Výzkum a nové technologie v kybernetické a informační bezpečnosti

Mohou hlasový asistenti odposlouchávat své majitele?

(03. 12. 2020, portswigger.net) Výzkumníci z University of Cambridge představili způsob, jak mohou být hlasový asistenti (voice assitants), jako například Alexa, zneužiti k narušení soukromí osob ve svém okolí. Klasická obava, že jelikož jsou tyto zařízení stále v provozu tak mohou přímo odposlouchávat komunikaci svého okolí je dle výzkumníků na místě. Nad to však demonstrovali i možnosti, jak tyto zařízení mohou odposlouchávat i takové činnosti jako je například zadávání PIN kódu na telefonu. V některých případech může dojít až k odposlechu celých textových zpráv.

Komentář: Voice assistants představují zařízení, jejichž popularita v poslední době značně roste. Jejich nebezpečí pramení především z toho, že jsou neustále v provozu a že jsou připraveny reagovat na hlasové pokyny svých majitelů. Mohou tak být zneužity k tzv. útokům postranním kanálem (side-channel attacks). Předcházení podobným incidentům však může být problematické. Nejjednodušší metodou je nemít tato zařízení stále zapnutá. Tím ale dochází k tomu, že se narušuje význam toho, proč si je lidé vůbec pořizují. Žádné výzkumy se zatím příliš nezabývají otázkou zabezpečení hlasových asistentů bez toho, aby došlo k narušení některé z jejich funkcí.

Průzkum množství škodlivého kódu v open source kódech

(17. 11. 2020; darkreading.com) Možnost získávání kódu nebo jeho části z open source databází je jednou ze základních potřeb většiny programátorských týmů. Řada výzkumníků (např. z Georgia Institute of Technology) se v letošním roce zaměřili na zmapování počtu škodlivého kódu v takovýchto databázích. Bylo tak například zrevidováno 268 000 různých balíčků kódů z největšího open source repositáře pro programovací jazyk Python. Z toho bylo jen velmi málo kódů škodlivých. Tedy v případech, že již dopředu nebylo uvedeno, že se jedná o škodlivý kód. Jednou z forem útoků, pomocí kterých se útočníci snaží využít těchto open source databází je tzv. typosquatting. Tato metoda spočívá v tom, že útočníci vytvoří baliček, který obsahuje škodlivý kód a zároveň jej pojmenují podobně jako nějaký legitimní a zavedený balíček kódu

Komentář: Využívání vektoru útoku skrze podobné open source se zdá dle uvedených dat poměrně ojedinělé. Tyto metody totiž vyžadují značné množství práce, které je třeba do tvorby škodlivého kódu nebo jeho inkorporace do jiného legitimního kódu vložit. Většina útočníků však využívá již někým jiným vytvořené kódy a programy (tzv. script kiddies).

PETR MARTINEK; p.martinek@nukib.cz
Oddělení výzkumu a evropské spolupráce, NÚKIB