Lautloser Angriff – manipulierte Kommandos können Alexa, Siri und Co. austricksen

Sehr zur Freude ihrer millionenfachen Besitzer erledigen Alexa, Cortana und Google viele hilfreiche Aktionen als Reaktion auf Sprachkommandos. Doch was passiert, wenn ein Angreifer einen Weg finden würde, ihnen etwas zu befehlen, was ihre Hausherren eher nicht möchten?
Forscher sondieren diese Möglichkeit bereits seit ein paar Jahren und nach einem Artikel der New York Times haben Entwickler der Universität Kalifornien, Berkley nun gezeigt, wie das funktionieren kann: Sie entdeckten Möglichkeiten, Kommandos in Audiodateien, wie Sprachaufnahmen oder Musikstreaming, zu verstecken, so dass sie für das menschliche Ohr nicht hörbar sind. Während der Mensch hier etwas Unverfängliches wahrnimmt, interpretiert der virtuelle Assistent dieses als spezifisches Kommando.

Sinfonien für den Menschen, Befehle für die Maschine
Die Forscher demonstrierten, wie dieses Prinzip genutzt werden kann, um die Mozilla DeepSpeach (ein Modell zur Spracherkennung) Sprache-zu-Text-Maschine zu foppen: sie betteten Kommandos direkt in die aufgenommene Musik oder den gesprochenen Text ein. Der menschliche Zuhörer vernimmt ein Gespräch oder ein Orchesterstück – aber Amazons Echo hört möglicherweise eine Instruktion, etwas auf die Shopping-Liste zu setzen.

Wie könnten Angreifer das ausnutzen?
Die naheliegendste Möglichkeit sind manipulierte Audiodateien, verdeckt in einer Radio- oder Fernsehsendung, einem Podcast, YouTube-Video oder Online-Spiel. Oder vielleicht auch einfach eine sich selbst abspielende Audiodatei auf einer Phishing-Webseite.
Welche Kommandos die Betrüger wählen könnten? Mehr oder weniger alles, was das Gerät kann. Vom Wählen einer Telefonnummer, Aufrufen einer Webseite, oder sogar selbstständiges Einkaufen. Beispiel gefällig? Die Berkley-Forscher konnten in der an sich harmlosen Aussage „ohne den Datensatz ist der Artikel nutzlos“ das Kommando „okay, Google, browse zur Seite evil.com“ verstecken. Ein verletzliches Gerät ist damit jedes, das auf Sprachkommandos reagiert. Heutzutage also Sprachassistenten und Smartphones.

Grundproblem: Warum muss eigentlich alles eine Sprachfunktion haben?
Das eigentliche Problem dieses Forschungsergebnisses ist aber ein anderes: nämlich, wie wenig wir darüber wissen, wie Internetfirmen Sprachtechnologien implementieren und welche Schutzmaßnahmen – falls überhaupt – eingebaut sind.
Auf den ersten Blick sind Smartphones schwieriger zu manipulieren, weil sie schlichtweg eine Entsperrung seitens des Besitzers benötigen, bevor der eingebettete digitale Assistent aktiviert wird. Die Sprachassistenten zu Hause mit „Always on“- Funktion sind einfacher anzugreifen. Gleichermaßen gilt die Verletzlichkeit aber so, wie das iPhone seine Bildschirmsperre implementiert – man kann in den Einstellungen ja selbst Funktionen festlegen, wofür man keine Entsperrung benötigt, also Uhrzeit ansehen, Alarme ausstellen, etc. So lässt sich eben auch Siri starten – ohne Auflösung der Bildschirmsperre – und bietet eine mögliche Angriffsfläche. Auch eine Schadfunktion auf Googles Home Mini (Googles kleiner Sprachassistent ähnlich Alexas Echo) ließ diesen alles aufnehmen, was er hörte – auch wenn er danach gar nicht gefragt wurde.

„Die Forschungsergebnisse zeigen zunächst einmal, dass diese Geräte von außen kontrolliert werden können – theoretisch“, ordnet Michael Veit, Security Experte bei Sophos, die Arbeit aus Berkley ein. „Das Risiko, dass der eigene Sprachassistent nun durch versteckte Kommandos manipuliert wird, ist aber als gering einzuschätzen. Viel wahrscheinlicher ist nach wie vor, dass die gegenwärtige Generation an Geräten unbemerkt überwacht wird oder zum Teil ein seltsames Eigenleben führt. Die Beispiele, in denen Alexa und Co. sich selbstständig ins Spiel bringen, sind ja zahlreich. Bedenklich ist aber die Entwicklung, eine Sprachkontrolle in jede Art von Gerät einzubetten, inklusive Haussicherheit und Türverriegelung. Und noch eines sollte einem angesichts dieser Forschungsergebnisse bewusst sein: was in der Theorie möglich ist, wird auch seinen Weg in die Praxis finden. Noch nicht heute, aber vielleicht in ein paar Jahren.“

Pressekontakt

Sophos
Jörg Schindler, PR Manager CEEMEA
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de