

ATTESTATION-BASED REMOTE BIOMETRIC AUTHENTICATION

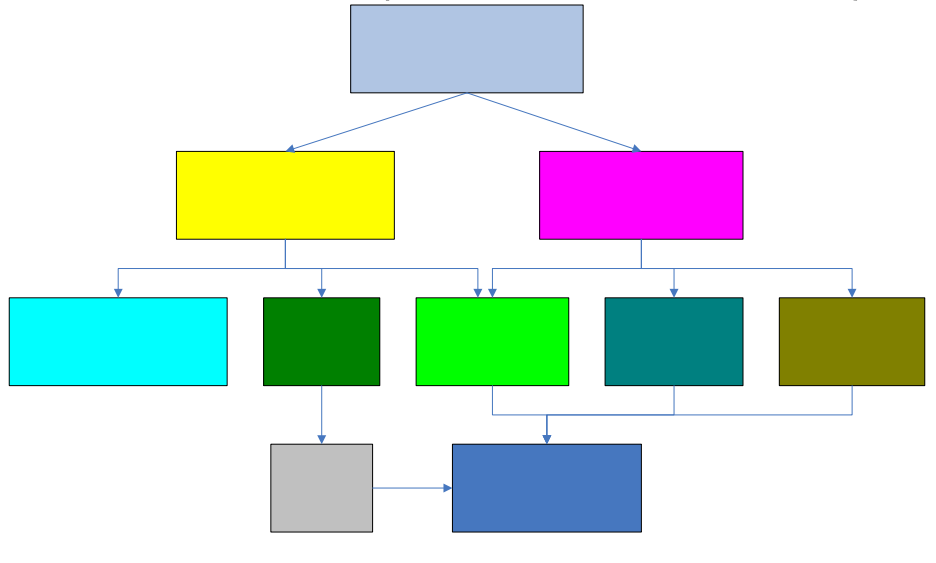
*Thomas Polon
Sam Sander
Clemson University
Clemson, SC*

Introduction

- Technical advances in three areas are required to increase security in biometric systems
 - Performance
 - Liveness Testing
 - Sample Authenticity
- As biometric identification becomes more widespread, users will be more accustomed to providing samples, and the possibility of an attack increases.
- The result is similar to reusing the same password for multiple systems.

Biometric samples are not secrets and should be treated more like evidence and less like a password.

Introduction (Basic Attack Tree)



Unauthorized
Log

Introduction

- An attacker can insert or capture a live sample at any point in the authentication chain.
- Ideally, trust would be in the sensor itself.
- This would cause a large administrative burden.

Attack

Signal
Injection

sensor

D
En

Problem Statement

- Establish a root of trust with device independence.
- Maintain trust throughout the authentication chain.
- Having a system independent of a specific biometric device or driver.
- Matching must be done by a trusted entity.

Proposed Solution

- Having a root of trust elsewhere in the system.
- Attestation Device
- The Trusted Computing Group's (TCG) Trusted Platform Module (TPM)
- BioAPI for biometric independence
- Remote matching service

Methodology

- User workstation hardware:
 - BioAPI compliant biometric device
 - Embedded TCG compliant TPM
- User workstation software:
 - Trusted boot loader
 - OS
 - Network Client
 - BioAPI
 - Biometric device driver

Methodology

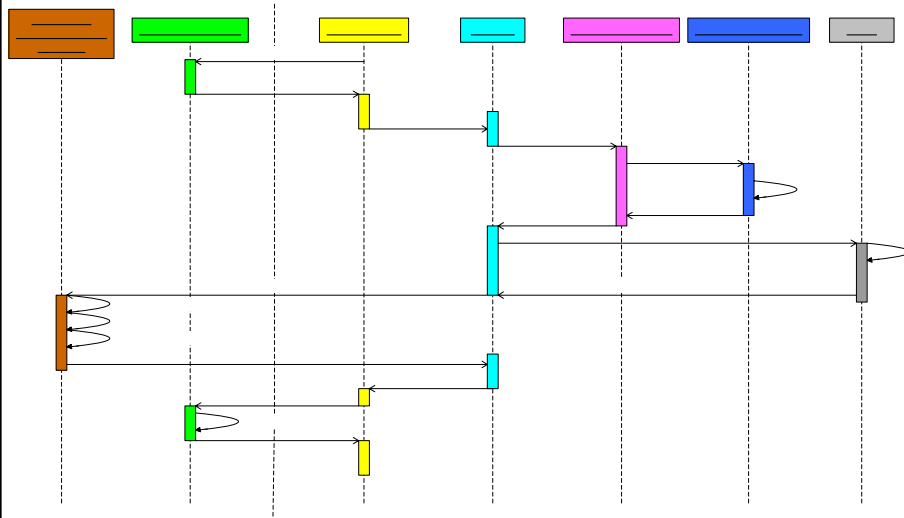
- A Biometric Authentication server (BAS) is used to evaluate the validity of the biometric sample.
- A remote biometric match enables the following security features:
 - User revocation
 - Workstation revocation
 - Multiple attempt lockout
 - Convenient algorithm updates
 - Reliable auditing
 - Intrusion prevention possibilities

Methodology

■ Research Platform:

- IBM Thinkpad z60t
- TCG TPM (Version 1.1b)
- Built-in UPEK fingerprint reader device
- Fedora Core 4 (kernel 2.6.15)
- BioAPI
- Trousers TCG

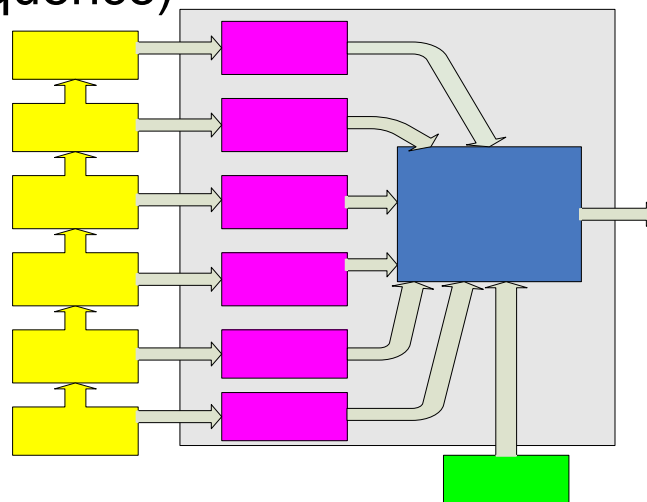
Methodology (Sequence Diagram)



Attestation Overview

- Our system implements the use of an attestation device to derive a trusted platform.
- System uses TPM Specification 1.1b.
- The TPM provides several security features to help make a system more secure.

Attestation Overview (Boot Sequence)



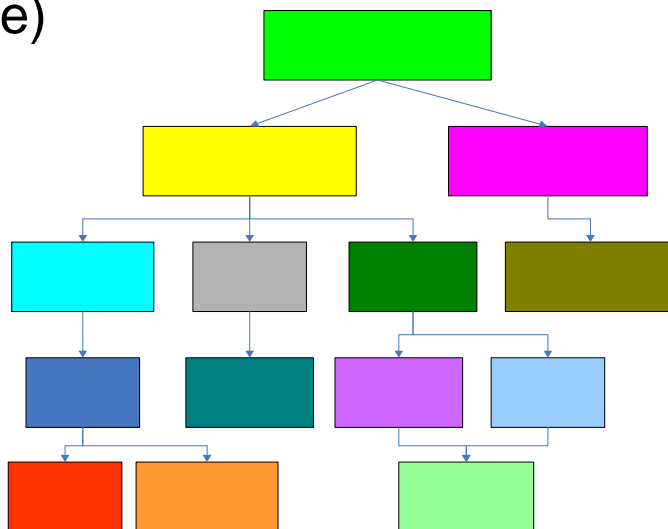
Attestation Overview

- The TPM's PCRs can be compared to reference values at any time.
- The TPM can also sign the hash values stored in the PCR.
- The TPM additionally can provide hardware based key management and authentication.

Results

- Preventing most, if not all attacks that do not exploit the capture device.
- With the added security features, this can be assured.
- The result is a system that can prevent additional types of attacks without the use of proprietary hardware or software.

Threat Assessment (New Attack Tree)



Unauth
Bio

Conclusions

- Current potential weaknesses in biometric authentication systems
- Solution will alleviate problems created by lack of secrets by adding verification to the sample collection process.
- The system involves a small amount of additional hardware and software.
- The system is independent of biometric device type and proprietary products.

Approved Platform

MIM Attack

Crypto attack
or protocol
attack

nal Injection