USB-KEY_SYSTEM: ELECTRONIC SECURITY KEY SYSTEM USING UNIVERSAL SERIAL BUS FLASH DRIVE INTEGRATION

Rony Setyawan and Lukman Sahid  
Telkom Institute of Technology, Bandung  
rony@setyawansyah.com dan lux_428@yahoo.com

ABSTRAK

Di era globalisasi ini, teknologi informasi dan komunikasi memegang peran aktif sebagai pendukung aktivitas dalam banyak bidang kehidupan. Kebutuhan akan teknologi yang semakin maju mendorong manusia untuk terus berinovasi membuat alat yang dapat membantu dan mempermudah pekerjaan manusia. Namun, di sisi lain, pentingnya keamanan sebagai salah satu paket dari kenyamanan yang ditawarkan oleh teknologi yang berkembang saat ini menjadi pertimbangan lain dari para pengembang teknologi untuk menciptakan alat yang dilengkapi dengan keamanan yang handal sebagai jaminan kenyamanan untuk pengguna teknologi. Makalah ini akan memperkenalkan sebuah sistem keamanan baru yang lebih praktis dan mudah, yaitu dengan menggunakan Universal Serial Bus Flash Drive (UFD) sebagai Identification (ID) user untuk mengakses problem domain/obyek tertentu dengan keamanan berlapis, fitur pendukung yang lengkap, beserta relay yang dijalankan penuh secara elektrik. Sistem ini disajikan dalam bentuk prototype sehingga mempermudah pemahaman mengenai struktur fungsional yang bekerja pada sistem tersebut. 

Kata Kunci: Universal Serial Bus Flash Drive (UFD), Identification (ID), Relay, Elektrik, Prototype.

1. Introduction
1.1 Background

In this globalization era, Information and Communication Technology has an important role in the development of human existence in a lot of circumstances. Requirement of technology draws them in the situation of sophisticated technology and automated things, even though there are security problems. Growing sophistication of security technology is in accordance with the development of technology that supports people.

Lots of methods are used in improving the safety of a particular object, from the conventional methods (physical) to a modern method with a specific technology. The conventional method is no longer able to be maintained because it tends to easily be broken, such as locks for motorcycles that can be easily destroyed by force simply by using a hammer. Modern methods began to emerge because they are more accountable to ensure reliability and to improve the security of a particular object.

Sophistication of security technology has developed in line with the development of technology that supports all kinds of human needs. Security exists because of the demand of technologies in order to increase the security level of a particular object. Therefore, new technological innovations in the field of security as alternatives which can cover the lack or weakness of previously existing technologies are needed. One innovation existing in the field of security technology is USB-KEY System.

1.2 Objective

The purpose this research are:
1) The creation of a new security system that enhances security.
2) The creation of an easy, but reliable security system implementation.
3) The creation of an alternative digital security at affordable prices.
4) Ease to be developed and applied to a wide range of technologies that are assumed in the future as a multifunctional key which is able to be used to access some kinds of objects with only one key (read: UFD) as a safety device.

1.3 Problem Definition

Based on the description of the background, the problems observed in this research are defined as follows.
1) How to create a host that able to be integrated with a Universal Serial Bus (USB) system.
2) How to make UFD that is able to be connected and detected as a key with multiple layered security on a USB system.
3) How to make a microcontroller that is able to be synchronized with the USB system.

2. Fundamental Theory
2.1 Universal Serial Bus (USB)

In information technology, Universal Serial Bus (USB) is a serial bus standard to interface the main computer equipment. USB is designed to allow many peripherals for using a socket connection directly to the standard and enhance the capabilities via plug and play hot swapping which allows peripherals to be connected and disconnected without booting up the back or shut down the computer components that are very far from the practicality and convenience of use. In
other respects, these features deliver the advantage of only requiring low energy consumption and without the required additional energy from outside of the computer itself and allow a lot of equipment to be used without a specific structure and without the need for installing certain drivers in advance in accordance with the equipment to be used.

USB is established to replace the many diverse legacy of serial and parallel ports. USB is able to connect computer peripherals such as mouse, keyboards, PDAs, game pad, scanner, joystick, digital cameras, personal media players, flash drives, etc. For most of those devices, USB has become the standard method of transmission. Basic USB is actually designed for personal computers, but it has generally been in the other devices such as PDAs and video game consoles and bridging power cord between the AC adapter that is installed in a wall plug for standard USB charging. Design is standardized by USB Implements Forum (USB-IF), an agency that became an industry standard incorporation of many leading computer companies and electronics industries.

![Figure 1. Schematic of the Universal Serial Bus System](image)

An Input-Output devices (I/O) USB is a combination of hardware and software. USB3 picture above shows the model of equipment software I/O routed to a host Personal Computer (PC). An interface I/O device, in fact, uses sensors to gather information from the real world such as temperature, color, size, and using actuators and transducers to control the real world. Data were collected from the real world that are placed in a local area called a buffer IN endpoint. Host PC will collect this data later. The data transmitted by the host PC into a local buffer is called the OUT endpoint. An I/O USB requires a CPU or a microcontroller, microprocessor, digital signal microprocessor or a state machine function. This CPU is responsible for translating the signals from the real world into the data in the IN endpoint and to translate the data in the OUT endpoint into the real world signals. This setting has been done by a local CPU in which the preand post-processes the data in a system implementation based on the USB. Think of this as an extension to Battery Input Output System (BIOS). The host PC operating system is to provide common data for the general equipment I/O through the OUT endpoint and handle the specifics on the I/O device that is set by the CPU specified in the equipment I/O. The same specific actions are required to input device specific data held by the CPU I/O and general data are provided to the host PC via an IN endpoint. A type of PC BIOS will handle the keyboard, mouse, display and I/O type of computer. USB model is an extension for handling many system acquisition and distribution of data and many data formats including voice and video.

A collection of endpoints is called an interface that describes a class of equipment. Class is an important concept that should be explained. A type of operating system like windows and linux support an array of I/O width. In the same group of tools will use a common class driver to interact with this group of the same equipment. A type of operating system would involve a driver-class area, such as printers, sound, human interface equipment (HID) and mass storage, to support a wide collection of equipment from the I/O. All operating system drivers allow writing equipment if the equipment I/O is not supported and there is no device class driver in it.

There is a one-to-one mapping of the interface I/O to the host PC device drivers.
Figure 2. The Work Principal of the Universal Serial Bus System

USB4 picture above is the hardware model of the USB system in which an I/O device can have up to 16 IN and 16 OUT endpoints through. All components must implement Endpoint 0. Regulatory protocol is the CPU I/O device that runs the program to react to the requests from the host PC. An I/O USB is always a slave such as demand response from the host PC. The demand here can be configured and set on the endpoints 0 or data requests to the endpoint 1. The operation of an I/O is fixed, and always responds in the same time. Demand data is manipulated by the application firmware. Endpoint OUT data is sent through the choice of I/O device in the real world. Real world input on IN endpoints are prepared to be collected by the host PC.

2.2 Circuit in VNC1L

Vinculum VNC1L is the first of FTDI vinculum family which is based on embedded integrated circuit which is able to be used as the USB host controller. Not only capable of handling as a USB host interface and data transfer functions, but also related to the building MCU and embedded flash memory. Vinculum classes are able to handle USB properly while
dealing with flashdrives. Vinculum also transparently handles the FAT file structure communicating via UART, SPI or parallel FIFO interfaces via at set of commands or instructions. Vinculum provides a new pricing as an effective solution for providing USB Host capability into the products that previously did not provide the source of its hardware.

2.3 Circuit on the Atmega8

Microcontroller or collectively, the Single Chip Microprocessor (SCM) is a microprocessor system with some supporting components which are packed in one chip. The AVR is a Modified Harvard architecture microcontroller 8-bit RISC. ATmega8 is a CMOS 8-bit microcontroller-based AVR RISC with low power consumption and can execute one instruction per clock cycle. ATmega8 is capable of achieving throughput of up to 1 Mega Instructions per Second (MIPS) per MHz that can facilitate the designer to optimize speed of work and power consumption. Voltage is needed between 4.5 to 5.5 Volt. When used with ration 3 Volt and working frequency of 4 MHz at 25°C, it will consume 3.8 mA of current when active and 1 mA when idle.

AVR core has 32 registers which are directly connected to the Arithmetic Logic Unit (ALU). This allows two different registers to be accessed with just one instruction where each instruction is executed in one clock cycle only. This architecture results in an improved efficiency of the instruction code, while increasing throughput up to ten times higher than CISC architected microcontroller.

ATmega8 has the following features 8K bytes In-System Programmable Flash with Read-While capabilities-Write, 512 bytes EEPROM, 1K bytes SRAM, 23 I/O ports, 32 registers, three Timer/Counters with flexible modes of comparison, the internal interrupt and external, one serial USART, a byte for Two Wire Serial Interface, a 6-channel ADC (eight channels in TQFP and QFN packages / MLF) with 10-bit accuracy, a programmable Watchdog Timer with Internal Oscillator, an SPI serial port, and five Power Saving mode that can be selected via software. Idle Mode stops the CPU while the SRAM, Timer/Counters, SPI port and interrupt system continue working. In the power down mode, the contents of the register is maintained, the oscillator is stopped, all other chips function until the suspended interrupt or Hardware Reset. In the power-save mode, the asynchronous timer continues to run while the other devices stop working. ADC Noise Reduction mode stops the CPU and all I/O modules, except asynchronous timer and ADC, minimize switching noise during ADC works. In the standby mode, crystal/resonator still oscillates while the other equipment does not work. This allows start-up process going very quickly with low power consumption.

ATmega8 chip is made with non-volatile memory technology of high density. Program memory is able to be reprogrammed via a serial SPI interface with non-volatile memory programmer or with conventional on-chip boot program on the AVR core. Boot program is able to use any interface to download a program application to application memory. Software in the Boot Flash section will continue to run while the Application Flash Section is updated. This is one of the functions of the operations Read-While-Write. By combining an 8-bit RISC CPU and In-System Self-Programmable Flash on a chip, a microcontroller ATmega8 is a very flexible and viable solution to control applications with low cost.

3. Research Methodology

The research methodology of the system is explained as follows.
1) Literature study
2) At this stage the deepening and understanding of concepts and materials through libraries, reliably sourced from books, journals, papers, paper, digital sources, etc. The library literature contains concepts and materials on the following matters.
   - Working principle of the USB system.
   - Architecture Universal Serial Bus Flash Drive (UFD).
   - Schematic Integrated Circuit (IC) VNC1L.
3) Design and Programming Tools
At this stage, the design of electronic circuits with ATmega8 microchip as a microcontroller which is able to connect the key and the host that uses the VNC1L chip form and make the dynamic relation according to a created program supported by Proteus7 software, AVRstudio4 and K-125USBAVRISP downloader programmer.

4) Simulation Phase
This stage executes the simulations or experiments on a finished prototype.

5) Analysis and Conclusion Phase
At this stage, analyze, and draw conclusions of the simulations that have been carried out.

4. USB-KEY System Work Principal Scheme

![USB-KEY Motorcycle Block Diagram](image)

Figure 7. Block Diagram of Implementation USB-KEY System on the Motorcycle

5. USB-KEY System Work Principal\(^5\)
USB-Key is a new innovation in the circumstance of security system that essentially uses Universal Serial Bus Flash Drive (UFD) as the primary identification (ID) user performed as a hardware. This system is flexible to be implemented in a problem domain / specific object and requires only a little modification on the mechanization and the system that adapts to the problem domain / integrated USB-KEY system object.

This USB key is able to replace the motorcycle manual key. To turn on the motorcycle machine, it is only insert the registered USB. These tools rely on passwords from each USB. Each USB have a different number. The unique code of USB has been registered and stored in the black box. Boxes which is going to be laid in the body of the motorcycle have a keypad and USB plug.

USB Host Controller (VNC1L) is going to detect and read part of flash drive while the part of flash drive of the host that has been established to be USB serial. Among them are unique code and password which have been executed an encryption existed in the flash drive. Subsequently, the micro chip (ATmega8) which is contained within the host is going to check the unique code and encrypted passwords that were sent via VNC1L by comparing with a preset program in the ATmega8. If it turns out the same, then it is going to be forwarded to the keyboard and the LCD that are made to set some additional features such as passwords and multiple modes LCD display options such as manual key system, change passwords, and lists of new keys. In the end, it is going to make the relays which is contained in the key of motorcycle. It is able to be connected as a seat lock relay, handlebar lock relay, starter relay, so that the motorcycle is able to run as normal and comfortable.

The function of the keypad is to enter a password if the user wants to do it. It is able to enter a code to unlock the trunk as well. Just enter the code number, then key is going to open the trunk of the motorcycle automatically. No need to
worry if the USB is lost. Black box of USB Key is able to receive two numbers at once, so it is possible to have a spare USB. If both are missing, just register a new USB one more time. In this case, manual key of the motorcycle is useless, ultimately the T key is not able to use by the per petrat or for turning the machine.

6. Conclusion
In summary, function of making the USB-Key is for replying anxiousness of public concerning problems of larceny. It is expected to support safety and pleasantness while using motorcycle. Disabling the manual lock and switching it to USB is able to improve the security for accessing the motorcycle.

7. Limitation of Research
Limitation in this paper is as follows:
1) The prototype is specifically applied to motorcycles.
2) The prototype is made by a series of host system and a microcontroller in integrated USB.
3) It is only used three layers security method, namely vendor IDs of flash drive, encrypted passwords in the microcontroller, and a personal password on each UFD which is used as the key.
4) It is used 3 relays on the prototype, namely starter, handle bar lock, and back seat lock in a used motorcycle.
5) Add a few features which physically unchangeable motorcycle and require a relatively simple installation such as Liquid Crystal Display (LCD), keypad, and several modes, among them change passwords, manual lock, and register a new flash drive as a key.
6) Testing the USB key is at:
   a. Level of sensitivity and time response since the system is entered via the flash drive.
   b. Layered levels security and USB key security system toward outside influences such as: hackers, rain, heat, age, etc.

Bibliography