeric keyboards and on other devices such as calculators, combination locks and telephones which require largely numeric input. An input device, sometimes part of a standard computer keyboard, consisting of a separate grid of numerical and function keys arranged for efficient data entry.

CONCLUSION

The three-factor authentication protocol based on Elliptic Curve Cryptosystem for USB consumer storage devices has been shown to have significant advantages, but as presented in this paper, there were still existing security vulnerability issues needed to be solved, specifically the password guessing attack, the DoS attack and the replay attack. This paper has presented a significantly enhanced security protocol to address previous weaknesses. The proposed protocol has been presented and rigorously analyzed in terms of security and computational cost. As shown, the proposed protocol is robust against conceivable attacks while at the same time having the same computational cost compared to the literature. The work is ideal to be embedded in the firmware of consumer based USB Mass Storage Devices thus relieving the user of extra security burdens and enabling the devices to be confidently used in the knowledge that the data stored is secure.

REFERENCES

[1] M. Alzarouni, "The reality of risks from consented use of USB devices," in Proc. 4th in Proc. 4th Australian Information Security Management Conference, pp. 312-317, December 2006.

[2] C. Wu, W. Lee, and W. J. Tsaur, "A secure authentication scheme with anonymity for wireless communications," *IEEE Communications Letters*, vol. 12, no. 10, pp. 722-723, Oct. 2008.

[3] M. S. Hwang, and L. H. Li, "A new remote user authentication scheme using smart cards," *IEEE Trans. Consumer Electron.*, vol. 46, no. 1, pp. 28-30, Feb. 2000.

[4] W. C. Ku, and S. M. Chen, "Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards," *IEEE Trans. Consumer Electron*, vol. 50, no. 1, pp. 204-207, Feb. 2004.

[5] E. Yoon, E. Ryu, and K. Yoo, "Further improvement of an efficient password based remote user authentication scheme using smart cards," *IEEE Trans. Consumer Electron*, vol. 50, no. 2, pp. 612-614, May 2004.

[6] H. C. Hsiang, and W. K. Shih "Weaknesses and improvements of the Yoon-Ryu-Yoo remote user authentication scheme using smart cards," *Computer Communications*, Elsevier, vol. 32, no. 4, pp. 649-652, Mar. 2009.

[7] K. -A. Shim, "Security flaws in three password-based remote user authentication schemes with smart cards," *Cryptologia*, Taylor and Francis, vol. 36, no. 1, pp. 62-69, Jan. 2012.

Authors profile:

Ms. N Hima Bindu M.**Tech**., (Assistant Professor)

Academic Record

Name of the Faculty	**Ms. N Hima Bindu**
Profile Picture	
Designation	Assistant Professor
Qualification	B.Tech (JNTUH) M.Tech (JNTUK)
Area of Specialization	VLSI
Experience	Teaching - 2 Industry -0.6
Publication	National - 1 International - 2 Seminars/Workshops - 1
Mobile Number	9491 531 031
E-Mail ID	Himabindu.naineni@gmail.com

International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 10, October 2015
Available at http://internationaljournalofresearch.org

MEKALA.POOJA

D.O.B:- 10/07/1990 (10TH JULY 1990)

ADDRESS: - H.NO:- 4-85/3, BUDHA NAGAR COLONY, PEERZADIGUDA (V) , UPPAL DEPOT, GHATKESAR(M),

DISTRICT- RANGAREDDY, PIN CODE- 500098, TELANGANA.

MAIL ID: - mekala.pooja@gmail.com, MOBILE: - 8099835874.

QUALIFICATION:- B-TECH (E.C.E)

(VIGNAN'S INSTITUTE OF MANAGEMENT AND TECHNOLOGY FOR WOMEN) (2008-2012) Affiliated to JNTU Hyderabad, (VILL)-KONDAPUR, (MDL)-GHATKESAR, (DIST)-RANGAREDDY.

M-TECH (EMBEDDED SYSTEMS), (PERSUING)

VIGNANA BHARATHI INSTITUTE OF TECHNOLOGY (2013-2015) Affiliated to JNTU Hyderabad, Aushapur (V), Ghatkesar (M), R.R.Dist-501301