Hochschule für Technik
und Wirtschaft Berlin
University of Applied Sciences

Ein aussagekräftiger Titel

Belegarbeit im Modul Informationssicherheit

vorgelegt von

Fatih Görgülü Matrikelnr.
Jakob Heiner-Scharf Matrikelnr.
Maik Peters Matrikelnr.
Eddy Klammer Matrikelnr.
Ägidius Haslauer 585016.

Berlin, 18. Mai 2024

Abstract

Der Method Confusion Angriff stellt einen Man-in-the-Middle (MITM) Angriff dar, der während des Verbindungsaufbaus über Bluetooth zwischen mehreren Geräten durchgeführt werden kann. Dieser Angriff nutzt eine Schwachstelle der Pairing Methoden aus, welche für einen Verbindungsaufbau mittels Bluetooth benötigt werden. Die Funktionsweise des Angriffs und der Pairing Methoden wird im folgenden weiter erläutert.
Der Angriff bietet dabei Risiken für die Nutzer von Bluetooth, welche in dieser Arbeit behandelt werden. Zudem werden Schutzmaßnahmen erläutert, welche die Benutzer vor diesem Angriff schützen können.

Schlüsselwörter

Bluetooth, MITM, Sicherheitsrisiken, Sicherheitsmaßnahmen

Inhaltsverzeichnis

1 Einleitung

Bluetooth ist eine Technologie, die eine drahtlose Kommunikation zwischen mehreren technischen Geräten ermöglicht. Seit der Entwicklung der Technologie der Bluetooth Special Industry Group (SIG) in 1998 hat sich Bluetooth zu einem weit verbreiteten Standard für die Kommunikation zwischen Geräten auf kurzer Reichweite entwickelt. [1] Dies zeigt sich dadurch, dass die Anzahl der verkauften Geräte weltweit, welche Bluetooth verwenden, in 2022 eine Summe von 4.9 Milliarden Geräten betrug. [2] Die Anwendungsfelder von Bluetooth sind dabei sehr vielfältig. Die Technologie wird in kabellosen Kopfhörern, in Autos oder auch in Smart-Home Geräten verwendet. [3]
Aufgrund dieser weiten Verbreitung ist es wichtig, dass diese Technologie die entsprechenden Sicherheitsmaßnahmen mitbringt, sodass die Nutzer vor potenziellen Sicherheitsrisiken geschützt sind und die Technologie weiterhin verlässlich verwenden können.
Dennoch gibt es neue Angriffsmethodiken, die darauf abzielen die Schwachstellen dieser Technologie auszunutzen um unbefugten Zugriff auf verbundene Geräte zu erlangen, Daten abzufangen, Daten zu manipulieren oder andere schädliche Aktionen durchzuführen. [3]
Ein Beispiel für einen solchen Angriff ist die Method Confusion Attack, bei dem der Angreifer eine man in the middle (MITM) Position erlangt und sich dadurch unerlaubten Zugriff auf die übertragenen Daten des Opfers verschafft. Es wurde eine Nutzerstudie mit 40 Teilnehmern durchgeführt, wobei der Angriff bei 37 der 40 Teilnehmer zu einem erfolgreichen Pairing Prozess erfolgte und somit der Angriff erfolgreich abgeschlossen wurde. Keiner der Teilnehmenden hat den Angriff bemerkt. [4] Der Angriff wird im Folgenden unter den Gesichtspunkten Angriffsmethodik, Risiken und Schutzmaßnahmen genauer betrachtet.

2 Angriffsstrategie

Die Method Confusion Attack ist ein Angriff, bei dem versucht wird, eine MITM Postion zu erlangen. In diesem Abschnitt werden die notwendigen Voraussetzungen und Pairing Methoden des Pairing Prozesses erläutert, welche für eine erfolgreiche Durchführung des Angriffs benötigt werden. Es wird darauf eingegangen, inwiefern eine Verwirrung durch den Angriff entsteht. Abschließend folgt eine Erklärung der bereits angesprochenen MITM Position und wie diese durch die Method Confusion Attack erreicht wird.

2.1 Voraussetzungen

Die Method Confusion Attack benötigt dabei eine Reihe an Voraussetzungen, sodass diese erfolgreich durchgeführt werden kann. Zunächst müssen die Geräte des Ziels einen Verbindungsaufbau initieren, es darf also keine bereits aktive Bluetooth Verbindung der beiden Geräte bestehen.
Zudem muss der Angreifer sich in der Nähe des Ziels, also in der Bluetooth Übertragungsreichweite der Geräte befinden. Die notwendige Reichweite ist dabei sehr stark von den Bluetooth Classes also den Geräten, sowie den äußeren Einflüssen abhängig, weswegen in dieser Arbeit nicht genauer auf diesen Aspekt eingegangen wird.
(Jamming des Signals)
Die beiden Geräte müssen dabei unterschiedliche Pairing Methoden verwenden. Dabei ist wichtig, dass eines der Geräte die Pairing Methode Passkey Entry und das andere Gerät die Methode Numeric Comparison verwendet. Was die einzelnen Pairing Methoden bedeuten wird unter 2.2 erklärt.
(Version) [4, 5]

2.2 Pairing

Ein essentieller Bestandteil des Verbindungsaufbaus ist der Pairing Prozess. Hier werden zunächst die Informationen ausgetauscht, welche benötgt werden um später die Pairing Methode auszuwählen. Zum Beispiel geht es darum, ob ein Gerät eine Anzeigefunktion besitzt oder nicht. Danach werden die öffentlichen Schlüssel beider Geräte ausgetauscht, welche dann wiederum dafür verwendet werden um den Diffie-Hellmann Schlüssel zu berechnen. Basierend auf diesen Schlüssel, welcher auf den ausgetauschten Informationen basiert, wird eine der möglichen Pairing Methoden ausgewählt. Es gibt dabei unterschiedliche Pairing Methoden, welche verwendet werden können und der weitere Pairing Prozess hängt stark von der verwendeten Pairing Methode ab. [6]
Im Folgenden werden lediglich die Methoden Passkey Entry (PE) und Numeric Comparison (NC) betrachtet. Dies hat den Hintergrund, dass die Pairing Methode Just Works hauptsächlich von legacy Geräten verwendet wird, die Sicherheitsmaßnahmen dementsprechend sehr veraltet sind und viele sicherheitstechnische Risiken bestehen. Es existiert kein MITM Schutz, wodurch eine Berücksichtigung der Methode für einen Angriff der auf eine MITM Position abzielt nicht notwendig ist. [3]
Out of Band Pairing (OOB) ermöglicht, dass Entwickler eigene Pairing Mechanismen

implementieren können. Dementsprechend hängen die sicherheitstechnischen Risiken sehr stark von den einzelnen Implementierungen ab. Mit den korrekten Konfigurationen kann OOB aber durchaus einen MITM Schutz bieten, da es nicht auf den MITM Schutz von Bluetooth basieren muss. Eine Berücksichtigung von OOB in den folgenden Abschnitten ist daher nicht sinnvoll, jedoch wird OOB in Abschnitt 4 Schutzmaßnahmen behandelt. [4, 7]

2.2.1 NC

Bei der Numeric Comparison Methode ist es notwendig, dass alle Geräte über ein Display verfügen, da hierbei der gleiche Wert auf allen Geräten angezeigt wird. Der Benutzer wird daraufhin aufgefordert die Werte auf den Geräten zu bestätigen, falls diese übereinstimmen. Wenn dies der Fall ist und der Benutzer das auch bestätigt, gilt der Verbindungsaufbau als erfolgreich und der Pairing Prozess ist damit abgeschlossen. [4]

2.2.2 PE

Die Passkey Entry Methode verwendet ebenfalls einen Wert für den Verbindungsaufbau, dieser ist 6-stellig. Hierbei wird ein Gerät benötigt das über eine Eingabe -und Ausgabefunktionalität verfügt und ein Gerät das einen Display besitzt. Der 6-stellige Wert wird zwischen den Geräten während des Pairing Prozesses ausgetauscht und der Benutzer wird dazu aufgefordert den angezeigten Wert auf dem Display des einen Gerätes in das andere Gerät einzugeben. Wenn beide Werte überprüft wurden und diese auch übereinstimmen, gilt der Verbindungsaufbau als erfolgreich und der Pairing Prozess ist damit abgeschlossen. [4]

2.3 Confusion

Zunächst werden statt einer einzelnen Koppelung zwischen den Geräten des Ziels zwei Kopplungen simultan mit dem Angreifer durchgeführt. Ein Gerät verbindet sich mit dem MitM-Responder (Sitzung 1), und der MitM-Initiator verbindet sich mit dem anderen Gerät (Sitzung 2). Es ist essentiell dabei, dass Sitzung 1 über Numeric Comparison erfolgt und Sitzung 2 über Passkey Entry. Für das Ziel scheint es dann so, als würde lediglich die Methode Passkey Entry zwischen den Geräten durchgeführt werden, da eins der Geräte den Passcode anzeigt (Sitzung 1) und das andere Gerät dazu auffordert (Sitzung 2), einen Passcode einzugeben.
Der Angreifer wartet, bis mittels Numeric Comparison (Sitzung 1) der Passcode angezeigt wird, sodass er diese Information verwenden kann, um diesen Passcode in Sitzung 2 zu verwenden. Damit wird der Benutzer aufgefordert, den angezeigten Passcode aus Sitzung 1 in das andere Gerät in Sitzung 2 einzugeben. Dadurch scheint es für den Benutzer wie ein legitimer Kopplungsversuch der beiden Geräte, aber in Wirklichkeit kontrolliert der Angreifer ab jetzt die Verbindung mit einer entsprechenden Koordination der beiden Verbindungen. [4, 6]
Die Verwirrung des Angriffs entsteht also grundsätzlich dadurch, dass zwei verschiedene

Pairing Methoden verwendet werden und der Benutzer sich dessen nicht bewusst ist. Dass beide Pairing Methoden auf diese Art und Weise für diesen Zweck verwendet werden können, liegt daran, dass ein Passcode mit der gleichen Form in beiden Methoden verwendet wird und auch nicht authentifiziert wird, welche Methoden im Kopplungsversuch verwendet werden. [4]

2.4 MITM

3 Risiken

Der Method Confusion Angriff bietet einige Risiken für die Benutzer von Bluetooth. Im Folgenden werden einige dieser Risiken erläutert und hinsichtlich des potenziellen Schadens und der Wahrscheinlichkeit des Eintretens betrachtet.
Wie eine Nutzerstudie ergeben hat, konnte niemand der Teilnehmer den Angriff bemerken und bei 37 von 40 Teilnehmern wurde der Pairing Prozess erfolgreich abgeschlossen, sodass eine MITM Position erlangt wurde. [4] Aufgrund dieses Ergebnisses, besteht eine große Wahrscheinlichkeit, dass bei einem Angriffsversuch der Angriff erfolgreich ist und der Angreifer unbemerkt bleibt. Die Schäden von MITM Angriffen sind schwer einzuschätzen

4 Schutzmaßnahmen

Um die oben genannten Risiken ausgehend des Method Confusion Angriffs zu minimieren bzw. zu verhindern werden Schutzmaßnahmen benötigt, die eine sichere Nutzung von Bluetooth ermöglichen.

4.1 Maßnahme 1

4.2 Maßnahme 2

5 Fazit

Literatur

[1] C. Bisdikian, "An overview of the bluetooth wireless technology," *IEEE Communications Magazine*, p. 1, 2001. .

[2] F. Laricchia, "Bluetooth device shipments worldwide from 2015 to 2027," 2023. Zuletzt aufgerufen am 15. Mai 2024.

[3] e. a. P. Muraleedharaa, "Any bluetooth device can be hacked. know how?," *sciencedirect*, pp. 1–4, 2024. .

[4] e. a. M. von Tschirschnitz, "Method confusion attack on bluetooth pairing," *IEEE Symposium on Security and Privacy*, pp. 1–5, 2021. .

[5] bluetooth, "Bluetooth reichweite verstehen." Zuletzt aufgerufen am 16. Mai 2024.

[6] e. a. M. K. Jangid, "Extrapolating formal analysis to uncover attacks in bluetooth passkey entry pairing," *NDSS-Symposium*, pp. 2–3, 2023. .

[7] bluetooth, "Bluetooth pairing part 5: Legacy pairing – out of band," 2017. Zuletzt aufgerufen am 16. Mai 2024.