Computer Security Symposium 2020
26 - 29 October 2020

日本版 App Store で公開されている iOS アプリの SSL 証明書検証不備に関する調査

岡澤 佳寛 [1,*]　白井 優武 [1]　小林 晴貴 [1]　齊藤 泰一 [2]

概要：モバイルアプリにおける証明書検証不備脆弱性，ホスト名検証不備脆弱性は，攻撃者が用意した偽アクセスポイントにアクセスしてしまうことにより，中間者攻撃に悪用されることがある．これらの脆弱性の Android アプリに対する調査がいくつか行われている．例えば，CERT Tapioca のような大規模調査が可能なツールが開発されている．池田らは，Google Play の日本向けの Android アプリに対して証明書検証不備脆弱性，ホスト名検証不備脆弱性の調査を行っている．本稿では iOS アプリに対して証明書検証不備脆弱性，ホスト名検証不備脆弱性の調査を行った．日本向けの App Store でダウンロードとインストールが可能な iOS アプリを調査対象とする．さらにこれらの脆弱性がないアプリがユーザに伝えるエラーメッセージについても分類し議論する．

キーワード：証明書検証不備，ホスト名検証不備，iOS アプリ，SSL/TLS

A Survey on Improper Certificate Validation in iOS Apps released in Japanese version of App Store

Yoshihiro Okazawa[1,*]　Masatake Shirai [1]　Haruki Kobayashi[1]　Taiichi Saito[2]

Abstract: In mobiles apps, vulnerabilities of improper certificate validation(CWE-295) and improper validation of certificate with host mismatch(CWE-297) may be exploited for man-in-the-middle attacks by connecting fake wireless access points installed by attackers. There have been several surveys on these vulnerabilities of Android apps, and large-scale assessment tools such as CERT Tapioca have been developed. Ikeda et al. are surveying these vulnerabilities in Google Play Android apps for Japan. In this paper, we survey iOS apps downloaded from the App Store for Japan. Furthermore, we classify and discuss the error messages that non-vulnerable apps show to users.

Keywords: Improper Certificate Validation, Improper Validation of Certificate with Host Mismatch, iOS App, SSL/TLS

1. はじめに

近年，モバイル端末による公衆無線 LAN の利用が増加している．政府は，災害時の連絡や教育への利用，オリンピックの観光客増加への対応などを目的に公衆無線 LAN の増設を目指している[1]．一方，公衆無線 LAN の普及に伴ってセキュリティ上の脅威が高まりつつあると考えられる．脅威の一つとして，攻撃者が設置する不正なアクセスポイントにモバイル端末が接続することによって行われる中間者攻撃が挙げられる．ここでの中間者攻撃とは，クライアントとサーバ間の通信を不正なアクセスポイントが中継することで通信内容の改ざんや盗聴が行われることである．

中間者攻撃への対策としては，モバイルアプリは，SSL/TLS プロトコルを用い，ルート証明書からサーバ証明書へ至る証明書チェーンを検証することで，中間者である攻撃者の不正な証明書を検知し通信を停止することができる．しかし，実装における SSL 証明書検証不備の脆弱性がモバイルアプリでは数多く存在していることが知られている．そして，日本向けの iOS モバイルアプリに対する SSL 証明書検証に関する調査はほとんど行われていない．

本稿では Apple が公開している日本向けの iOS モバイルアプリを複数ジャンルから選びそれらに対してプロキシを用いた動的方法により SSL 証明書検証不備脆弱性の調査を行った結果を報告する．さらに，SSL 証明書検証不備脆弱性が存在しないアプリに関してもどのようなエラーメッセージを表示するのか調査し分類する．

1.1 SSL 証明書に関する脆弱性

戸田[2]によると，中間者攻撃で用いられる SSL 証明書検証不備脆弱性は 2 つに分類される．

一つは“証明書検証不備”脆弱性である．これは通信先のサーバ証明書がモバイル端末が信頼していない認証局から発行されたものであっても，その証明書をアプリが適切に検証をしないことによって，正しい証明書として誤認する脆弱性である．これにより不正なアクセスポイントの SSL プロキシとしての動作を検出できず，中間者攻撃による通信内容の盗聴・改ざんを許してしまう．Improper Certificate Validation (CWE-295)[3]ともよばれている．

1 東京電機大学大学院 工学研究科
Graduate School of Engineering, Tokyo Denki University
2 東京電機大学 工学部
School of Engineering, Tokyo Denki University

もう一つは“ホスト名検証不備”脆弱性である．これはアプリ側が適切な検証を行わない事によって，サーバ証明書のサーバ名と，アプリがアクセスするホスト名が異なることを検出できないというものである．これにより攻撃者がSSL プロキシとしての動作すること，あるいは攻撃者が偽サイトにリダイレクトしアプリと偽サイトとの HTTPS 通信をさせることを可能にする．Improper Validation of Certificate with Host Mismatch(CWE-297)[4]ともよばれている．

2. 関連研究

2.1 モバイルアプリの証明書検証不備

Fahl ら[5], Dormann[6], Sounthiraraj ら[7]などの研究では，自動化されたツールを開発し，Android アプリの証明書の検証に関わる脆弱性について大規模調査を実施している．

一方，Fahl ら[8]は，手動で 1,009 個の iOS アプリを調査し，それらのアプリに対してプロキシを用いて中間者攻撃を行っている． 通信を行う 884 個のアプリがあり，そのうち 82 個が http 通信を使用して機密情報を転送していた．また，SSL を利用するアプリが 697 個あったが，そのうち 98 個が証明書検証を正しく実装しておらず、中間者攻撃が可能だった．中間者攻撃に対して脆弱でなかった 599 個のアプリのうち，312 個のアプリがユーザに警告メッセージを表示し，58 個のアプリが SSL 証明書に問題があったことを示す警告メッセージを表示したが，254 個は状況を適切に説明していない警告メッセージを表示した．287 個のアプリはハングアップするか，クラッシュした．

2.2 SSL/TLS ライブラリの証明書検証不備

Georgiev ら[9]，Brubaker ら[10]は証明書を取り扱うライブラリの脆弱性について調査している．

Fahl ら[8]は iOS で用いられるフレームワークと証明書検証不備の関係を論じている．iOS アプリの証明書検証不備脆弱性は SSL ライブラリの不備に起因する可能性があると指摘している．福本[11]は，iOS そのものにサーバ証明書検証をバイパスさせる API が用意されているため，iOS アプリの証明書検証不備脆弱性が発生することを指摘している．

2.3 Certificate Pinning とホスト名検証不備

Sounthiraraj ら[7]は Certificate Pinning を行っていてもホスト名検証不備が発生する可能性があることを指摘している．

Certificate Pinning でルート証明書や中間 CA 証明書が固定されているとき，動的にホスト名検証不備脆弱性をテストするには、固定されている証明書の認証局にテスタが管理するホストに対する証明書を発行してもらう必要がある．そのような証明書を用いて，Chothia ら[12]は英国の大手銀行が提供するモバイルアプリのホスト名検証不備脆弱性を発見した．

一方，Stone ら[13]は，固定された証明書を証明書チェーンに含むような証明書を持つ一般のサイトにトラフィックをリダイレクトし SSL/TLS ハンドシェイクをさせることによりホスト名検証不備脆弱性をテストしている．

ここまで，Android アプリを中心とする関連研究を述べてきたが，iOS アプリに関する証明書検証不備の調査は少ない．

3. 調査内容

調査対象の選定には池田ら[14]の調査に倣い，「多くのユーザが利用するアプリを選定するために無料でダウンロード可能で」，Apple が提供するカテゴリ別のランキングにリストされているという条件を用いる．また，インターネットに接続した状態での使用が必須で，アプリの言語が日本語または英語であるものとする．本稿では条件に該当するアプリのジャンルに，銀行，フード・ドリンク，ショッピング，ブラウザの 4 つのジャンルとした．

4. 実験環境

今回の調査を行うにあたり，中継用 PC 上にプロキシを導入し，モバイル端末からの通信がプロキシを経由してインターネットへ接続する環境を構築した．図 1 に実験環境を示す．なお，実験環境の作成にあたり，[15]の構成を参考にした．モバイル端末には iPhoneXR(iOS 13.5.1)を使用し，プロキシには Burp Suite Professional を使用した．

実験では，調査対象アプリの http，及び https 通信をプロキシ上で傍受し，証明書検証不備及びホスト名検証不備を調査した．iOS 上のモバイル端末が中継用 PC を経由させるために iOS のプロキシ設定を用いる．プロキシ設定には，中継する PC の IP アドレスとポート番号を入力する． 証明書検証不備の調査では，iOS 端末に Burp Suite プロキシのルート証明書をインストールしない状態で実験を行う．またホスト名検証不備の調査では，ルート証明書をインストールした状態で検査を行い，事前に Burp Suite プロキシのサーバ証明書のホスト名を変更した．

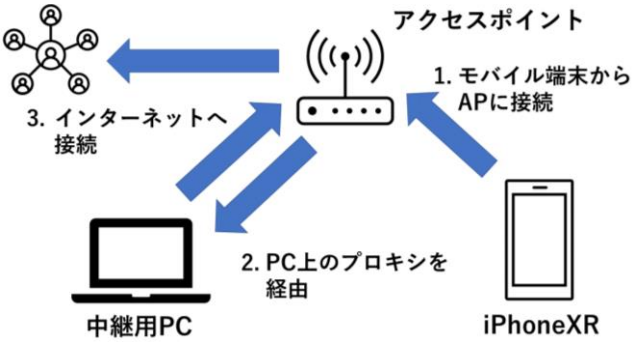

図 1 実験環境

5. 調査結果

調査結果について，アプリのジャンルごとに結果を示す．また，表 1 - 4 までに記載している各エラーメッセージの詳細は付録で記述する．

5.1 ショッピング系アプリ

5.1.1 SSL 証明書検証不備

ショッピング系アプリに関しては App Store のショッピングカテゴリ内の調査条件に当てはまる 183 件を調査対象とした．調査の結果，14 件のアプリに SSL 証明書検証不備脆弱性を確認した．これは調査対象全体の約 7.7%を占めている．また，証明書検証不備脆弱性およびホスト名検証不備脆弱性の両方を持つアプリは 14 件であった．また，不正な証明書を検証した際に，エラーメッセージを表示するが SSL 通信を行ったアプリが 3 件あった．

5.1.2 エラーメッセージの分類

調査対象である 183 件のアプリの内，102 件はエラーメッセージを表示しなかった．残りの 81 件のアプリについて，エラーメッセージの内訳を表 1 に示す．

5.2 銀行系アプリ

5.2.1 SSL 証明書検証不備

銀行系アプリに関しては調査条件に当てはまる 139 件のアプリを調査対象とした．調査の結果，12 件のアプリに SSL 証明書検証不備脆弱性を確認した．これは調査対象アプリの約 8.6%を占めている．12 件のアプリのうち，すべてのアプリが証明書検証不備脆弱性及びホスト名検証不備脆弱性の脆弱性を抱えていた．

5.2.2 エラーメッセージの分類

調査対象である 139 件から，脆弱性のある 12 件を除いた 127 件の内，63 件はユーザに対してメラ―メッセージを示さなかった．残りの 64 件で発生したエラーメッセージの内訳を表 2 に示す．

5.3 ブラウザ系アプリ

5.3.1 SSL 証明書検証不備

ブラウザ系アプリに関しては 86 件のアプリを調査対象とした．8 件のアプリに関して SSL 証明書検証不備脆弱性を確認した．これは全調査対象アプリの約 9.3%を占めている．8 件の内，すべてのアプリが証明書検証不備脆弱性，ホスト名検証不備脆弱性を抱えていた．また，8 件の内，5 件は不正な証明書の検証時，エラーメッセージを表示しても，SSL 通信を行うアプリがあった．

5.3.2 エラーメッセージの分類

調査対象である 86 件の内，55 件のアプリはユーザに対してエラーメッセージを示さなかった．残りの 31 件で発生したエラーメッセージの内訳を表 3 に示す．

表 1. エラー分類（ショッピング系）

エラーメッセージ	件数(件)
証明書エラー	6
通信エラー	30
ネットワークエラー	11
データ取得エラー	7
読み込みエラー	6
メンテナンスエラー	3
SSL エラー	2
初期化処理エラー	2
更新チェックエラー	1
システムエラー	1
処理エラー	1
想定外エラー	1
位置情報エラー	0
ログインエラー	0
検索エラー	0
タイムアウトエラー	0
その他	10

表 2. エラー分類（銀行系）

エラーメッセージ	件数(件)
証明書エラー	2
通信エラー	25
処理エラー	10
システムエラー	7
更新チェックエラー	4
ネットワークエラー	3
想定外エラー	2
タイムアウトエラー	1
初期化処理エラー	0
データ取得エラー	0
SSL エラー	0
位置情報エラー	0
ログインエラー	0
検索エラー	0
読み込みエラー	0
メンテナンスエラー	0
その他	10

5.4 フード・ドリンク系アプリ

5.4.1 SSL 証明書検証不備

App Store アプリのフード・ドリンクカテゴリ内にある 200 件のアプリ，検索機能でリストしたアプリ，合計 203 件を調査対象とした．その中で 60 件のアプリが条件に該当しなかった．これらを除外した 143 件のアプリの内，7 件のアプリに SSL 証明書検証不備脆弱性を確認した．これは全体の約 4.9%を占めている．証明書検証不備脆弱性およびホスト名検証不備脆弱性の両方を持つアプリは 7 件であった．

5.4.2 エラーメッセージ分類

調査対象である 143 件の内，脆弱性のある 7 件を除いた 136 件について SSL 証明書検証時に発生したエラーメッセージの分類を行う．136 件中，60 件はユーザに対してメラ―メッセージを示さなかった．よって残りの 76 件で発生したエラーメッセージの内訳を表 4 に示す．

6. 考察

6.1 各ジャンルのアプリの SSL 証明書検証不備

今回の調査の結果，全てのジャンルのアプリに共通して脆弱性が確認されたアプリには，証明書検証不備とホスト名検証不備の両方の脆弱性があった．これは，開発者が証明書の検証の部分を独自に開発していた場合，証明書検証の 2 つの処理の内，片方の処理を適切に実装していることを確認すれば，もう片方の処理の実装不備を見落とす可能性は低いと思われる．

6.2 エラーメッセージに関する考察

証明書検証時にエラーメッセージを表示したアプリの割合は銀行系，ブラウザ系，フード・ドリンク系，ショッピング系の順で，それぞれ約 50%，約 36%，約 56%，約 44%であり，いずれも割合が高いとは言えない．証明書に関するエラーメッセージは銀行系，ブラウザ系，フード・ドリンク系，ショッピング系では，ブラウザ系を除き，1 割以下であった．一方で，ブラウザ系を除いた全てのジャンルで証明書検証時に通信エラーとして表示される割合が高いことが判明した．考えられる原因として，開発者が証明書に関するエラーを通信エラーにまとめている可能性がある．あるいは，証明書検証の実装不備による中間者攻撃を考慮していない場合も考えられる．証明書検証が適切に実装されていれば，証明書検証エラー時にエラーメッセージを表示する必要はないと思われる．

しかし，実際にユーザが偽アクセスポイントに接続している場合は，アプリが証明書に関するエラーを表示することにより，攻撃を受けていることをユーザに気付かせることが出来れば，接続している偽アクセスポイントをユーザに切り替えさせ中間者攻撃を回避させることが可能かもしれない．

表 3.　エラー分類（ブラウザ系）

エラーメッセージ	件数(件)
証明書エラー	10
SSL エラー	7
通信エラー	4
ネットワークエラー	2
検索エラー	1
読み込みエラー	1
初期化処理エラー	0
データ取得エラー	0
位置情報エラー	0
更新チェックエラー	0
システムエラー	0
想定外エラー	0
ログインエラー	0
タイムアウトエラー	0
処理エラー	0
メンテナンスエラー	0
その他	6

表 4.　エラー分類（フード・ドリンク系）

エラーメッセージ	件数(件)
証明書エラー	4
通信エラー	22
ネットワークエラー	14
初期化処理エラー	12
データ取得エラー	8
SSL エラー	5
位置情報エラー	2
更新チェックエラー	2
システムエラー	1
想定外エラー	1
ログインエラー	1
検索エラー	0
読み込みエラー	0
タイムアウトエラー	0
処理エラー	0
メンテナンスエラー	0
その他	4

表 5 ジャンル別の SSL 証明書検証不備

ジャンル	調査対象数	証明書検証不備	ホスト名検証不備	証明書検証不備 かつ ホスト名検証不備
ショッピング系	183	14	14	14
銀行系	139	12	12	12
フード・ ドリンク系	143	7	7	7
ブラウザ系	86	8	8	8

6.3 Certificate Pinning と調査の関係

アプリが Certificate Pinning によりルート証明書あるいは中間 CA 証明書を固定している場合，ホスト名が異なるサーバ証明書を用いてホスト名検証不備を確認するためには，そのサーバ証明書に至るための証明書チェーンが固定されている証明書を含む必要がある．この証明書を含まない場合にはサーバ証明書は受理されない．本稿の調査ではアプリが Certificate Pinning を使用しているか調べていないため，ホスト名検証不備を見逃している可能性がある．また，アプリが生成するエラーメッセージが Certificate Pinning に由来する可能性がある．

7. まとめ

日本国内向けの App Store で公開されている iOS アプリに対して SSL 証明書検証不備脆弱性に関する調査を行った．また，検証に失敗した場合に表示されるエラーメッセージについても調査した．今後は，調査するアプリのカテゴリの範囲を拡げるほか，証明書検証やホスト名検証だけでなく，証明書の有効期限についても調査を行う．

なお，今回の調査で確認された脆弱性を持つアプリは，情報セキュリティ早期警戒パートナーシップガイドライン[16]に基づき，IPA，JPCERT/CC ならびにアプリ開発者に対して順次報告中である．

参考文献

[1] 総務省, 2020 年に向け全国約３万箇所の Wi-Fi 整備を目指して, https://www.soumu.go.jp/main_content/000548781.pdf, (参照 2020-8-19)

[2] 戸田洋三, 〜誰かの失敗を他山の石に〜脆弱性事例に学ぶセキュアコーディング「SSL/TLS 証明書検証」編, JavaDayTokyo2015, https://www.slideshare.net/jpcert_securecoding/cert-verifjavadaytokyo2015, (参照 2020-08-19)

[3] CWE, CWE-295: Improper Certificate Validation, https://cwe.mitre.org/data/definitions/295.html, (参照 2020-8-19)

[4] CWE, CWE-297: Improper Validation of Certificate with Host Mismatch, https://cwe.mitre.org/data/definitions/297.html, (参照 2020-8-19)

[5] Fahl, S., Harbach, M., Muders, T., Baumgärtner, L., Freisleben, B., Smith, M., “Why eve and mallory love android: an analysis of android ssl (in) security”, *Proceedings of the 2012 ACM Conference onComputer and Communications Security*, pp. 50‑61.

[6] Will Dormann, Finding Android SSL Vulnerabilities with CERT Tapioca, CERT/CC BLOG, https://insights.sei.cmu.edu/cert/2014/09/-finding-android-ssl-vulnerabilities-with-cert-tapioca.html, (参照 2020-8-19)

[7] Sounthiraraj, D., Sahs, J., Greenwood, G., Lin, Z., Khan, L., “Smv-Hunter: large scale, automated detection of ssl/tls man-in-the-middle vulnerabilities in android apps”, *Proceedings of the 21th Network and Distributed System Security Symposium*.

[8] Fahl, S., Harbach, M., Perl, H., Koetter, M., Smith, M., “Rethinking SSL development in an appified world.”, *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*.

[9] Martin Georgiev, Subodh Iyengar, Suman Jana, Rishita Anubhai, Dan Boneh, and Vitaly Shmatikov , ”The Most Dangerous Code in the World: Validating SSL Certificates in Non-Browser Software”, *Proceedings of the 2012 ACM conference on Computer and communications security*.

[10] Chad Brubaker, Suman Jana, Baishakhi Ray, Sarfraz Khurshid, and Vitaly Shmatikov, “Using Frankencerts for Automated Adversarial Testing of Certificate Validation in SSL/TLS Implementations”, *Proceedings of 2014 IEEE Symposium on Security and Privacy*

[11] 福本郁哉, iOS アプリセキュアコーディング入門, https://www.jssec.org/dl/20160323_Ikuya_Fukumoto.pdf, (参照 2020-8-19)

[12] Chothia, T., Garcia, F., Heppel, C., and McMahon Stone, C. "Why banker Bob (still) can’t get TLS right: A Security Analysis of TLS in Leading UK Banking Apps", *Financial Cryptography and Data Security: 21st International Conference*, pp. 579-597.

[13] Stone, C.M., Chothia, T., and Garcia, F.D, “Spinner: Semi-Automatic Detection of Pinning without Hostname Verification”, *Proceedings of the 33rd Annual Computer Security Applications Conference*.

[14] 池田 康平, 中村大, 徳生紳之介, 中原黎, 白井優武, 小林 晴貴, 齊藤 泰一, "日本における Android アプリの SSL 証明書検証不備脆弱性の調査", *Proceedings of 2020 Symposium on Cryptography and Information Security*.

[15] SST 株式会社セキュアスカイ・テクノロジー, SST なるほど！コーナー 04 Android で HTTP プロキシを使ってみよう！, https://www.securesky-tech.com/column/naruhodo/04.html, (参照 2020-8-19)

[16]（独）情報処理推進機構, 情報セキュリティ早期警戒パートナーシップガイドライン, https://www.ipa.go.jp/files/000073901.pdf, (参照 2020-8-20)

付録

エラーメッセージの種別

・証明書エラー

アプリが証明書検証時のエラーである．エラーメッセージに証明書に関する単語が含まれているものを示す．

・通信エラー

通信時に発生するエラーである．エラーメッセージに”通信”などの単語が含まれているものを示す．

・ネットワークエラー

ネットワーク接続時に発生するエラーである．エラーメッセージに”ネットワーク”などの単語が含まれているものを示す．

・初期化処理エラー

アプリが起動した際に初期化処理を行う時に発生するエラーである．エラーメッセージに”初期化処理”という単語が含まれているものを示す．

・データ取得エラー

アプリがデータを取得する際に発生するエラーである．エラーメッセージに”取得”などの単語が含まれているものを示す．

・SSL エラー

アプリが SSL 通信時に発生するエラーである．エラーメッセージに”SSL”という単語が含まれているものを示す．

・位置情報エラー

アプリが位置情報を入手する際に発生するエラーである．エラーメッセージに”位置情報”などの単語が含まれている物を示す．

・更新チェックエラー

アプリが起動した際に，最新のバージョンであるか確認する際に発生するエラーである．エラーメッセージに更新やバージョンなどの単語が含まれる物を示す．

・システムエラー

アプリのシステムに問題が発生した際に発生するエラーである．エラーメッセージに”システム”などの単語が含まれている物を示す．

・想定外エラー

アプリ側が想定していないエラーが発生した際に発生するエラーである．エラーメッセージに”想定外”などの単語が含まれている物を示す．

・ログインエラー

ログインをする際に発生するエラーである．エラーメッセージに”ログイン”などの単語が含まれている物を示す．

・検索エラー

アプリに検索機能があり，それを用いて検索した際に発生するエラーである．エラーメッセージに”検索”などの単語が含まれている物を示す．

・読み込みエラー

アプリがデータを読み込み際に発生するエラーである．エラーメッセージに”読み込み”が含まれている物を示す．

・タイムアウトエラー

アプリがタイムアウトを起こした際に発生するエラーである．エラーメッセージに”タイムアウト”が含まれている物を示す．

・処理エラー

エラーメッセージに”処理エラー”という単語が含まれている物を示す．

・メンテナンスエラー

エラーメッセージに”メンテナンス”という単語が含まれている物を示す．

Certificate Pinning とホスト名検証不備

iOS を含む各オペレーティングシステムは，信頼のおけるはずのルート証明書のリストを持ち，それらのルート証明書からはじまる正しい証明書チェーンを信用する．しかし，いずれかのルート証明書の認証局が（侵害されたり騙されたりミスを犯したりして),攻撃者が管理していないサーバに対するサーバ証明書を発行し，攻撃者に与えてしまう可能性がある．中間 CA 証明書についても同様である．またマルウェアやソーシャルエンジニアリングにより，攻撃者の作成したルート証明書をリストに加えてしまう可能性もある．これらの手段が成功すると，攻撃者は，そのサーバのなりすましや，中間者としてのそのサーバとの通信の傍受・改ざんができるようになる．このようなリスクに対処するために Certificate Pinning がある．モバイルアプリにおける Certificate Pinning は，アプリが使用する証明書を固定することであり，それにより攻撃者の証明書を利用させなくすることができる．

Certificate Pinning の実装の方法としては，モバイルアプリがサーバ証明書や公開鍵を格納しそれのみを利用する方法と，ルート証明書や中間 CA 証明書を固定しそれを含む証明書チェーンのみを利用する方法がある．

アプリが SSL/TLS 通信を初めて行うときに得た証明書を信用し固定する方法もあるが，攻撃者が証明書を固定してしまう可能性がある．そのため Web アプリケーションでは Certificate Pinning が使われなくなってきている．

本稿の実験では，サーバ証明書が元々アクセスするはずのホスト名と異なるサーバ名（Common Name か Subject Alternative Name）を持っているが，ルート証明書からのサーバ証明書までの証明書チェーンが"署名"検証に成功するという状況を作り，そのときにアプリがエラーを出力せずに通信が継続される時にアプリはホスト名検証不備脆弱性を持つと判断する．

しかし，アプリの Certificate Pinning 機能によりルート証明書あるいは中間 CA 証明書が固定されている場合は，それらが証明書チェーンに含まれない時にエラーを出力する．そのため，ホスト名検証不備の検証の際に，Certificate Pinning によるエラーが出力されてしまう可能性がある．

また，このような Certificate Pinning のもとにホスト名検証不備が存在した場合に，攻撃者が，固定されたルート証明書か中間 CA 証明書を証明書チェーンに含むような自分の管理するサーバ名に対するサーバ証明書を正規の方法で手に入れることにより, 中間者攻撃が可能になってしまう.