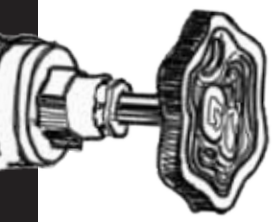
10/2014

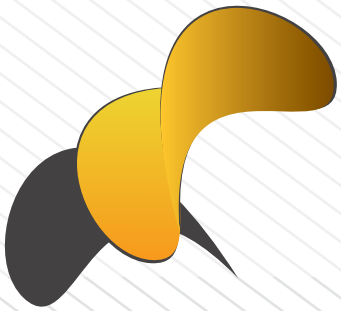
FUNDACJA bezpieczna cyberprzestrzeń



zawór bezpieczeństwa 10/2014

Chipsy, które podsłuchują

Naukowcy z MIT, Adobe i Microsoft opracowali algorytm, dzięki któremu możliwe jest odtworzenie dźwięku z mikroskopijnych ruchów przedmiotów otaczających rozmówców. Problem jaki między innymi chcieli pokonać to sytuacja kiedy rozmowa ma miejsce w pomieszczeniu wykonanym z dźwiękoszczelnego, przezroczystego materiału i nie jest możliwe ustalenie treści konwersacji. Jak wiadomo fale dźwiękowe



oddziaływają na otoczenie, w sposób mikroskopijny, ale jednak oddziaływują. Z wykorzystaniem bardzo dokładnego zapisu video (nawet do 6 tysięcy klatek na sekundę) możliwe jest zaobserwowanie tych oddziaływań, a z zaobserwowanego ruchu odtworzenie dźwięku, który je wywołał. Tak właśnie zrobili wspomniani naukowcy. W dźwiękoszczelnym pomieszczeniu, oprócz rozmówców, umieścili paczkę chipsów. Sfilmowali mikroskopijne ruchy opakowania chipsów, które miały miejsce w czasie rozmowy, a następnie odtworzyli konwersacje. Wygląda na to, że organizatorzy poufnych rozmów będą musieli sprawdzać, czy rozmówcy nie mają przy sobie nie tylko telefonów i innych urządzeń elektronicznych, ale również czy w czasie rozmowy nie mają zamiaru zajadać prosto z opakowania chipsów czy delicji. Podsłuchiwanie w restauracjach stało się jeszcze łatwiejsze. Na razie nic nie wiadomo czy jest reakcja zwrotna - czy smak czipsów jest w stanie wywołać pieprzne lub słodkie słowa rozmówców. [1]

Przed wypłatą z bankomatu możesz zagrać w Dooma

Ed Jones - australijski haker, który jak sam siebie opisuje ma tendencję do niszczenia, postanowił "zniszczyć" regularny bankomat i zamienić go w konsolę do gry w Dooma. Wynik swoich dokonań

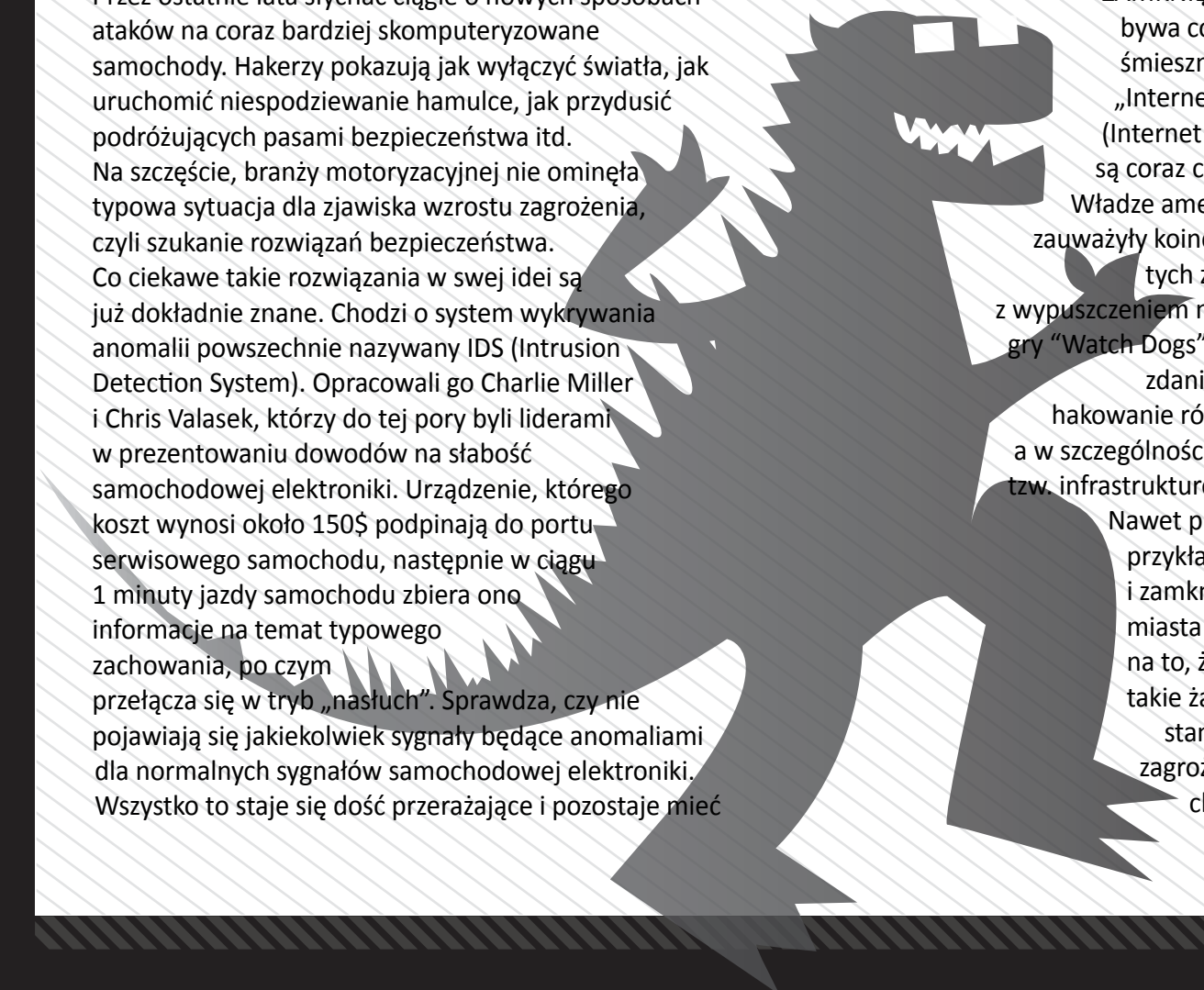
zamieścił w serwisie YouTube, gdzie można obejrzeć jak korzystając ze standardowych przycisków znajdujących się na bankomacie rozgrywa swoją partię z pistoletem w ręku. Zabawa Australijczyka wydaje się mało szkodliwa w porównaniu do wielu innych prób hakowania bankomatów, np: do wypłacania pieniędzy poprzez wysyłanie SMS-ów do bankomatu, do którego wcześniej nielegalnie podpięto telefon (o czym pisaliśmy w ZB 5/2014). Jeśli więc zauważycie kogoś blokującego bankomat przez dłuższy czas - lepiej poszukajcie innego bankomatu. Podobno graczy w Dooma jest bardzo ciężko oderwać od konsoli. [2] i [3]

Jest IDS dla samochodów

Przez ostatnie lata słychać ciągle o nowych sposobach ataków na coraz bardziej skomputeryzowane samochody. Hakerzy pokazują jak wyłączyć światła, jak uruchomić niespodziewanie hamulce, jak przydusić podróżujących pasami bezpieczeństwa itd. Na szczęście, branży motoryzacyjnej nie ominęła typowa sytuacja dla zjawiska wzrostu zagrożenia, czyli szukanie rozwiązań bezpieczeństwa. Co ciekawe takie rozwiązania w swej idei są już dokładnie znane. Chodzi o system wykrywania anomalii powszechnie nazywany IDS (Intrusion Detection System). Opracowali go Charlie Miller i Chris Valasek, którzy do tej pory byli liderami w prezentowaniu dowodów na słabość samochodowej elektroniki. Urządzenie, którego koszt wynosi około 150$ podpinają do portu serwisowego samochodu, następnie w ciągu 1 minuty jazdy samochodu zbiera ono informacje na temat typowego zachowania, po czym przełącza się w tryb „nasłuch". Sprawdza, czy nie pojawiają się jakiekolwiek sygnały będące anomaliami dla normalnych sygnałów samochodowej elektroniki. Wszystko to staje się dość przerażające i pozostaje mieć nadzieję, że o prowadzeniu samochodu nie będą tylko decydowały dwie zwalczające się maszyny na przemian hamujące i przyśpieszające samochód. [4]

Zawracaj. Atak godzilli!

„GODZILLA ATTACK! TURN BACK!" Taki atak ukazał się kierowcom w San Francisco. Na szczęście poziom wiary w sensacyjne wiadomości zdecydowanie zmalał od czasów radiowej audycji z lat 30-tych XX wieku, informującej o ataku Marsjan. Kierowcy co najwyżej doszli do wniosku, że to reklama nowego filmu o znanym potworze. Trochę mniej fantastycznie było po wyświetleniu komunikatów "IT'S TOO DAMN HOT. CITY CLOSED" (JEST PIEKIELNIE GORĄCO. MIASTO ZAMKNIĘTE). W ogóle bywa coraz mniej śmiesznie gdyż ataki na „Internet Rzeczy" (Internet of Things - IoT) są coraz częstsze. Władze amerykańskie zauważyły koincydencję tych zdarzeń z wypuszczeniem na rynek gry "Watch Dogs", która ich zdaniem promuje hakowanie różnych urządzeń, a w szczególności stanowiących tzw. infrastrukturę krytyczną. Nawet przywołane przykłady z Godzillą i zamknięciem miasta jasno wskazują na to, że coraz częściej takie żarty mogą stanowić poważne zagrożenie. Zabrzmiał chyba donośny



alarmowy dzwonek dla producentów i operatorów IoT, aby poważniej podeszli do produkcji i wykorzystywania tych urządzeń. Ustalmy przy okazji, że „ATAK GODZILLI" to maksymalnie dobry komunikat – żart na drodze. [5]

Tak NIE przygotowuje się cyber exercises

BAE Systems - potężny brytyjski koncern zbrojeniowy i lotniczy poinformował, że jeden z jego klientów stracił miliony dolarów w wyniku cyberataku. Jeden z najważniejszych przedstawicieli firmy (Global Product Manager) powiedział w wywiadzie telewizyjnym o wspomnianym ataku, który jego zdaniem wydarzył się w końcu 2013 r. i przez miesiące nie był wykryty. Firma uznała atak za bardzo istotny i był on rozpatrywany na najwyższym szczeblu. Efekty informacji były natychmiastowe - 1,6 % spadku na giełdzie w ciągu dnia, przy zwiększonych obrotach na akacjach, co zazwyczaj wskazuje na nieprzypadkowy ruch giełdowy. Sytuacja tym bardziej niebezpieczna gdyż BAE od pewnego czasu reklamuje się jako dostawca usług cyberbezpieczeństwa. Wyjaśnienie przyszło trzy tygodnie po komunikacie TV. Okazało się, że olbrzymia strata to wynik nie tyle ataku cybernetycznego, co braku świadomości o tym, że w korporacji odbywały się ćwiczenia sprawdzające reakcje na cyberataki. Reakcja przedstawiciela firmy była nie najlepsza, aczkolwiek przysporzyła sporo materiału analitycznego. W naszych dwóch edycjach Cyber-EXE™ Polska na razie obyło się bez takiej eskalacji. W tym roku również na to liczymy. [6]

[1] http://tinyurl.com/kdqqbdt
[2] http://tinyurl.com/lxdbneo
[3] http://tinyurl.com/ndfq8z3

[4] http://tinyurl.com/p8ewjcs
[5] http://tinyurl.com/omz4fvx
[6] http://tinyurl.com/koocr3s

Jeśli chciałbyś podzielić się z uczestnikami konferencji „SECURITY CASE STUDY 2014" swoją wiedzą na tematy związane z bezpieczeństwem teleinformatycznym, ZAPRASZAMY DO ZGŁOSZENIA WŁASNEJ PROPOZYCJI REFERATU JUŻ TYLKO DO 15 SIERPNIA! Szczegółowe informacje na stronie konferencji: https://www.securitycasestudy.pl/cfp/

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: http://cybsecurity.org
Twitter: @cybsecurity_org
Facebook: https://www.facebook.com/FundacjaBezpiecznaCyberprzestrzen
LinkedIn: https://www.linkedin.com/company/cybersecurity-foundation