SECURITY PROTOCOLS FOR USB MASS STORAGE DEVICES

R TULASI[1], Embedded systems, LIMAT, Vijayawada, India
K Ravi kiran[2], Embedded systems, LIMAT, Vijayawada, India

ABSTRACT: Security for the Universal serial bus is more important in the present commercial society. Data transferring from mass storage devices is widely used in consumer. Large amount of data is carried in the mass storage devices. In many commercial industries or institutes MSDs are not allowed. This is to maintain security for the data present in the commercial society. There are many systems to provide security for the data like biometric, password... This is due to provide authentication for the data in mass storage devices. This paper proposes the three way security factor and authentication. This paper helps to protect data in mass storage devices from many attacks like modification, unauthorized reply and data hacking. This paper provides the solution for all this types of attacks. So high security for the data transmission in commercial society through MSBs is provided.

Keywords: authentication, denial attacks

INTRODUCTION:

In this project, a data transfer between pen drive to pen drive without using a computer or laptop is discussed by providing three types of securities. A data transfer is done by using computer or laptop means it consumes more power and it is not a handy device to carry to particular locations. To overcome this, a data transfer is done by using a ARM processor (handy device).

The proposed BioFIM is a revolutionary idea for the USB data security, by which a combination of fingerprints, portable flash drive and touch screen based password. The features of the proposed BioFIM conclude that this particular scheme will be more resilient against storage theft than the existing schemes in terms of security and user convenience. A pen drive is inserted into the USB port then a signal will be sent to the ARM processor. By using this signal processor identifies the host pen drive is detected. Now the ARM processor will start fetching the data from the source pen drive into the buffer and the ARM processor waits for the signal from destination pen drive. When ARM processor gets the signal from the slave pen drive, the ARM processor is ready to transfer the data. Before transferring a data the ARM processor should get the input from external touch panel from the user. Once the user press the touch panel then automatically finger print module will enable and waiting for finger print. Once the finger print is verified on touch screen the numeric digits will display we need to enter the password on the touch screen then the arm processor gets the information to transfer the data between two pen drives.

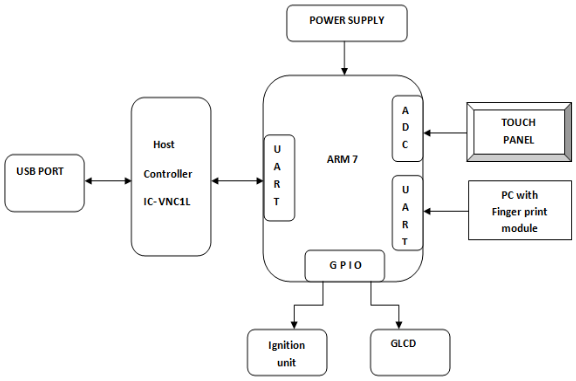
EXISTING SYSTEM

- Direct pen drive access
- High power consumption
- No touch screen based technology

PROPOSED SYSTEM:

- Security based on USB ports
- Touch based password technology
- Security with finger print

BLOCK DIAGRAM:



The main heart of the project is ARM7. The security provided for the USB devices are biometric, password, authentication. These three factor modules are connected to the LPC2148. Whenever the wrong authentication is processed buzzer will be intimated as a sign of wrong authentication. When an authorized person gives the sign of verifications then the security factors will be verified one by one. USB port is connected to the ARM through Host controller. The biometric of authorized person was stored in the database of a personal computer. The VISUAL BASIA is the software used in the PC for biometric and authentication.

The main operation is when an mass storage device is incerted to the USB port the GLCD will be enabled then the particular operation to be done is selected, then the password will be enabled. If the password is correct then it will be entered to the biometric. If the biometric also matches then the particular operation which was selected previously was performed.

HARDWARE:

- ARM 7 Processor
- USB host controller IC- VNC1L
- Pen drive
- Touch screen
- Finger print
- Ignition unit

SOFTWARE:

- Keil ide
- Orcad
- Flash magic
- Visual basic6

APPLICATION:

- Low power consumption
- Security applications
- Voting applications
- Data transfer applications

ARM PROCESSER:

- ARM968E-S processor running at frequencies of up to 125 MHz maximum.
- Multi-layer AHB system bus at 125 MHz with four separate layers.
- Two Tightly Coupled Memories (TCM), 32KB Instruction TCM (ITCM), 32 KB Data

- TCM (DTCM).
- Two separate internal Static RAM (SRAM) instances; 32 KB SRAM and 16 KB SRAM

BIOMETRIC MODULE:

FPC-AM3 module is equipped with the robust fingerprint sensor FPC1011F3. The module acts as a biometric sub-system with onboard template storage. Integrating the FPC-AM3 module into a product drastically reduces time-to-market with its easy-to-integrate serial command interface and proven robust fingerprint sensor solution FPC-AM3 features the robust fingerprint sensor FPC1011F3 and biometric processor ASIC FPC2020. The sensor FPC1011F3 with its hard protective coating protects the sensor against ESD well above 30 kV, as well as scratches, impact and everyday wear-and-tear. The sensor FPC1011F3 with its 3D pixel sensing technology can read virtually any finger; dry or wet. The robust sensor assisted by the massive biometric processing power and low power consumption means that the module FPC-AM3 is the correct choice of biometric module for any embedded application.

Graphical LCD

- 128x64 LCD implies 128 columns and 64 rows. In total there are (128x64 = 1024) pixels.
- 128x64 LCD is divided equally into two halves. Each half is controlled by a separate controller and consists of 8 pages. In above diagram, CS stands for Controller Select.
- Each page consists of 8 rows and 64 columns. So two horizontal pages make 128 (64x2) columns and 8 vertical pages make 64 rows (8x8).

CONCLUSION:

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] 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.

[2] 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.

[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. M28-30, 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] D. -J. Kim, and K. -S. Hong, “Multimodal biometric authentication using teeth image and voice in mobile environment,” *IEEE Trans. Consumer Electron.*, vol. 54, no. 4, pp. 1790-1797, Nov. 2008.

[6] D. -J. Kim, K. -W. Chung, and K. -S. Hong, "Person authentication using face, teeth and voice modalities

for mobile device security", *IEEE Trans. Consumer Electron*, vol. 56, no. 4, pp. 2678-2685, Nov. 2010.

[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.

[8] S. -H. Lee, D. -J. Kim, and J. -H. Cho, "Illumination-robust face recognition system based on differential components," *IEEE Trans. Consumer Electron.*, vol. 58, no. 3, pp. 963-970, Aug. 2012.

BIOGRAPHIES

R. TULASI[1] pursuing M-Tech in LIMAT, Vijayawada affidavit to JNTUK. Completed B-Tech in Gudlavalleru Engineering College (autonomous) affidavit to JNTU Kakinada.

K. Ravi kiran[2] received M-Tech degree from JNTU Kakinada, present he is working as assistant professor.