TH Brandenburg
Studiengang IT Sicherheit
Fachbereich Informatik und Medien
Entwicklung Sicherer Softwaresysteme
Prof. Dr.-Ing. Martin Schafföner

Einsendeaufgabe: Nichtfunktionale Sicherheitsanforderungen

Sommersemester 2024
Abgabetermin 5. Juni 2024

Mara Schulke
Matrikel-Nr. 20215853

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Einführung

In der vorherigen Einsendeaufgabe wurde die Online-Meeting-Plattform Google Meet analysiert und ausgewertet. Die Sicherheitsbegutachtung von Google Meet wird im Rahmen dieser Aufgabe fortgeführt und um Sicherheits-Akzeptanzkriterien bzw. sicherheitsspezifische Anforderungen erweitert. Außerdem werden die verschiedenen Vorgehensweisen verglichen und es werden Testszenarien definiert, mittels derer die Sicherheits-Akzeptanzkriterien verifiziert werden können.

2 Funktionale Anforderungen

Da die funktionalen Anforderungen im Rahmen der letzten Einsendeaufgabe noch nicht konkret benannt worden sind, ist der erste Schritt um sinnvolle Sicherheitsanforderungen zu definieren die Benennung der funktionalen Anforderungen an Google Meet. Im konkreten (angenommen, es wird nur der grundlegende Umfang einer Meeting-Plattform abgedeckt) handelt es sich dabei um die folgenden Anforderungen:

- **Benutzerauthentifizierung:** Google Meet muss es Benutzern ermöglichen, sich zu registrieren, anzumelden und abzumelden.
- **Meeting-Planung:** Google Meet muss es den Benutzern ermöglichen, Besprechungen mit bestimmten Teilnehmern zu planen.
- **Video- und Audio-Streaming**: Google Meet muss Video- und Audiostreaming in Echtzeit unterstützen.
- **Chat-Funktionalität:** Google Meet muss Textchats in Echtzeit während der Sitzungen unterstützen.
- **File-Sharing:** Google Meet muss es den Nutzern ermöglichen, während einer Besprechung Dateien gemeinsam zu nutzen bzw. zu teilen.

- **Bildschirmfreigabe:** Google Meet muss es den Nutzern ermöglichen, ihren Bildschirm während einer Besprechung gemeinsam zu nutzen.

3 Nichtfunktionale Sicherheitsanforderungen

Die nichtfunktionalen Sicherheitsanforderungen an Google Meet bauen auf den funktionalen Anforderungen auf und decken die zugrundeliegenden Sicherheitsmechanismen ab. Sie benennen die konkreten Aspekte die Software-Entwickler bei der Umsetzung der obigen Anforderungen in einem System berücksichtigen müssen. Bei der Formulierung von nichtfunktionalen Sicherheitsanforderungen stehen einige Möglichkeiten zur Verfügung:

3.1 Verschiedene Vorgehensweisen

3.1.1 Evil User Stories

Evil User Stories sind ein Mittel, um potenzielle Sicherheitsbedrohungen zu identifizieren, indem man aus der Perspektive eines böswilligen Nutzers (bzw. Angreifers) denkt. Diese Methode hilft Software-Entwicklern, Schwachstellen im System zu erkennen und entsprechende Gegenmaßnahmen zu planen. Diese folgen in der Regel der Struktur:

> "Als [böswilliger Akteur] möchte ich [schädliche Aktion], um [negativen Effekt] zu erreichen."

Ein Beispiel für diese Vorgehensweise könnte sein:

> "Als Angreifer möchte ich unverschlüsselte Daten abfangen, um vertrauliche Informationen zu stehlen."

3.1.2 Sicherheits-Akzeptanzkriterien

Sicherheits-Akzeptanzkriterien sind spezifische, messbare Bedingungen, die erfüllt sein müssen, damit ein Sicherheitsfeature als erfolgreich implementiert gilt. Diese Kriterien helfen dabei, sicherzustellen, dass die Sicherheitsanforderungen korrekt und vollständig umgesetzt wurden.

Ein Beispiel für diese Vorgehensweise könnte sein:

> "Alle Datenübertragungen müssen mit mindestens mit AES-256 verschlüsselt sein."

3.1.3 Sicherheitsspezifische Anforderungen

Sicherheitsspezifische Anforderungen sind detaillierte, konkrete Anforderungen, die Sicherheitsmechanismen und -verfahren beschreiben, um das System vor Bedrohungen zu schützen. Diese Anforderungen sind spezifisch und oft technischer Natur.

Ein Beispiel für diese Vorgehensweise könnte sein:

> "Implementiere HMAC für alle Nachrichten, um ihre Integrität sicherzustellen"

3.2 Auflistung der nichtfunktionale Sicherheitsanforderungen

	Sicherheits-Akzeptanzkriterien	**Sicherheitsspez. Anforderungen**
Authentifizierung	Die Verfahren zur Benutzerauthentifizierung müssen einen Penetrationstest bestehen, um die Robustheit der Multi-Faktor-Authentifizierung zu überprüfen.	Alle Authentifizierungen müssen durch eine Multi-Faktor-Authentifizierung geschützt sein. Passwörter müssen mit einer dem Industriestandard entsprechenden Verschlüsselung (z. B. bcrypt) gespeichert werden.
Datenübertragung	Alle Datenübertragungen müssen mit einem Netzwerkprotokoll-Analysator validiert werden, um sicherzustellen, dass die Verschlüsselungsstandards eingehalten werden.	Alle zwischen den Clients und dem Server übertragenen Daten müssen mit TLS 1.2 oder höher verschlüsselt werden.
Zugangskontrolle	Die Zugriffskontrollmechanismen müssen anhand rollenbasierter Zugriffsszenarien getestet werden, um eine ordnungsgemäße Durchsetzung sicherzustellen. Unerlaubte Zugriffsversuche müssen protokolliert und während eines Audits überprüft werden.	Die Nutzer dürfen nur auf Sitzungen zugreifen, zu denen sie ausdrücklich eingeladen wurden. Es muss eine rollenbasierte Zugriffskontrolle (RBAC) implementiert werden, um den Zugriff auf Verwaltungsfunktionen zu beschränken.
Datenschutz	Die Verschlüsselung von Besprechungsaufzeichnungen muss durch unbefugte Zugriffsversuche überprüft werden.	Sitzungsaufzeichnungen müssen verschlüsselt und sicher gespeichert werden und nur autorisierten Benutzern zugänglich sein.
Protokollierung	Die Protokolle müssen monatlich überprüft werden, um sicherzustellen, dass sie detailliert und gegen Manipulationen geschützt sind. Automatisierte Tools müssen die Protokolle auf verdächtige Aktivitäten überwachen, wobei Warnungen innerhalb von 24 Stunden überprüft werden müssen.	Jeder Zugriff auf sensible Informationen und jede Aktion muss protokolliert und auf verdächtige Aktivitäten überwacht werden. Die Protokolle sind vor Manipulationen zu schützen und mindestens ein Jahr lang sicher aufzubewahren.
Notfallmanagement	Vierteljährlich muss eine Übung zur Reaktion auf Zwischenfälle durchgeführt werden, über die ein Bericht erstellt und auf ihre Wirksamkeit überprüft wird.	Google Meet muss über einen Plan zur Reaktion auf Zwischenfälle verfügen, der Verfahren zur Erkennung, Meldung und Behebung von Sicherheitsvorfällen enthält.

4 Vergleich und Präferenz

Sicherheitsspezifische Anforderungen bieten Software-Entwicklern klare und umsetzbare Schritte zur Implementierung von einzelnen Sicherheitsmaßnahmen. Sie sind spezifisch und können leicht in die Entwicklung integriert werden, allerdings kann es ihnen an Kontext fehlen und sie können manchmal zu präskriptiv sein, was weniger Raum für Flexibilität lässt.

Sicherheits-Akzeptanzkriterien bieten den Vorteil, dass sie sich auf die Ergebnisse und überprüfbaren Bedingungen konzentrieren. Sie gewährleisten, dass die implementierten Maßnahmen wirksam sind, anstatt eine konkrete Implementierung vorzuschreiben. Außerdem bieten sie eine Möglichkeit, bzw. ein klares Szenario, diese Maßnahmen zu testen.

Ich persönlich bevorzuge den Einsatz von Sicherheits-Akzeptanzkriterien, weil sie einen klaren Rahmen für die Überprüfung der Wirksamkeit von Sicherheitsmaßnahmen bieten. Dieser Ansatz stellt sicher, dass die Sicherheit nicht nur implementiert, sondern auch getestet und validiert wird, wodurch die Sicherheit des Systems besser gewährleistet werden kann und das System allgemein robuster wird.

5 Testszenarien

Mithilfe von verschiedenen Testszenarien lässt sich eine bessere Sicherheit für das Gesamtsystem sicherstellen. Die Verwendung von Sicherheits-Akzeptanzkriterien ist hier sehr dienlich, da diese eine konkrete Ableitung eines Testszenarios zulassen.

Um diese Ausarbeitung in einem angemessenen Umfang zu halten habe ich untenstehend zwei Szenarien je definierter nichtfunktionaler Sicherheitsanforderung aus dem zweiten Abschnitt erarbeitet:

Authentifizierung

> Nach mehrfachen Versuchen, sich mit falschen MFA-Codes zu authentifizieren muss sichergestellt werden, dass die Mechanismen zur Kontosperrung ausgelöst wurden.
>
> Versuch die gespeicherten Passwörter zu knacken, um die Stärke der Verschlüsselung zu überprüfen.

Sicherheit der Datenübertragung

> Unter Verwendung eines Netzwerk-Analysetools wie z.B. Wireshark – das Datenübertragungen abfangen und überprüfen kann – muss verifiziert werden, ob alle Daten verschlüsselt sind.
>
> Versuch die TLS-Version herabzustufen und anschließende Überprüfung, ob das System die Verbindung ablehnt.

Zugangskontrolle

> Versuchen, auf ein Meeting ohne Einladungslink zuzugreifen. Es muss sichergestellt werden, dass der Zugang verweigert wird.
>
> Durchführung eines Tests mit verschiedene Benutzerrollen, um sicherzustellen, dass die Berechtigungen korrekt durchgesetzt werden.

Datenschutz

Versuch, unbefugten Zugriff auf verschlüsselte Besprechungsaufzeichnungen zu erhalten mit anschließender Übprüfung, dass der Zugriff verweigert wird.

Protokollierung und Überwachung

Generierung von Sicherheitsereignissen (z.B. durch fehlgeschlagene Anmeldeversuche, Datei-Uploads usw.) mit anschließender Überprüfung, ob diese korrekt protokolliert werden.

Test des Überwachungssystems, indem verdächtige Aktivitäten simuliert werden mit anschließender Überprüfung, dass Warnungen generiert und darauf reagiert wird.

Notfallmanagement

Durchführung eines simulierten Sicherheitsverstoßes und anschließende Befolgung des Reaktionsplans, um dessen Wirksamkeit sicherzustellen.

Überprüfung des Berichts über die Reaktion auf einen Vorfall, um sicherzustellen, dass alle Schritte befolgt wurden, und um Bereiche mit Verbesserungsbedarf zu ermitteln.