KERENTANAN KEAMANAN PADA VOICE ASSISTANT GOOGLE HOME

Muhammad Fiqri Fatriansyah
Program Studi Sistem dan Teknologi Informasi
Sekolah Teknologi Elektro dan Informatika
Institut Teknologi Bandung
Bandung, Indonesia
18217031@std.stei.itb.ac.id

Abstrak

Voice assistant merupakan sebuah teknologi yang memungkinkan pengguna untuk memerintahkan perangkat untuk melakukan berbagai layanan aktivitas dan menjawab segala pertanyaan dari pengguna. Saat *Internet of Things* (IOT) populer, *voice assistant* dikembangkan dan dimanufaktur sedalam-dalamnya sehingga meningkatkan kapabilitas *voice assistant* agar dapat berinterasi balik dengan cara memberikan *feedback* kepada pengguna, salah satunya dengan cara bertanya balik ke pengguna. Contoh *voice assistant* yang saat ini popular di masyarakat adalah Google Home. Namun, banyak orang yang tidak mengetahui tingkat keamanan dan kerentanan dari Google Home. Informasi privat dari pengguna mungkin dapat diakses tanpa sepengetahuan pengguna. Pada makalah ini, saya akan membahas kerentanannya Google Home pada berbagai serangan yang dapat terjadi.

1 Introduksi

Saat masa IOT dimulai, *Voice assistant* menjadi salah satu teknologi terbaru yang muncul dan berkembang secara pesat. Dengan *voice assistant*, pengguna dapat berinteraksi dan memerintahkan dengan perangkat IOT menggunakan *interface* untuk suara pengguna. Saat ini, Google mengembangkan perangkat *voice assistant* sendiri yang bernama Google Home. Dengan Google Home, pengguna dapat "berbicara" kepada perangkat tersebut dan memerintahkannya untuk melakukan suatu layanan aktivitas atau menanyakan sesuatu, seperti "Tolong putarkan lagu Despacito," "Tolong bangunkan saya besok jam 5 pagi," dan "Bagaimana penyebaran COVID-19 saat ini?" Google juga mempunyai ekosistem yang besar untuk mengembangkan Google Home agar dapat melakukan aktivitas-aktivitas yang kompleks. Ekosistem Google juga menyediakan tempat bagi para pengembang untuk membuat aplikasi sendiri dengan menggunakan Google Home. Google Home sudah tersebar luas di berbagai perumahan dan perkantoran di seluruh dunia dan digunakan oleh jutaan pengguna.

Namun, keamanan merupakan aspek yang sulit dalam pengembangan *voice assistant*. Pada dasarnya, memverifikasi pengguna dalam medium suara yang terbuka dan banyak suara merupakan hal yang sangat sulit untuk dilakukan. Dengan menggunakan suara ultrasonik, penyerang dapat meniru suara pengguna dan memerintahkan Google Home untuk melakukan aktivitas yang tidak diinginkan pada jarak jauh. Penyerang juga dapat menyisipkan kode yang tidak diinginkan dengan suara ultrasonik tersebut dan memberikan akses penuh ke Google Home. Jika penyerang sudah mendapatkan akses penuh, penyerang dapat melakukan segala aktivitas yang tidak diinginkan atas nama pengguna Google Home.

Hasil studi Universitas Indiana menunjukkan bahwa Google Home dapat diserang pada jarak yang cukup jauh. Dengan menggunakan teknik khusus, penyerang dapat mengambil informasi privat dari pengguna dengan berinteraksi dengan Google Home. Penyerang dapat membuat aksi pada Google Home yang mirip dengan perintah sehari-hari. Misalnya, penyerang membuat aksi "Google Home, tolong bangunkan aku ya" yang berisi aksi-aksi yang diinginkan penyerang. Saat pengguna memerintah "Google Home, tolong bangunkan aku ya," Google Home akan melaksanakan aksi yang tidak diinginkan tanpa pengguna menyadarinya. Penyerang juga dapat membuat aksi yang terkesan sudah

selesai, padahal aksi tersebut masih berjalan dan memanfaatkannya untuk melakukan aksi tersembunyi.

Hasil survey Universitas Indiana menunjukkan bahwa pengguna Google Home mempunyai dialek suara yang sangat bervariasi. Hal ini mudah sekali dimanfaatkan oleh penyerang untuk memanfaatkan dialek suara tersebut dan menjalankan aksi lain berdasarkan dialek suara tertentu. Analisis yang berkelanjutan menunjukkan bahwa Google Home memilih suatu aksi dari berbagai aksi yang dapat dilakukan dengan melihat jumlah kata yang paling banyak cocok pada perintah pengguna. Google Home juga tidak dapat mendeteksi beberapa nama dari suatu aksi dengan akurat sehingga ketidak-akuratan tersebut dapat dimanfaatkan oleh penyerang untuk menyisipkan aksi yang tidak diinginkan.

2 Background

2.1 Voice Assistant

Voice assistant merupakan salah satu dari teknologi terbaru yang muncul seiring dengan era *Internet of Things* (IOT) yang dapat berinteraksi hanya dengan menggunakan suara sebagai masukan dan keluarannya. *Voice assistant* bekerja dengan cara menerima masukan berupa suara dari pengguna dan menerjemahkannya dengan *speech recognition* menjadi suatu teks. Teks tersebut akan digunakan untuk melakukan suatu layanan yang menghasilkan file berisi teks yang akan diubah menjadi *speech* dan disuarakan ke pengguna. Layanan-layanan yang terdapat pada *voice assistant* terdiri dari layanan bawaan dari pengembang *voice assistant* dan layanan-layanan lainnya dari pihak ketiga. Layanan-layanan ini bervariasi, mulai dari prediksi cuaca hingga pemutar musik.

2.2 Google Home

Gambar 1 Perangkat Google Home

Google Home merupakan sebuah perangkat IOT dari Google LLC yang menggunakan *voice assistant* sebagai fitur utamanya. Google Home mulai disebarluaskan ke publik pada tahun 2016. Keunikan dari Google Home ini adalah *interface* suara sebagai cara utama untuk berinteraksi dengan perangkat. Keunikan ini ditekankan dengan hilangnya *interface* I/O dan tombol yang hanya berfungsi untuk mengatur volume. Mikrofon yang berbentuk silinder didesain untuk menangkap segala suara 360 derajat yang memungkinkan Google Home untuk menangkap suara pengguna di posisi manapun dari ruangan. Google Home menerapkan Google Assistant sebagai *voice assistant*. Google Assistant sudah terpasang pada hampir seluruh perangkat Android di seluruh dunia. Google Home

dapat diaktifkan dengan memberikan perintah suara berupa “Hey Google” yang diikuti dengan perintah yang diinginkan pengguna. Google Home mempunyai kapabilitas yang sudah terbentuk bertahun-tahun sejak Google Assistant terbentuk, seperti *task planning*, laporan stock, dan bertelepon. Kapabilitas tersebut dapat diatur oleh pengguna dengan *smartphone* mereka.

Kapabilitas aksi Google Home terdiri dari aksi-aksi yang dibuat oleh berbagai pihak ketiga. Pihak ketiga membuat aksi-aksi yang memungkinkan Google Home untuk melakukan layanan yang awalnya tidak disediakan oleh Google, seperti *Walmart* dan *Hands-free Calling*, untuk dilaksanakan saat suatu aksi terpanggil. Aksi-aksi tersebut dapat dibuat menggunakan *developer kit* bernama *Actions on Google* yang disediakan oleh Google secara gratis. Daftar aksi yang dapat dilakukan terus bertambah seiring waktu dengan bertambahnya aksi-aksi baru yang dibuat oleh pihak ketiga.

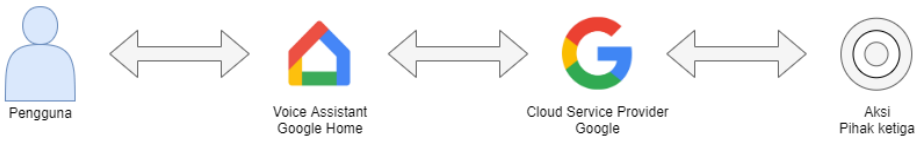
2.3 Aksi pada Google Home

Aksi dapat dilaksanakan dengan dua acara, yaitu secara eksplisit dan implisit. Pelaksanaan secara eksplisit dilakukan dengan cara menyebut aksinya secara langsung. Contohnya “Hey Google, tolong nyalakan alarm jam 6 pagi” menyebutkan aksi “menyalakan alarm” secara langsung dan Google Home akan mengidentifikasi aksi yang akan dilakukan berdasarkan aksi yang disebut. Aksi implisit dilakukan dengan cara memberikan perintah yang tidak menyebutkan aksinya secara langsung. Aksi implisit biasanya terjadi Ketika pengguna menanyakan pertanyaan kepada Google Home. Contohnya “Hey Google, apakah alarm saya sudah menyala?” Perintah tersebut tidak menyebutkan aksi secara spesifik sehingga Google Home harus mengidentifikasi aksi yang cocok dari konteks perintah. Google Home berkomunikasi dengan penggunanya dengan model *interaction model*. Dalam hal ini, Google Home dapat menafsirkan setiap suara dan mentranslasikannya menjadi sebuah perintah yang digunakan sebagai penggerak aksi.

Untuk melaksanakan suatu spesifik aksi pada Google Home, pengguna harus memakai kata unik yang menandakan perintah suara tersebut ditujukan ke Google Home, yaitu “Hey Google”. Lalu, pengguna harus mengikuti kata tersebut dengan

suatu frasa *trigger*, yang biasanya merupakan sebuah perintah. Contoh dari frasa *trigger* yaitu “hidupkan”. Terakhir, pengguna mengikuti kata tersebut dengan nama invokasi dari suatu aksi tersebut. Contoh dari nama invokasi yaitu “alarm”. Nama invokasi dari suatu aksi dapat berbeda dengan aksi itu sendiri. Bila digabungkan, kita mendapatkan satu perintah yang dapat diberikan ke Google Home, yaitu “Hey Google, tolong hidupkan alarm”.

Untuk mengembangkan suatu aksi, pengembang harus menentukan intent-intent agar memetakan masukan suara pengguna ke berbagai interface dari suatu aksi yang pengguna harapkan. Lalu, untuk menyambungkan suatu kalimat ke suatu intent, pengembang harus memberikan sampel contoh penyebutan perintah yang merupakan set kalimat yang dapat digunakan oleh pengguna untuk mengakses aksi tersebut. Pengembang dapat membuat satu atau lebih intent untuk memetakan perintah pengguna ke aksi dari pengembang tersebut.



Gambar 2 Sistem Infrastruktur Google Home

Cara kerja sistem infrastruktur pada Google Home dapat dilihat pada gambar 2. Pertama, pengguna memberikan perintah “Hey Google” yang diikuti dengan frasa trigger dan nama invokasi dari suatu aksi. Saat Google Home menerima suara “Hey Google”, Google Home mengidentifikasi perintah tersebut ditujukan kepada Google Home dan perangkat tersebut akan menerima masukan perintah dari pengguna dan mengirimkannya ke cloud service provider, dalam sistem ini yaitu cloud Google. Service provider akan melakukan speech recognition untuk mentranslasikan suara perintah menjadi bentuk teks, mencari aksi yang tepat untuk diinvokasi, dan memberikan informasi kesebut ke web service, yaitu aksi dari pihak ketiga. Web service dari pihak ketiga akan mengirimkan respon dengan format plaintext atau Synthesis Markup Language (SSML) ke cloud service provider. Lalu cloud akan mengubahnya menjadi sebuah speech dan mengirimkannya ke Google Home pengguna agar speech dapat diputar. SSML dapat digunakan untuk mengirimkan file audio sebagai respon sehingga perintah seperti memainkan musik dapat terealisasi.

Untuk menerbitkan aksi baru, pengembang harus memberikan informasi aksi berupa nama aksi, nama invokasi untuk menjalankan aksi, deskripsi aksi, dan *endpoint* tempat aksi di-*host* agar aksi dapat disertifikasi oleh Google. Proses ini dilakukan agar memastikan sebuah aksi fungsional dan mematuhi kebutuhan keamanan dan kebijakan Google. Setelah suatu aksi diterbitkan, pengguna dapat mengakses aksi tersebut dengan cara memanggil nama invokasi dari aksi tersebut.

2.4 Konteks Penyerang

Penyerang pada konteks makalah ini menunjuk kepada penyerangan kepada *voice assistant* Google Home dari jarak jauh dengan cara menerbitkan aksi yang berbahaya. Aksi-aksi yang berbahaya ini dapat diakses oleh pengguna tanpa disadari dengan perintah suara. Karena aksi-aksi berbahaya ini tidak perlu diunduh atau dipasang, aksi-aksi tersebut dapat mempengaruhi sebagian besar pengguna Google Home di seluruh penjuru dunia.

3 Pembahasan

3.1 Metode Pemilihan Aksi pada Google Home

Aksi dari Google Home akan dilaksanakan ketika pengguna mengucapkan kata invokasi dari aksi tersebut. Pada kenyataannya, terdapat beberapa aksi dengan nama invokasi yang mirip. Ketika terdapat suatu nama invokasi yang mirip, Google Home memilih invokasi dengan panjang kata yang cocok terbanyak. Contohnya saat pengguna mengucapkan "Hey Google, tolong ceritakan dongeng Indonesia dari Jawa," Google Home akan menangkap "dongeng Indonesia dari Jawa" dibandingkan dengan "dongeng Indonesia" saja. Studi kasus juga membuktikan bahwa beberapa nama invokasi tidak dapat diterka oleh Google Home sehingga aksi yang salah dapat dijalankan Ketika aksi tersebut mempunyai nama invokasi yang mirip dengan nama invokasi dari aksi yang diharapkan pengguna.

Desain dari Google Home membuat Google Home hanya dapat menjalankan satu aksi dalam satu waktu sehingga aksi akan berjalan sampai selesai terlebih dahulu sebelum dapat meneruskan ke aksi lainnya. Pengguna dapat mengucapkan "Stop" untuk menghentikan aksi yang sedang dilakukan oleh Google Home. Namun, tidak ada indikasi jelas yang menandakan bahwa suatu aksi benar-benar sudah selesai dilaksanakan. Satu-satunya indikasi yang menandakan Google Home sedang menerima masukan atau mengeluarkan suara adalah indikator lampu. Sebagian besar dari limitasi pada penyerangan dengan cara ini menyebabkan penyerangan dengan suara hampir tidak mungkin dilakukan dan hasil yang didapat tidak sepadan dengan upaya yang perlu dikerahkan oleh penyerang. Namun, penyerangan Google Home pengguna dengan cara suara merupakan penyerangan yang paling berbahaya bila serangan berhasil dengan akses penuh ke Google Home pengguna sebagai efeknya.

3.2 Penyerangan dengan Imitasi Suara

Penyerang dapat mengimitasi suara pengguna dengan memanfaatkan suara ultrasonik. Bila penyerang berhasil mendapatkan suara pengguna, penyerang akan mengkonversi suara tersebut ke frekuensi yang tidak dapat didengar manusia. Lalu, suara tersebut dapat digunakan untuk melewati verifikasi suara "Hey Google" pada Google Home. Bila verifikasi berhasil, penyerang dapat memberikan perintah ke

Google Home tanpa disadari oleh pengguna sama sekali. Penyerang juga dapat memanfaatkan teknologi *Artificial Intelligence* (AI) untuk mengubah suara pengguna untuk menyuarakan kode yang dapat mengontrol Google Home. Jika suara pengguna yang menyebutkan kode tersebut berhasil dilakukan, penyerang akan mendapatkan akses penuh ke Google Home pengguna dan penyerang dapat mengalihkan fungsionalitas dari Google Home tersebut.

Namun, teknik penyamaran suara sangat tidak praktis untuk dilakukan. Pertama, penyerang harus mendapatkan suara pengguna dengan jumlah cukup yang dapat mengisi seluruh kemungkinan ejaan kosakata untuk mengeksekusi perintah yang diinginkan penyerang. Perintah "Hey Google" sangat jarang diucapkan oleh pengguna di luar interaksi dengan Google Home sehingga penyerang akan mengalami kesulitan dalam mencari suara pengguna yang pas agar dapat membentuk ejaan "Hey Google" dari pecahan suara pengguna. Lalu, penyerang harus mencari cara agar suara palsu penyerang dapat mencapai jarak dengar Google Home. Penyerang juga perlu memastikan bahwa lingkungan sekitar Google Home tidak mempunyai *noise* yang cukup signifikan yang dapat mempengaruhi identifikasi perintah dari Google Home. *Noise* yang besar dapat menyebabkan Google Home sulit untuk mengidentifikasi suara palsu dari penyerang. Penyerang juga harus mencari *speaker* yang berkualitas agar dapat memastikan frekuensi suara yang dikeluarkan dari perangkat *speaker*-nya pas dengan suara yang telah dibuat dari aplikasi penyerang.

3.3 Penyerangan dengan Aksi Palsu

Google menyatakan bahwa pengetesan invokasi aksi dari para pengembang memastikan agar aksi dapat dijalankan dengan kemungkinan sukses yang tinggi. Namun, penyerang dapat menerbitkan aksi dengan invokasi aksi yang mirip dengan target aksi yang diinginkan. Misalnya "dongeng Indonesia dari Jawa" dapat ditarget dengan menambahkan invokasi "dongeng Indonesia dari Java" atau "dong eng Indonesia dari Jawa" dan kemungkinan-kemungkinan lainnya Dengan *noise* dari alam yang tidak dapat diredam sepenuhnya dan dialek suara manusia yang bervariasi, perbedaan tersebut menjadi sulit untuk dibedakan dengan kapabilitas teknologi yang ada saat ini. Hal ini dapat dimanfaatkan penyerang untuk membuat aksi berbahaya dengan invokasi aksi yang mirip dengan aksi yang dipakai sehari-

hari untuk mengambil informasi privat pengguna. Aksi-aksi yang membutuhkan informasi privat pengguna, seperti nomor telepon, tempat tinggal, dan nomor kartu kredit, untuk menjalankannya merupakan target utama dari teknik ini.

Device	Source	Invocation Name		"Open" + Invocation Name			Mis-recognized Invocation Name	
		# of incorrect utterances	# of incorrect skills	# of incorrect utterances	# of incorrect skills	# of completely incorrect skills	# of attack skills invoked	# of utterances invoked attack skill
Alexa	Amazon TTS	232/500	62/100	125/500	33/100	17/100	10/17	45/85
	Google TTS	164/500	41/100	104/500	26/100	17/100	12/17	63/85
	Human (Avg)	N/A	N/A	90/200	58/100	31/100	N/A	N/A
Google	Amazon TTS	96/500	24/100	42/500	12/100	7/100	4/7	20/35
	Google TTS	62/500	19/100	26/500	6/100	4/100	2/4	10/20
	Human (Avg)	N/A	N/A	19/200	14/100	6/100	N/A	N/A

Gambar 3 Hasil Eksperimen *Voice Assistant* Universitas Indiana

Dari hasil eksperimen dari Universitas Indiana pada gambar 3, dengan Google *text-to-speech* (TTS) dapat terlihat bahwa Google Home melakukan kesalahan dalam pengidentifikasian perintah sebesar 12% dengan nama invokasi saja dan 5% dengan menambahkan kata "open" sebelum nama invokasi. Dari error tersebut, 2 dari 4 aksi yang berbahaya terpanggil. *Margin error* tersebut termasuk cukup besar dan dengan penggunaan Google Home yang sering, terdapat frekuensi harapan kesalahan interpretasi perintah sebesar 12 dan terkena aksi berbahaya sebesar 2. Dengan penggunaan Google Home yang rutin (3 atau 4 kali sehari), pengguna dapat diserang oleh aksi tersebut setidaknya 3 hari sekali tanpa disadari.

3.4 Penyerangan dengan Penyamaran Aksi

Seperti yang dijelaskan pada 3.1, desain pada Google Home mengakibatkan hanya satu aksi pada Google Home hanya dapat dilaksanakan pada satu waktu dan aksi berikutnya harus menunggu hingga aksi sebelumnya selesai berjalan. Namun, banyak pengguna Google Home yang tidak mengetahui akan hal ini. Hal ini dapat dimanfaatkan oleh penyerang untuk membuat suatu aksi dengan suatu *command* yaitu *switch* yang dapat digunakan untuk memberikan impresi bahwa aksi sudah selesai dan kontrol kembali ke pengguna, padahal aksi tersebut belum selesai. Akibatnya, informasi yang seharusnya hanya diberikan ke aksi tertentu akan masuk ke aksi yang dibuat oleh penyerang. Penyerang dapat menggunakan aksinya untuk meniru aksi-aksi asli sebanyak mungkin untuk meningkatkan kemungkinan suksesnya serangan. Google Home mencoba menangkal hal ini dengan mengeluarkan suara berupa "Sure, here is " ditambah dengan nama aksi dan suara

penanda khusus. Suara penanda khusus tersebut juga berbunyi ketika aksi sudah selesai dijalankan. Google Home juga berbicara dengan aksen yang berbeda untuk membedakannya dengan aksi. Namun, pengaman ini masih kurang cukup. Dengan memanfaatkan SSML, sinyal dan notifikasi dapat ditiru dan sulit untuk dideteksi oleh telinga manusia. Penyerang juga dapat memanfaatkan *emulator* Google untuk mendapatkan suara unik dari Google Assistant untuk pemalsuan.

Penyerang juga dapat memalsukan terminasi dari suatu aksi dengan memanfaatkan opsi expect_user_response, membuat nilai opsi menjadi *true*. Opsi tersebut biasanya digunakan untuk mematikan aksi setelah aksi merespon. Setelah aksi selesai, aka nada suara "Goodbye" dari Google Home. Dengan mengeset opsi menjadi *false* dan memalsukan suara "Goodbye" dengan rekaman SSML, penyerang dapat memalsukan terminasi aksi dan menipu pengguna bahwa aksi sudah selesai dijalankan.

Setelah aksi selesai dijalankan, Google Home memberikan waktu 8 detik untuk pengguna merespon balik. Jika tidak ada suara apapun, opsi *reprompt* akan berjalan untuk menandakan pengguna bahwa aksi masih berjalan. Jika masih tidak ada respon dari pengguna setelah 8 detik tambahan, Google Home akan melakukan *reprompt* dan menunggu 8 detik sekali lagi sebelum aksi akan distop secara paksa. Opsi *reprompt* ini dapat diisi dengan file *audio* dengan maksimal waktu 2 menit. Desain Google Home ini dapat dimanfaatkan oleh penyerang untuk memasukkan *reprompt* yang berisi file *audio* tanpa suara apapun selama 2 menit. Akibatnya, aksi penyerang dapat bertahan hingga maksimal 6 menit 24 detik sebelum aksi penyerang dimatikan secara paksa. Jika Google Home mendeteksi suara dari pengguna, waktu tersebut akan diulang kembali dan menunggu 6 menit 24 detik kembali untuk respon suara pengguna. Hal ini dapat menyebabkan aksi penyerang terus hidup dan mencuri informasi privat pengguna dengan syarat terdapat suara pengguna dalam jangka waktu 6 menit 24 detik tersebut.

Dengan teknik penyamaran aksi, penyerang dapat mengimitasi sistem Google Home dan berpura-pura memberikan kendali ke pengguna atau berpura-pura mematikan aksi. Ketidak-awasan pengguna pada lampu indikator dan mematikan aksi secara eksplisit dapat menyebabkan aksi-aksi berbahaya tersebut

tetap berjalan dan mendapatkan informasi-informasi privat yang didapat dari suara pengguna.

4 Kesimpulan

Kesimpulan dari makalah ini, Google Home mempunyai celah keamanan dengan memanfaatkan aksi berbahaya yang menyebabkan informasi privat pengguna terancam. Penyerang dapat melakukan serangan dengan menggunakan suara pengguna untuk membuat suara buatan palsu yang dapat diidentifikasi oleh Google Home sebagai pengguna, memberikan akses penuh kepada penyerang. Penyerang juga dapat menyerang Google Home pengguna dengan menerbitkan aksi palsu dengan invokasi aksi yang menyerupai invokasi aksi aslinya. Faktor-faktor yang tidak dapat dihindari seperti *noise* dalam ruangan dan dialek manusia yang bervariasi membuat suara pengguna tidak teridentifikasi secara tepat dan menjalankan aksi berbahaya tersebut tanpa pengguna sadari. Lalu, penyerang dapat menambahkan aksi berbahaya mereka dengan berpura-pura memberikan kontrol kepada pengguna dan meniru aksi asli sebanyak-banyaknya yang membuat pengguna tertipu dan berpikir Google Home sedang melaksanakan aksi yang dia harapkan. Terakhir, penyerang dapat menambahkan aksi berbahayanya yang menyebabkan aksi tersebut *standby* selamat 6 menit lebih dan dapat berjalan lebih dari itu selama Google Home mendeteksi suara dari pengguna yang tidak sadar bahwa aksi penyerang masih berjalan. Desain dari Google Home masih mempunyai celah keamanan pada aspek aksi yang merupakan fitur utama dari Google Home sehingga perbaikan desain perlu dilakukan untuk memperbesar tingkat keakuratan dalam mengidentifikasi perintah dari pengguna dan memperketat sertifikasi dalam penerbitan aksi agar aksi-aksi berbahaya dapat terdeteksi dan dapat dihilangkan sebelum aksi mencapai Google Home pengguna. Pengguna juga perlu awas agar tidak memberikan informasi yang sensitif ke Google Home dan tidak menggunakan Google Home pada tempat-tempat yang rawan informasi privat, seperti kantor perusahaan.

5 Referensi

1. Diao, Wenrui, et al. "Your voice assistant is mine: How to abuse speakers to steal information and control your phone." *Proceedings of the 4th ACM Workshop on Security and Privacy in Smartphones & Mobile Devices*. 2014.
2. Emerick, Charles Thomas, et al. "Voice assistant system." U.S. Patent No. 9,171,543. 27 Oct. 2015.
3. Li, Bo, et al. "Acoustic Modeling for Google Home." *Interspeech*. 2017.
4. Alepis, Efthimios, and Constantinos Patsakis. "Monkey says, monkey does: security and privacy on voice assistants." *IEEE Access* 5 (2017): 17841-17851.
5. Schönherr, Lea, et al. "Adversarial attacks against automatic speech recognition systems via psychoacoustic hiding." *arXiv preprint arXiv:1808.05665* (2018).
6. Zhang, Nan, et al. "Understanding and mitigating the security risks of voice-controlled third-party skills on amazon alexa and google home." *arXiv preprint arXiv:1805.01525* (2018).