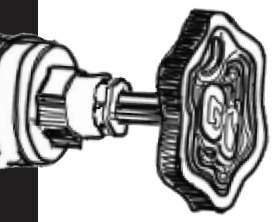
21/2015

FUNDACJA
bezpieczna
cyberprzestrzeń



zawór bezpieczeństwa 21/2015

Barbie „DługoUcha”

Mamy czas przedświąteczny, dzieci z utęsknieniem czekają na prezenty gwiazdkowe. Co kupić? Rynek przejmują inteligentne zabawki.
W latach 80-tych panował szał na gadającego misia Ruxpina. Misia w stylu puchatego odtwarzacza, bo niestety nie wchodził on w interakcje, a tylko śpiewał piosenki i opowiadał historie. Trzydzieści lat później firma Mattel wypuszcza nową wersję interaktywnej Barbie „Hello Barbie”. Wyposażona w mikrofon i odbiornik wifi aktywowany po naciśnięciu guzika na brzuchu, lalka będzie w stanie angażować się w krótkie konwersacje. Gdy dziecko mówi do „Hello Barbie” rozmowa jest nagrywana i zaszyfrowane dane wysyłane są na serwer, gdzie przetwarza je oprogramowanie do rozpoznawania mowy. W efekcie lalka odpowiada dziecku przy pomocy zaprogramowanych fraz. Co ważne, Barbie nie nagrywa biernie rozmów, mikrofon nie jest cały czas włączony.
W czym więc problem? Amerykańska grupa „Campaign for a Commercial-Free Childhood” (CCFC) rozpoczęła w mediach społecznościowych kampanię przeciwko „podsłuchującej” lalce pod hasłem „Hell No Barbie”, podnosząc wiele kwestii związanych z prywatnością dzieci. Nagrania z dziecięcych rozmów przechowywane są przez firmę ToyTalk, która dostarcza technologię rozpoznawania głosu dla Barbie. CCFC twierdzi, że materiały mogą być potem wykorzystane do tego, aby kierować do najmłodszych spersonalizowane reklamy. Mattel i ToyTalk zapewniają, że nie będą do takich celów wykorzystywać rozmów.
Aby założyć konto „Hello Barbie” Mattel wymaga zgody rodziców. Mają oni dostęp do nagranych rozmów i mogą je skasować, kiedy zechcą. Mimo tych zapewnień polityki prywatności obu firm pozostawiają wątpliwości.
Oprócz oczywistych obaw o prywatność CCFC wskazuje na jeszcze jeden niepokojący aspekt: dzieci potrzebują interakcji z prawdziwymi ludźmi, a nie komputerowymi algorytmami. Gdyby i Ken zaczął mówić, to obu lalkom towarzystwo dzieci przestałoby być potrzebne. [1]

I teraz komu mandat?

Jedziesz zbyt szybko - źle. Za wolno też niedobrze. Policja drogowa w Mountain View w Kalifornii zatrzymała samochód za zbyt powolną jazdę i tamowanie ruchu. Pojazd poruszał się z prędkością 24 mil na godzinę po drodze z ograniczeniem prędkości do 35 m/h.
Jakież było zdziwienie policjanta, gdy okazało się, że to samosterujący pojazd Google. Firma celowo

ograniczyła prędkość ze względów bezpieczeństwa. Prawo stanu Kalifornia pozwala autonomicznym samochodom poruszać się po drogach. Koncern testuje tego typu auta od 2009 roku i jest w tej sprawie w częstym kontakcie z policją.
W specjalnym komunikacie Google chwaliło się nawet, że: „Po pokonaniu 1,2 miliona mil w trybie autonomicznej jazdy z dumą oświadczamy, że nigdy nie dostaliśmy mandatu". Kilka zaliczonych wypadków z udziałem samochodów Google spowodowali inni uczestnicy ruchu.
Policjant ostatecznie skontaktował się z operatorem Google. Niezłą musiał mieć minę, gdy okazało się, że nie ma kogo prosić o okazanie prawa jazdy oraz dowodu rejestracyjnego, nie mówiąc o wypisaniu mandatu. Ciekawe czy jego reakcję można będzie wkrótce zobaczyć na zdjęciach Google Earth? [2]

Zabawki na celowniku

Trwa zła passa dla producentów zabawek, bo tym razem znowu o nich...
Chińska firma VTech, produkująca elektroniczne zabawki edukacyjne, przyznała, że ich baza danych na AppStorze padła ofiarą ataku hakerskiego w dniu 14 listopada.
Z AppStore'a ściągnąć można gry, e-booki i kontent edukacyjny dla zabawek VTech. Baza danych zawierała dane klientów: imię i nazwisko, adres mailowy, hasło, adres IP, adres korespondencyjny i historię pobrań. Dane dzieci zawierały: imię, płeć i datę urodzin.
Firma zapewniła, że wśród danych nie było informacji na temat kart kredytowych. Choć sama nie podała ilu osób może dotyczyć problem, magazyn Motherboard, który pierwszy podał informację o ataku, określił, że mogły ucierpieć dane 5 milionów rodziców i ponad 200 tysięcy dzieci.
Motherboard o ataku poinformował anonimowy haker, który twierdził, że nie zamierza nic robić z pozyskanym danymi. Zdarza się, że hakerzy włamują się do systemów, aby po prostu pokazać ich niedoskonałość. Równie często usiłują sprzedać dane klientów na internetowym czarnym rynku, oddając je w ręce osób dokonujących ataków phishingowych. Jeśli liczba poszkodowanych podana przez Motherboard jest prawdziwa, byłby to jeden z największych ataków w ostatnich latach.
Tymczasem w związku z nadchodzącymi Świętami poszkodowani klienci liczą na karty podarunkowe do AppStore. Ciekawe czy hakerów stać będzie na taki gest. [3]

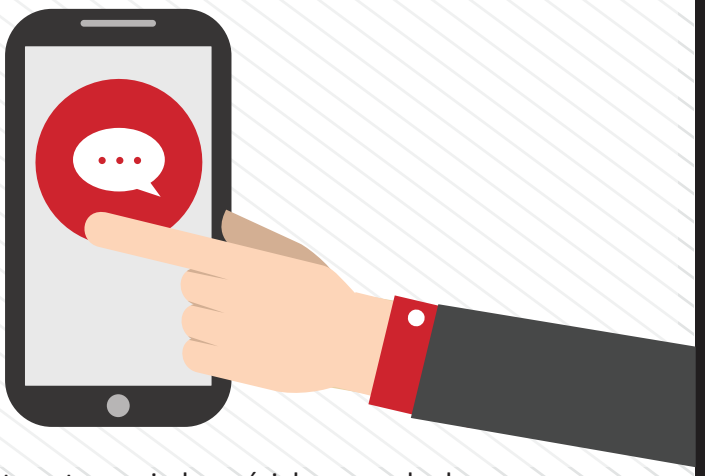
Już nie schowasz się za ścianą

Naukowcom z Massachusetts Institute of Technology udało się stworzyć urządzenie, które jest w stanie odróżniać kim jesteś, gdzie jesteś i którą ręką poruszasz - nawet wtedy, gdy znajdujesz się za ścianą lub po drugiej stronie budynku. Czyli gdy wydawałoby się, że jesteś niewidoczny.
Naukowcy pracowali nad śledzeniem ludzkiego ruchu od 2013 roku. Technologia nazwana RF-Capture pozwala na podglądanie osób znajdujących się za ścianą przy wykorzystaniu sygnału wifi. Ludzie nie muszą nosić żadnego czujnika. Urządzenie wysyła sygnał wifi, fale radiowe odbijają się od osoby znajdującej się za ścianą i trafiają do odbiornika. Sprzęt zbiera informacje, wysyła komputerowi do analizy i na ich podstawie specjalne oprogramowanie tworzy obraz sylwetki. RF-Capture może śledzić ruchy ludzkiej ręki, określić jak osoba za ścianą się porusza, a nawet rozróżnić - - z prawie 90% dokładnością - między kilkunastoma różnymi osobami, porównując elementy budowy ciała.

Na co to wszystko? Naukowcy twierdzą, że w przyszłości technologia RF-Capture może np. pomóc wezwać pomoc w nagłych przypadkach, gdy ktoś z rodziny upadnie lub straci przytomność. To szczególnie przydatne zastosowanie w szpitalach czy domach opieki dla osób starszych. Można będzie też jej użyć do sterowania światłem i telewizorem, czy do stosowywania ogrzewania w zależności od tego, w którym miejscu mieszkania człowiek przebywa. Twórcy technologii chcą też ułatwić pracę aktorom, którzy obecnie przy produkcji filmów muszą nosić na sobie specjalne czujniki. Dzięki technologii RF Capture można śledzić ruch aktorów bez nich. Naukowcy jak zwykle widzą ocean możliwości, zwykli użytkownicy na myśl o tej inwigilacji już nie mogą schować się za ścianą. W końcu te mają już nie tylko uszy, ale i oczy. [4]

Ostrożnie z odpowiadaniem na smsy!

W opublikowanym na swoim kanale na YouTube filmiku firma Symantec przestrzega przed nową metodą włamywania się na konta. Aby zhakować czyjeś konto mailowe, atakującmu potrzebny jest jedynie adres mailowy i numer telefonu komórkowego. Żadnych umiejętności technicznych. Jak to działa? Atak wykorzystuje proces odzyskiwania zapomnianego lub zagubionego hasła. Po wpisaniu adresu mailowego i kliknięciu ikonki pomocy „Need help?", atakujący wybiera opcję „Nie znam hasła". System prosi o wpisanie adresu email i gdy zaznaczymy opcję, że nie pamiętamy hasła, prosi nas o wpisanie kodu weryfikacyjnego, który właściciel konta dostaje smsem na telefon.
Wtedy do ofiary wiadomość wysyła przestępca, prosząc ją o kod weryfikacyjny. Jeśli ta nie zorientuje się w podstępie i odpowie na wiadomość, umożliwi przestępcy włamanie się na swoje konto.
Symantec przestrzega, aby nigdy nie odpowiadać



na tego typu wiadomości, bo sms z kodem generowany jest automatycznie. Tego typu atak może zostać przeprowadzony na różne usługi, które bazują na kodzie weryfikacyjnym wysyłanym smsem. Cóż, komunikacja smsowa, która niegdyś wniosła rewolucję do komunikacji, szybko okazała się przekleństwem. [5]

Internet dźwięku

Uwaga audiofile! Historia zatacza koło: od zarania dziejów do celów komunikacyjnych w życiu ludzi służył dźwięk. Alarm podnosiły dzwony, a informacje z wioski do wioski przekazywano sobie na przykład przy pomocy rytmów wybijanych przez bębny.
Ten koncept odradza się w nowej formie.
Chirp to start-up z Londynu i aplikacja, która pozwala przesyłać dane przy pomocy dźwięku.
Jej działanie jest proste: wybierz link, kawałek tekstu albo obrazek do przesłania, naciśnij przycisk w aplikacji, aby rozpocząć procedurę przesyłania. Dane wędrują na serwer. Telefon „zaszczebiota" w charakterystyczny sposób. To znak, że osoba zainteresowana może materiał odebrać. Pod warunkiem, że ma włączoną aplikację. Twórca pomysłu twierdzi, że dźwięk może działać jak sieć, choć póki co jego potencjał pozostaje niewykorzystany. A przecież dźwięk jest w stanie dotrzeć tam, gdzie inne sieci nie dają rady. Wszystkie metody wykorzystujące dźwięk do przesyłu danych mają swoje mocne i słabe strony.

FUNDACJA bezpieczna cyberprzestrzeń

Przekaz danych przez audio jest z konieczności wolny. Sygnał przesyłu może nieść dużą ilość danych, ale być nieprzyjemny dla ucha. Lub odwrotnie: dźwięki kwartetu smyczkowego mogą nieść bardzo niewiele. Równie dobrze może się zdarzyć, że sygnał jednocześnie będzie niemiły i zawodny w kwestii przesyłu. Z danymi dźwiękowymi wiąże się też wiele kwestii bezpieczeństwa: póki co może je odebrać każdy.
Chirp rozpoczął zbieranie środków na dalszy rozwój na platformie crowdfundingowej Crowdcube. Potrzeba 400 tys. euro, w zamian do wzięcia jest 16,7% udziałów w firmie. My na razie wstrzymujemy się z inwestycją, czekamy aż ktoś w końcu na poważnie zajmie się wiatrem. **[6]**

Z Okazji Nadchodzących Świąt
i Zbliżającego się Nowego 2016 Roku
Chcielibyśmy Przesłać Wszystkim
Serdeczne Życzenia.
Dla Was Ślemy Naszą Kartkę Świąteczną!!!
Trzymajcie się Ciepło.

[1] http://tinyurl.com/jgunyln
[2] http://tinyurl.com/jxlwtma
[3] http://tinyurl.com/jl9obpo
[4] http://tinyurl.com/jo5bdtw
[5] http://tinyurl.com/owah6jz
[6] http://tinyurl.com/j5kyhng

Kolejne numery można śledzić również na serwisie społecznościowym LinkedIn

Fundacja Bezpieczna Cyberprzestrzeń zaangażowana jest w wiele inicjatyw, konferencji, szkoleń i projektów dotyczących tematyki bezpieczeństwa teleinformatycznego. Celem Fundacji jest działanie na rzecz bezpieczeństwa cyberprzestrzeni, w tym na rzecz poprawy bezpieczeństwa w sieci Internet.

www: https://cybsecurity.org
Twitter: @cybsecurity_org
Facebook: https://www.facebook.com/FundacjaBezpiecznaCyberprzestrzen

Redakcja: Adrianna Maj, Agnieszka Wrzesień-Gandolfo