Introduction Information Security, 2015 Spring

Security Design Project

Anant Kambli

Brian MacKay

Michelle Mulkey

Raleigh Murray

Shahed Shuman

Kathryn Whitmire

Table of Contents

[Overview 2](#_Toc414903428)

[Secure Design Principals 2](#_Toc414903429)

[Security Policy 2](#_Toc414903430)

[Security Mechanisms 3](#_Toc414903431)

[Access Control 5](#_Toc414903432)

[Security Tools 5](#_Toc414903433)

[Test 5](#_Toc414903434)

[Other Security Related testing 5](#_Toc414903435)

# 

# Overview

<Overview of the software system you are building and its core functionality>

# Secure Design Principals

<How would you change your software architecture design to reflect basic secure design principals (e.g. principle of least privilege, no single point of failure, etc.) we have discussed in class>

**Assumptions**

* there is a datalink between mobile app and VistA
* mobile app stores data
* mobile app uses username and password for authentication

## Security Policy

The top three types of information breached:

* Real names
* Birth dates
* Government ID numbers (Social Security)

The mobile app requires access to user data which includes real names and government ID numbers. This information must be protected against mobile device malware and unauthorized access during data transmission.

The mobile app security policy provides for Confidentiality, Integrity, and Availability:

* Confidentiality - user data is NOT disclosed to arbitrary users of the mobile device.
* Integrity – user data is NOT modified by arbitrary users of the mobile device.
* Availability – user data is exchanged with VistA when user checks in.

## Security Mechanisms

Only an authorized user shall access their user data. The mobile app uses password hash and encryption to enforce the security policy. User authentication, via a password, is used to verify the identity of users. Information authentication, via a hash, is used to verify data authenticity.

Encryption is used to protect information transmitted over the datalink and stored on the mobile device. The data being transmitted contains personal information, which left unprotected, could lead to “inference” on a patient’s health. For example, the same patient is scheduling a series of appointments at a specialty facility.

Design principals and assurance the security policy and mechanisms are sound.

<http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=786&FType=2>

Assume the Vista side of the house already follows a security policy (e.g. VA Handbook 6500 Risk Management for VA Information Systems, Appendix F VA System Security Controls)

**Separation of Duties** – not an issue, the mobile app is a single user system. Only one user is authorized to use the mobile app at a time. The authorized user only has access to the same user’s data. Brian will implement concept of a session, session identifier, and session expiration (auto-logoff.)

**Least Privilege** – not an issue, the mobile app only provides tasks for the single authorized user. The mobile app does not escalate user privilege. No administrator, one level/type of user.

**Unsuccessful Logon Attempts** – the mobile app enforces a limit of consecutive invalid logon attempts by a user during a specified time period and automatically takes action when the maximum number of unsuccessful attempts is exceed. (future enhancement to add a captcha)

**System Use Notification** – the mobile app displays to user a system use notification message or banner before granting access to the system that provides privacy and security notices. (lorem ipsum now, future enhancement)

**Previous Logon (Access) Notification** – the mobile app notifies the user, upon successful logon (access) to the system, of the date and time of the last logon (access). Brian will implement.

**Concurrent Session Control** – The mobile app limits the number of concurrent sessions for each account to a maximum number of sessions. (The app does NOT allow concurrent sessions.)

**Session Lock** – the mobile app prevents further access to the system by initiating a session lock after a period of inactivity or upon receiving a request from a user; and retains the session lock until the user reestablishes access using established identification and authentication procedures. (no session locks, the middleware is stateless)

**Session Termination** – The mobile app automatically terminates a user session after defined conditions or trigger events requiring session disconnect. (termination trigger is no activity between phone and middleware for 5 minutes)

**Remote Access** – not an issue, the mobile app uses the VistA VPN. (Today, the middle ware can only be accessed through a phone. Future enhancement could be website access.)

Note: The use of VPNs does not technically make the access non-remote; however, the use of VPNs, when adequately provisioned with appropriate security controls may provide sufficient assurance to VA that it can effectively treat such connections as internal networks. Still, VPN connections traverse external networks and the VPN does not enhance the availability of remote connections.

**Access Control for Mobile Devices** – not an issue, the mobile app does not store/transmit VA data. (There is no VA data stored on the phone. A future enhancement would be security questions, device recognition (e.g. drop a cookie to recognize an existing device.)

Note: All mobile devices that store/transmit VA data must be GFE, and must be included in VA’s Technical Reference Model (TRM). All applications developed and used must store and transmit data using a FIPS 140-2 (or its successor) validated application (or the application data resides in a container-based encryption solution), and must be listed in VA’s TRM. FIPS 140-2 is required for data at rest and data in transit when it contains PII/PHI/sensitive information. There are two methods for this. Either the device itself must provide full-device encryption for all storage and have a protected connection back to VA or the application must be "wrapped" by a FIPS 140-2 validated solution. This would protect the information on a device that does not have data protected any other way. The storage and data in transit must be protected with FIPS 140-2 (or its successor) validated encryption

**Non-Repudiation** – the mobile app protects against an individual being falsely denied having performed actions to be covered by non-repudiation. (future enhancement?) (hint: “we don’t have an appointment for you, come back next year.”) At check-in, the user does “Checkin” and the phone requests GPS location and time, and sends to middle tier. Within 30 minutes of appointment time and within lat/long of the facility. The middle-tier downloads appointments. Just like the phone app barcode for checking into the airport, if there is a technical failure the user will fall back to a real person for help. If within Check-in boundaries (space/time), user receives instructions on how to proceed. The middle-tier checks appointment status for the user each time the user logs in. The user appointment may be changed or cancelled; the user will be notified.

Multiple users may share a phone device.

## Access Control

Pull access control diagram from notes, annotate for mobile app…walk through the mobile app use cases

Subject – access request - reference monitor - object

Source: class notes “Overview of Information Security”

List my appointments, updates, reminders, confirmation…

Phone – **SSL** – middle-tier

SSL authenticates the server (being either VistA or the middle tier) SSL prevents Man in the middle Attack.

Subject has a username/password (middle-tier stores HMAC password) The Reference monitor is the middle-tier (generates GUID like large something, this is used in access request transactions.)

**Questions:**

Is mobile app DAC or MAC? DAC, discretionary access is defined by VistA

Is mobile app using a DBMS? The middle-tier has a database to store user information (list of appointments, list of facilities, fact there is a user, a cache) Future enhancement is to encrypt the database; the appointments are PHI, the name is PII.

Is mobile app using another form of authentication? (Future enhancement is for authentication is user name/ password. retina scan, fingerprint, etc?)

Is mobile app data accessible by VistA? Is there mobile app data that should NOT be accessible by VistA?

# Security Tools

<Which security tools (e.g. access control, encryption, etc.) are you planning to implement in your project and why? Please also discuss in which components you are planning to implement these security tools>

TSL (no SSL)

HMAC algorithm to encode passwords

Opaque token (a very large GUID)

The VistA VPN provides encryption over an unencrypted Wi-Fi connection. This ensures the logon details and contents of messages remain encrypted. This renders intercepted traffic useless to a hacker.

# Test

<How are you going to test your system against some of the vulnerabilities (e.g. SQL injection vulnerabilities, buffer overflows etc.)?>

Uninstall/reinstall the mobile app

Fallback upon the Amazon Security Policy

Activity logging, every time something happens the middle-tier will log it. Future enhancement is IDS/IPS)

Fallback upon the DBMS XYQ Security Policy

Buffer flow not an issue, JavaScript handles this. We will do Fuzz testing (e.g. input parameters.)

# Other Security Related testing

<Please discuss other security related testing you are planning to conduct.>