ILLINOIS INSTITUTE OF TECHNOLOGY

IPRO 304 - SafeByte's Action

Securely Transporting Health Records

Objectives

To make a Health Record system that is:

- Portable

- Secure/Accurate

- Possessive of a method of Certification

- Cost-effective

- Easy to use

- Capable of having multiple users

- HIPAA Compliant

Problem

- Protection against flash device attacking computing device
- Flash drives can transmit viruses
- Protection against modification of Electronic Health Record (EHR) software
- Paper records are less secure
- No secure way of storing and changing authenticated medical records exists

	Patients		Doctors		Pharmacist		Emergency
	See	*Edit*	*See*	*Edit*	*See*	*Edit*	*See*
Personal Information	X	X	X		X	X	X
Allergies and Illnesses	X	X	X	X	X	X	X
Medications	X		X	X	X	X	X
Vaccinations	X		X	X	X		

teamwork

Application and Design

- Put health records on a flash drive
  - ➢Conform to emerging security standards
  - ➢ Fit in to emerging health IT infrastructure
- HIPAA Compliance
  - ➢Health Insurance Portability and Accountability Act
  - ➢Insures patient privacy and health information protection

Demonstrates the basic ability to:

-Store records securely

-Multi-user environment
- ➢Patient
- ➢Doctors
- ➢Pharmacists
- ➢EMS workers

- Basic Records Kept in Safebyte
  - ➢General patient information
  - ➢Allergy information
  - ➢Medications
  - ➢Vaccinations

Physical X-Rays/EKG's

Paper Health Records

Doctor/Pharmacist Input

Teamwork

- Physical interface security
- ➢*Michael Brenyo (Aero. Eng.)*
- ➢*Steven Banaska (E.E.)*

- Application authentication
- ➢*Usman Abubakar (CPE/CIS.)*
- ➢*Ikechi Emelogu (E.E.)*

- Application
- ➢*Shaan Khan (Pre-Med)*
- ➢*Kanishk Sharma (Pre- Med.)*
- ➢*Pooja Oza (Pre-Med.)*
- ➢*Lutfi Dughman (E.E.)*
- ➢*Dmitry Ratnikov (C.S.)*

What is the Future?

-Have the ability to authenticate one's personal medical application

- Will be able to authenticate the identities of Doctors, etc. using a third party source (internet)
- Will be able to store wider range of Medical records

Acknowledgements

- We would like to thank Dr. Brett Trockman for his generous contribution

- Also, we'd like to thank Dr. Wai Gen Yee for his guidance throughout this project.

ILLINOIS INSTITUTE OF TECHNOLOGY

Putting the “Safe” in SafeByte

SafeByte Protects the User’s IT Infrastructure from Flash Drive Based Attacks

A USB Flash Drive Can Harm a Host Computer By:

- Automatically executing harmful code from “plug-and-play” USB devices

- Malicious code and data masquerading as the authentic application.

SafeByte software prevents these attacks in the following ways…

Physical Interface Security

SafeByte’s First Line of Defense Prevents the Activity of Malicious Software

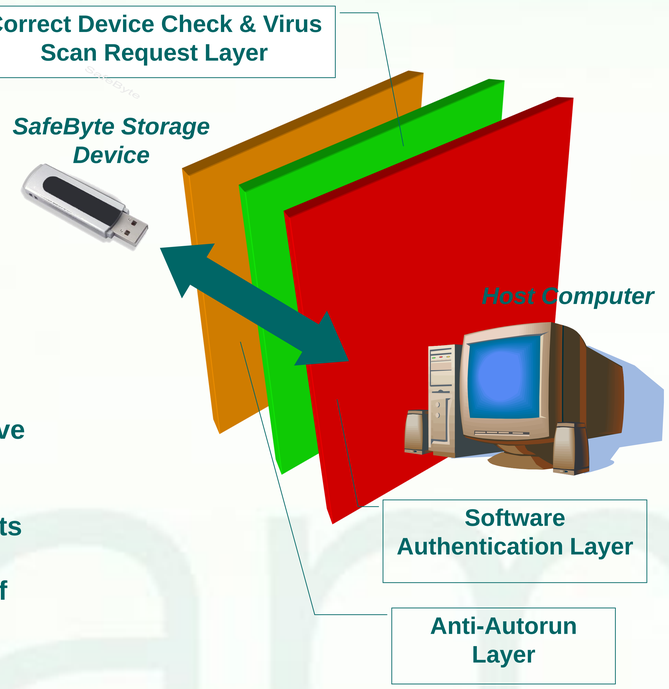
“Auto-run” Prevention:

- During Installation, SafeByte offers the user the option of disabling the auto-run feature of plug and play media, including USB flash drives.

Preventing Onboard Software Triggered Attacks:

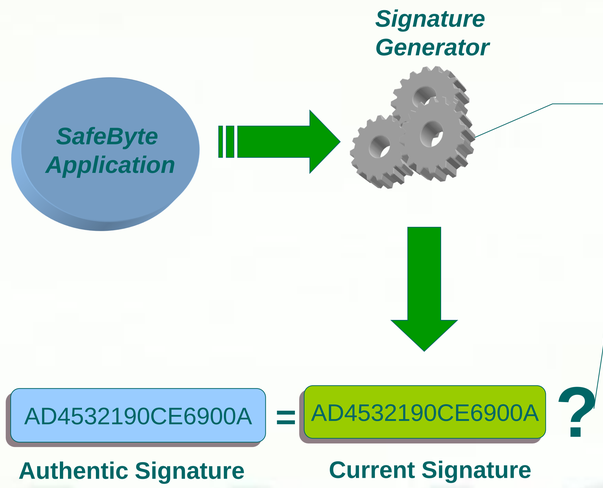
- SafeByte checks all drives for an identification file to ensure the correct drive with the SafeByte application is found.

- SafeByte automatically pauses & requests that the user scan the drive with a third-party virus scanner to add another level of security before accessing the drive.



Application Authentication

SafeByte Verifies the Integrity of the Application, using Digital Signatures



The application is authenticated only if both signatures match

Application Authentication:

- SafeByte ensures that the contents and data on the USB flash drive are authentic, by comparing the application’s authentic digital signature with its current signature.

- The drive contents’ signatures are generated by industry standard cryptographic hash functions like MD5 and SHA.

- If the contents of the drive are changed by a malicious user, virus, or compromised by an error, SafeByte’s authentication software will alert the user.

teamwork