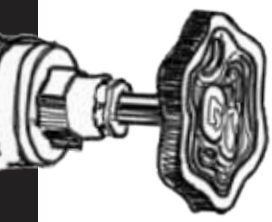
7/2016

FUNDACJA bezpieczna cyberprzestrzeń



zawór bezpieczeństwa 7/2016

Smartfon na ba-K-terie?

Bakterie mogą być wykorzystane do zasilania małych urządzeń, w tym smartfonów, donoszą naukowcy z Uniwersytetu Oksfordzkiego. Według nich to jeden z przyszłościowych sposobów na generowanie niewielkich ilości energii dla mikromaszyn. Bakterie poruszają się w sposób chaotyczny i same z siebie są zbyt mało zorganizowane, by móc generować użyteczną energię. Jednak naukowcy zdołali zapanować nad ich ciągłym ruchem i udało im się stworzyć rodzaj bakteryjnej farmy wiatrowej, odpowiedzialnej za stałe zasilanie dla małych urządzeń. Bakterie miałyby wprawiać w ruch miniaturowe wirniki, które z kolei przekazywałyby energię dalej i utrzymywały działanie telefonu. Choć to źródło energii jest niewielkie, naukowcy widzą w tym odkryciu duży potencjał i są przekonani, że na smartfonach się nie skończy. Zastosowanie energii bakteryjnej widzą również w szeregu innych urządzeń, typu przełączniki optyczne czy mikrofony w telefonach.
Ciekawe czy ta fascynacja bakteriami okaże się zdrowa? Oby bakteryjne farmy wiatrowe nigdy nie wymagały antybiotykoterapii. Historia pokazuje, że walka człowieka z drobnoustrojami bywa często nierówna. [1]

Lądowanie Apollo 11 bez tajemnic

NASA udostępniła kod źródłowy komputera, który sterował misją Apollo 11 - pierwszego statku kosmicznego, którym trzej astronauci dotarli w lipcu 1969 na Księżyc.

Choć od dawna kod był udostępniany bez większych problemów każdemu zainteresowanemu, który zgłosił się do NASA, to teraz oficjalnie stał się on częścią domeny publicznej. Kod dostępny jest na stronie GitHub: https://github.com/chrislgarry/Apollo-11. Komputery skonstruowane w latach 60-tych na potrzeby programu Apollo były cudami techniki tamtych czasów, a stworzenie oprogramowania do lotu Apollo 11 stanowiło nie lada wyzwanie. Kod źródłowy został napisany przez programistów w assemblerze - zapomnianej dziś metodzie programowania. Twórcy okrasili go licznymi barwnymi komentarzami i żartami. Dla przykładu, funkcję, odpowiedzialną za uruchamianie silników rakietowych nazwali „BURN, BABY, BURN" w nawiązaniu do zwyczaju zapowiadania premierowych utworów przez jednego z DJów w rozgłośni radiowej w tamtych czasach. Oprogramowanie zajmujące się obsługą przycisków, w jaki wyposażony był komputer pokładowy programu Apollo (Apollo Guidance Computer), określono jako „PINBALL GAME BUTTONS AND LIGHTS". W kodzie znalazło się też miejsce na cytaty z Szekspira.
Ciekawe czy na takie smaczki z misji na Marsa też przyjdzie nam czekać 50 lat? [2]

Dostęp do Internetu twoim podstawowym prawem!

A teraz o uchwale o niebagatelnym znaczeniu dla wszystkich: Rada ds. Praw Człowieka ONZ przyjęła niedawno rezolucję, która podkreśla, że obok prawa do życia i jedzenia, dostęp do Internetu należy do podstawowych praw człowieka. Rezolucja głosi, że wszystkie kraje powinny zapewnić obywatelom dostęp do sieci i potępia te, które go utrudniają. Uchwałę poparło 70 krajów. Przeciwko niej głosowały Rosja, Chiny i Arabia Saudyjska. Zaskakująca opozycja przyszła także z RPA, Indii i Indonezji, które zgłosiły problem z zaakceptowaniem paragrafu odnośnie „jednoznacznego potępienia środków, mających celowo uniemożliwiać lub utrudniać dostęp do rozprzestrzeniania informacji online". O czym jeszcze mówi rezolucja? Na przykład o tym, że „te same prawa, które obywatele mają offline muszą być także chronione online", głównie w odniesieniu do wolności słowa. Dodatkowo wspomina o odpowiedzialności za naruszenia praw człowieka w Internecie, ochronie prywatności online i konieczności edukacji dziewcząt w obszarze nowych technologii. Rezolucja nie ma charakteru wiążącego, ale może stanowić ważny mechanizm nacisku na kraje, które mają z Internetem - delikatnie mówiąc – problemy. Zatem menu podstawowych praw człowieka poszerzyło się, jednak my życzymy każdemu, aby wszystkie pozycje, począwszy od dostępu do jedzenia, wody, a na Internecie skończywszy, były dla niego zawsze dostępne. Samym Internetem głodnego ani spragnionego się nie nakarmi. [3]

Aparat Apple pod kontrolą

Apple ma zamiar opatentować technologię, która pozwoli na wyłączenie kamery w iPhone'ie czy iPadzie podczas koncertów, różnych wydarzeń artystycznych, wizyt w muzeach czy w innych miejscach, gdzie fotografowanie czy nagrywanie jest niemile widziane.
Coraz częściej zdarza się, że przed występem artyści proszą gości o powstrzymanie się od rejestrowania wydarzenia, jednak w praktyce mało kto się do tego stosuje. Technologia, nad którą pracuje Apple ma ich właśnie chronić przed nielegalnymi zdjęciami i nagraniami wrzucanymi do sieci.
Jak ma to działać? iPhone lub iPad otrzymywałby zakodowane sygnały w podczerwieni pochodzące z nadajników, które czasowo wyłączałyby możliwość nagrywania lub fotografowania w wybranych miejscach.
Ochrona artystów to oczywiście tylko jedno z możliwych zastosowań. Technologia ta sprawdzi się też w innych okolicznościach, np. aby zablokować możliwość nagrywania na przejściach granicznych państw. Dzięki niej można będzie także przesyłać różne informacje równolegle na wiele komórek, wśród osób znajdujących się w tym samym miejscu. Jednocześnie jednak nietrudno sobie wyobrazić zakusy wielu rządów, które przy jej użyciu np. zabraniałyby nagrywania i relacjonowania w mediach społecznościowych protestów czy innych wydarzeń. Skonsternowani użytkownicy „jabłuszka" pytają o dalsze plany firmy, a co poniektórzy twierdzą, że najlepszym patentem jakim mogą na ten pomysł odpowiedzieć jest blokada zakupu takich produktów. [4]

Włam przez YouTube na smartfona

Polecenia głosowe ukryte w filmikach na YouTube mogą być wykorzystane przez przestępców do włamań do smartfonów, donoszą amerykańscy badacze.
Aby atak się powiódł, smartfon musi mieć zainstalowaną aplikację osobistego asystenta Apple Siri albo Google Now, których działanie opiera się na systemie rozpoznawania mowy.
Włamanie możliwe jest dzięki poleceniom głosowym ukrytym w plikach wideo na YouTube. Filmik wcale nie musi być odtwarzany na danym smartfonie, telefon może po prostu znajdować się odpowiednio blisko innego emitującego urządzenia, aby „usłyszeć" i zinterpretować ukryte komendy. W ten sposób przestępcy mogą zmusić urządzenie mobilne np. do zainstalowania złośliwego oprogramowania czy zmiany określonych ustawień.

Warto zaznaczyć, że ukryte polecenia są niezrozumiałe dla ludzkiego ucha, choć urządzenia mobilne doskonale sobie z nimi radzą. Użytkownik może jednak dostrzec, że urządzenie dostało jakieś zlecenie i zamierza je podjąć, dzięki notyfikacjom dźwiękowym, o ile te nie zostały celowo zamaskowane przez inny hałas. Rzecz jednak w tym, że użytkownicy często ignorują takie alerty.
Czy w tej sytuacji najbardziej niezawodną metodą ochrony jest oglądanie filmików z wyłączonym dźwiękiem? [5]

Inteligentne gadżety mogą cię zdradzić!

Internet przedmiotów po raz kolejny okazuje się kłopotliwy z punktu widzenia bezpieczeństwa. Różne inteligentne gadżety, które na co dzień nosimy, takie jak smart-zegarki czy opaski elektroniczne, mogą zostać w łatwy sposób wykorzystane przez cyberprzestępców do wyłudzenia naszych wrażliwych danych, takich jak PIN do karty kredytowej czy hasła do zamków elektronicznych. Chińscy specjaliści przeprowadzili 5000 testów na trzech systemach bezpieczeństwa, w tym bankomatach, z udziałem ponad dwudziestu osób noszących różnego rodzaju smart-gadżety przez okres minimum 11 miesięcy. Badacze znaleźli sposób, aby z 80% skutecznością ukraść PIN lub hasło, infekując tego typu mini urządzenia. Dzięki znajdującym się w nich np. akcelerometrom, żyroskopom czy magnetometrom, udało im się śledzić i zapisać co do milimetra najdelikatniejsze ruchy, które wykonuje ręka osoby wpisującej kod PIN czy hasło.
Ten news chyba ostatecznie obalił przydomek „inteligentny" w przypadku tego typu gadżetów. Sami bądźmy więc SMARTniejsi – następnym razem wpisując hasło czy PIN nie zapomnijmy o ściągnięciu zegarka czy opaski. [6]

[1] http://tinyurl.com/j5ab69n
[2] http://tinyurl.com/hbn9f62
[3] http://tinyurl.com/jgc265n
[4] http://tinyurl.com/zmxk9a4
[5] http://tinyurl.com/z23ecw2
[6] http://tinyurl.com/hwcwatf

Kolejne numery biuletynu „Zawór Bezpieczeństwa" można również śledzić 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