HAKOWANIE ANDROIDA™

Kompletny przewodnik xdadevelopers po rootowaniu, ROM-ach i kompozycjach

Jason Tyler, Will Verduzco

Tytuł oryginału: XDA Developers' Android Hacker's Toolkit:
The Complete Guide to Rooting, ROMs and Theming

Tłumaczenie: Tomasz Walczak

ISBN: 978-83-246-5682-0

This edition first published 201.

Wydawnictwo HELION
ul. Kościuszki 1c, 44-100 GLIWICE
tel. 32 231 22 19, 32 230 98 63
e-mail: helion@helion.pl
WWW: http://helion.pl (księgarnia internetowa, katalog książek)

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
http://helion.pl/user/opinie/hakand
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Printed in Poland.

SPIS TREŚCI

CZĘŚĆ I CO MUSZĘ WIEDZIEĆ?

CZĘŚĆ II PORADNIKI DOTYCZĄCE KONKRETNYCH URZĄDZEŃ I PRODUCENTÓW

2

ROOTOWANIE URZĄDZEŃ Z ANDROIDEM

W TYM ROZDZIALE:

- Czym jest rootowanie?
- Po co rootować urządzenia z Androidem?
- Tworzenie kopii zapasowej danych przed rootowaniem.
- Różne techniki rootowania urządzeń z Androidem.
- Jak uzyskać dostęp do konta root w dwóch konkretnych urządzeniach?

Prawdopodobnie słyszałeś, jak lokalny ekspert od Androida wspominał o rootowaniu. A może przeczytałeś w sieci o rootowaniu urządzeń z Androidem? Rootowanie może wydawać się magiczne i tajemnicze, jest to jednak dość proste zagadnienie. Rootowanie zapewnia właścicielowi większą kontrolę nad urządzeniem i dostęp do niego.

Najwyższy poziom uprawnień w Linuksie uzyskuje się po zalogowaniu do konta root (nazywanego czasem kontem administratora lub superużytkownika). Pojęcia „root", „administrator" i „superużytkownik" oznaczają w tym kontekście to samo.

Skąd się wzięła nazwa „root"?

Pojęcie „root" (czyli korzeń) powstało z uwagi na hierarchiczny charakter systemu plików i uprawnień w systemach UNIX oraz Linux. Gałęzie systemu plików i hierarchia użytkowników przypominają w nich odwrócone drzewo. Katalog *root* w systemie plików jest nadrzędny względem wszystkich plików i katalogów. W systemie uprawnień root to nadrzędny element dla wszystkich uprawnień, dający najwięcej możliwości.

Uprawnienia root w systemach linuksowych zapewniają dostęp administracyjny. Po zalogowaniu się na konto root można zrobić prawie wszystko. Użytkownik ma wtedy uprawnienia do odczytu i zapisu danych w większości miejsc systemu plików oraz może zmieniać ustawienia systemowe. Dlatego głównym celem hakera urządzenia z Linuksem jest zalogowanie się na konto root.

To właśnie uzyskanie takiego wysokiego poziomu uprawnień jest celem w czasie rootowania urządzeń z Androidem. Poziom ten jest potrzebny przy wprowadzaniu wielu modyfikacji w takich urządzeniach.

PO CO ROOTOWAĆ URZĄDZENIE?

Korzyści płynące z rootowania urządzeń to między innymi oszczędność pieniędzy (ponieważ można wydłużyć czas korzystania z urządzenia i zwiększyć przydatność sprzętu), a także możliwość naprawienia błędów popełnionych w czasie rozwijania systemu i produkcji. Inne zalety to uzyskanie dodatkowych funkcji i zniesienie ograniczeń wbudowanych przez operatora lub producenta. Jednak korzystanie z aplikacji administracyjnych jest związane z pewnymi zagrożeniami, ponieważ użytkownik ma dostęp do wszystkich danych z wszystkich aplikacji zainstalowanych w urządzeniu. Na szczęście ryzyko można ograniczyć, przyznając uprawnienia z poziomu root tylko zaufanym aplikacjom.

ZWIĘKSZANIE CZASU ŻYCIA URZĄDZENIA

Pewien mój współpracownik kupił jedno z pierwszych urządzeń z Androidem, HTC Dream (znane także jako G1). Matt uwielbiał ten telefon, jednak szybko odkrył, że nowsze wersje Androida działają w urządzeniu wolno lub w ogóle nie chcą się uruchomić.

Po wprowadzeniu wersji Éclair Androida dla producentów i operatorów nieopłacalne było inwestowanie w rekompilowanie Androida pod kątem starszego sprzętu oraz naprawianie błędów. Dla urządzenia G1 Matta ostatecznie pojawiła się nowa wersja platformy, ale stało się to dopiero po pewnym czasie. Operatorzy i producenci wolą, kiedy użytkownicy kupują nowe urządzenia z najnowszą wersją Androida. Jednak programiści ze społeczności związanej z Androidem i hakowaniem telefonów tworzą odmiany nowych wersji Androida przeznaczone dla starszych urządzeń. Pozwala to wydłużyć czas życia takich urządzeń przez wzbogacenie ich o dodatkowe możliwości i funkcje. Pojedynczy programiści (na przykład Koushik „Koush” Dutta) i całe zespoły zajmują się dostosowywaniem nowych wersji Androida do starszych urządzeń długo po tym, jak producenci i operatorzy przestaną świadczyć pomoc techniczną dla danego sprzętu. Aby zainstalować nowszą wersję Androida w starszym urządzeniu, trzeba zrootować sprzęt i uzyskać pełny dostęp do systemu plików.

Matt na co dzień nadal używa swojego G1. Dzięki hakerom z serwisu XDA i społeczności skupionej wokół Androida na urządzeniu działa wersja Froyo. Producenci nie planowali, że G1 będzie w użyciu tak długo. Matt musiałby kupić przynajmniej dwa inne urządzenia po G1, aby mieć fabrycznie zainstalowane funkcje Androida Froyo. Dzięki dostępowi do konta root Matt będzie korzystał z G1 jeszcze przez pewien czas (tak, odpowiada mu to).

NAPRAWIANIE USTEREK FABRYCZNYCH

Z powodu błyskawicznych zmian w branży sprzętu przenośnego zbyt wiele urządzeń z Androidem ma fabryczne usterki. Niektóre problemy są drobne i dotyczą przerywania połączeń lub wolnego zapisu danych na karcie SD. W innych urządzeniach występują poważne usterki. Na przykład urządzenie Samsung Galaxy X (sprzedawane przez Verizon pod nazwą Fascinate, a przez innych operatorów pod jeszcze innymi nazwami) ma atrakcyjne, zakrzywione kształty, które jednak powodują, że antena GPS-u znalazła się w nieodpowiednim miejscu. Z tej przyczyny domyślny kod do przetwarzania sygnału GPS błędnie określa lokalizację lub w ogóle sobie z tym nie radzi. Tak więc w tym pięknym i wydajnym urządzeniu występuje niepotrzebna i irytująca (a zdaniem niektórych nieakceptowalna) usterka.

Na forach XDA i w innych społecznościach hakerów Androida zwykle dość szybko pojawiają się rozwiązania usterek projektowych — choć rozwiązanie problemów sprzętowych za pomocą oprogramowania bywa trudne, a nawet niemożliwe. Jednak zainstalowanie poprawki często wymaga dostępu do zapisu plików systemowych, do czego z kolei niezbędne są uprawnienia na poziomie root. Użytkownicy Androida przyzwyczaili się do tego, że każdy defekt (i każdą niewygodę) można naprawić za pomocą poprawek opracowanych przez społeczność hakerów Androida. Mówi się, że nawet producenci czasem czekają na pojawienie się poprawek przygotowanych przez społeczność, aby zobaczyć, jak rozwiązać problem.

Nazwy kodowe wersji Androida

Pierwsza wersja Androida nie miała nazwy, jednak dla każdej następnej odmiany w Google'u wymyślano nazwę projektu. Pierwsze urządzenie z Androidem, które zyskało popularność, nazywało się G1. Działała w nim wersja 1.5 Android (Donut).

Ktoś z firmy Google musi lubić słodycze, ponieważ nazwy wszystkich wersji (począwszy od wersji Donut, czyli pączek) pochodzą od nazw łakoci. Kolejne wersje to Éclair (eklerka), Froyo (rodzaj deseru z mrożonego jogurtu), Gingerbread (piernik) i Honeycomb (czyli plaster miodu; ta nazwa to odejście od wyrobów cukierniczych — tu pomysłodawcy zdecydowali się uhonorować naturalną słodkość). Najnowszą wersję, Android 4.0, nazwano Ice Cream Sandwich (kanapka lodowa).

ZWIĘKSZANIE MOŻLIWOŚCI

Wielu producentów tworzy urządzenia z komponentami, których możliwości nie są wykorzystywane. W licznych urządzeniach z Androidem możliwe jest na przykład odbieranie sygnału stacji radiowych FM, jednak funkcji tej nigdy nie wykorzystano. Nie powstały też aplikacje przeznaczone do odbioru radia. Dzięki pracy społeczności skupionej wokół Androida w urządzeniu Nexus One można zarówno odbierać stacje FM, jak i nagrywać obraz w rozdzielczości 720p.

Przetaktowanie

Prawie każde urządzenie z Androidem jest wyposażone w procesor, który może działać szybciej od ustawień fabrycznych. Procesory często są spowalniane w celu wydłużenia czasu pracy na baterii i zmniejszenia zagrożenia przegrzaniem. Standardowo urządzenia Xoom działają z szybkością 1 GHz, jednak mogą bezpiecznie i stabilnie pracować z szybkością 1,4 – 1,5 GHz. Zapewnia to bardzo duży wzrost wydajności w i tak świetnym urządzeniu. Także w licznych innych urządzeniach z Androidem można przyspieszyć pracę procesora. Zwiększa to wydajność i zapewnia użytkownikom dodatkowe możliwości, co jest dobrym powodem do rootowania urządzeń. Przyspieszanie procesora to tak zwane przetaktowanie (ang. *overclocking*).

Tworzenie przenośnego hotspotu

Wielu operatorów produkuje urządzenia działające jak bezprzewodowy punkt (przenośny hotspot), z którym można się połączyć jak ze standardowym hotspotem Wi-Fi. Takie urządzenia umożliwiają noszenie hotspotu ze sobą. Przenośny hotspot przesyła dane przez sieć komórkową — podobnie jak telefon. Urządzenie przenośne żądające danych z internetu i przenośny hotspot pobierający takie dane pod względem funkcjonalnym są podobne do siebie. Hotspoty często kosztują tyle, co smartfony, i wymagają wykupienia drogiego abonamentu na transfer danych (obok abonamentu na dostęp do tych samych danych przez urządzenie z Androidem).

Po zrootowaniu urządzenia z Androidem można korzystać z telefonu jak z przenośnego hotspotu. Warto mieć możliwość utworzenia w razie potrzeby tymczasowego hotspotu. Biznesmen w czasie podróży służbowej może tego potrzebować dość często. Ponieważ użytkownik płaci operatorowi za dane, powinien móc decydować, jak chce z nich korzystać. Większość producentów wyłącza omawianą funkcję w urządzeniach z Androidem (chyba że użytkownik wykupi drogi pakiet dla hotspotu), a dla operatorów korzystne jest, aby klienci kupowali więcej urządzeń i droższe abonamenty. Warto też zauważyć, że używanie telefonu jako hotspotu często stanowi naruszenie warunków korzystania z usługi, dlatego zachowaj ostrożność.

Przetaktowanie urządzenia

Przetaktowanie polega na przyspieszeniu procesora. Nazwa pochodzi od mierzonych w hercach taktów zegara, w których określa się szybkość komputerów. Wartości 500 MHz, 800 MHz czy 1 GHz określają, ile taktów zegara jest wykonywanych w procesorze w ciągu milisekundy. Przetaktowanie oznacza wymuszenie wyższej szybkości taktowania od domyślnej. Zwykle związane jest to ze zwiększeniem napięcia układu, co prowadzi do większego zużycia energii, generowania większej ilości ciepła i — co najważniejsze — przyspieszenia pracy urządzenia.

Wady przetaktowania to zwiększenie emisji ciepła i skrócenie czasu pracy na baterii, co może prowadzić też do skrócenia życia urządzenia. Producenci całymi miesiącami wyznaczają odpowiednie taktowanie sprzętu na podstawie rozmieszczenia układów, oczekiwanego czasu życia, rozpraszania ciepła itd.

DOSTOSOWYWANIE URZĄDZENIA DO POTRZEB

Choć prawdopodobnie nie jest to najważniejszy czynnik, dla hakerów często pierwszym powodem rootowania urządzenia jest chęć uzyskania pełnej kontroli nad wyglądem i działaniem urządzenia. Jeśli użytkownik nie może zapisywać danych w systemie plików, wprowadzone zmiany będą tymczasowe lub ograniczone.

Po zainstalowaniu niestandardowego programu przywracania danych można zapisywać dane w całym systemie plików, w tym w miejscach, których zwykle w ogóle nie można modyfikować. Instalowanie niestandardowego firmware'u zwykle polega na dodawaniu firmware'u lub jądra z grafiką i układami interfejsu, skryptami, pakietami aplikacji itd. Czas potrzebny na przygotowanie takich zmian zniechęca większość użytkowników do ich wprowadzania. Jednak zaangażowani programiści poświęcają długie godziny na modyfikowanie domyślnego firmware'u i udostępniają go w postaci ROM-ów lub innych pakietów, pozwalających osobom z dostępem do konta root szybko wprowadzać duże zestawy zmian. Wielu programistów udostępnia nowe pakiety ROM (lub informacje o nich) na forach XDA.

TWORZENIE KOPII ZAPASOWEJ DANYCH

Większość danych jest bezpieczna w trakcie rootowania. Jednak w czasie rootowania lub odblokowywania urządzeń niektóre aplikacje i ich dane są usuwane. Na przykład opisany w rozdziale 3. proces odblokowywania za pomocą Fastboota prowadzi do wykasowania partycji */data*. Dlatego należy utworzyć kopię ważnych danych i pamiętać o tym, że hakowanie może prowadzić do utraty wszystkich informacji.

Po udanym zrootowaniu urządzenia utworzenie kopii całego systemu plików Androida jest bardzo łatwe. Pozwala to zachować spokój w czasie wymiany lub modyfikowania urządzeń. W zrootowanym urządzeniu można albo wykonać kompletną kopię zapasową za pomocą narzędzia NANDroid (jeśli dostępny jest program do przywracania systemu), albo zarchiwizować dane konkretnych aplikacji, używając programu Titanium Backup lub podobnego narzędzia.

DANE KONTAKTOWE

Google przechowuje wszystkie numery telefonu i adresy e-mail z książki adresowej w chmurze danych (czyli na serwerach Google'a). W momencie aktywowania telefonu z wykorzystaniem loginu wszystkie dane są przesyłane z powrotem do telefonu. Jeśli użytkownik specjalnie nie utworzył danych przechowywanych tylko w telefonie, urządzenie z Androidem automatycznie synchronizuje wszystkie dane z serwerami Google'a, dlatego nie trzeba się martwić o utratę informacji.

Rootowanie telefonu lub innego urządzenia z Androidem często prowadzi do przywrócenia ustawień fabrycznych, co jest związane z wykasowaniem informacji (w tym danych kontaktowych). Oznacza to, że trzeba zarejestrować konto Google i zsynchronizować wszystkie informacje. Wiele uruchamianych jednym kliknięciem metod rootowania, powodujących uruchomienie exploita w urządzeniu, nie prowadzi do wykasowania danych, jednak zawsze warto tworzyć kopię zapasową informacji.

APLIKACJE I ICH DANE

Podobne uwagi dotyczą aplikacji ze sklepu Google Apps Marketplace. W czasie pobierania i instalowania aplikacji na serwerach Google'a zapisywane są dane łączące login z określonym programem. Po ponownym aktywowaniu urządzenia z wykorzystaniem loginu następuje automatyczna synchronizacja ze sklepem Google Apps Marketplace i instalacja wszystkich brakujących aplikacji.

Rozruch z karty SD

Rootowanie niektórych urządzeń z Androidem, na przykład tabletów Nook Color i WonderMedia, wymaga niestandardowej karty SD. Na takiej karcie przy użyciu komputera trzeba zapisać specjalny system plików i skrypt aktualizacji. Tak przygotowaną kartę SD należy umieścić w urządzeniu i ponownie je włączyć. Rozruch urządzenia odbywa się z karty SD, co pozwala zainstalować niestandardowe programy rozruchowe i firmware.

Jeśli z forum XDA dowiesz się, że urządzenie potrzebuje do rozruchu karty SD, najlepiej jest użyć odrębnej karty tego rodzaju, na której nie przechowujesz danych. Większość technik tworzenia rozruchowych kart SD powoduje całkowite wykasowanie zapisanych na niej danych.

Choć aplikacje są przywracane, powiązane z nimi dane zostają zwykle utracone, chyba że użytkownik utworzył kopię zapasową lub zapisał informacje na karcie SD. W niektórych urządzeniach kasowane są też wszystkie dane użytkownika, na przykład zdjęcia i dokumenty. Jeśli dane utworzone przez aplikację są dla Ciebie ważne, warto się dowiedzieć, jak zarchiwizować informacje i je przywrócić (poszukaj na forum XDA). Najlepiej jest przyjąć, że w trakcie hakowania wykasowane zostaną wszystkie dane.

DANE NA KARCIE SD

Android zapisuje zdjęcia i filmy na karcie SD. Warto zarchiwizować te dane przed rozpoczęciem hakowania. Dane z karty SD w urządzeniu z Androidem są zwykle bezpieczne w czasie rootowania. Jednak zawsze warto zastosować protokół Media Transport Protocol (w większości urządzeń z Androidem 3.0 i nowszymi wersjami; w pozostałych może to być pamięć USB) lub polecenie PULL w ADB (zobacz rozdział 3.) i skopiować wszystkie dane z karty SD do katalogu z kopią zapasową na komputerze.

JAK ZROOTOWAĆ URZĄDZENIE I UWOLNIĆ SIĘ SPOD KONTROLI PRODUCENTA?

Przebieg procesu rootowania urządzenia z Androidem zależy od modelu sprzętu. Dla urządzeń, które są dostępne już stosunkowo długo, może istnieć kilka metod rootowania. W następnym punkcie opisano, jak zrootować dwa konkretne urządzenia. W rozdziałach 3. i 4. omówiono większość umiejętności oraz narzędzi potrzebnych w tym procesie.

Oto ogólne kategorie technik rootowania:

- wykorzystanie fabrycznego narzędzia do zastępowania oprogramowania w celu zapisania firmware'u;
- zastosowanie exploitów;
- zastępowanie oprogramowania za pomocą wbudowanego narzędzia Fastboot;
- użycie skryptu lub techniki automatycznej.

Są to bardzo ogólne i subiektywnie wybrane kategorie, wymyślone na potrzeby tego podrozdziału. Wielu programistów prawdopodobnie nie zgodzi się z tym, do której kategorii przypisałem opracowane przez nich metody lub narzędzia.

Dostępne metody rootowania można znaleźć na forum XDA poświęconym konkretnemu urządzeniu. Na przykład informacje i procedury związane z moim tabletem Xoom znajdują się na podforum Xoom Android Development na forum Motorola Xoom (*http://forum.xda-developers.com/forumdisplay.php?f=948*). Większość sprawdzonych procedur jest przyklejona w górnej części listy wpisów, co pozwala łatwo znaleźć potrzebne informacje.

Niezależnie od tego, czy program rozruchowy lub program do przywracania systemu jest zastępowany za pomocą przeznaczonego do tego oprogramowania, exploita czy Fastboota, zasada postępowania jest taka sama — uzyskanie dostępu do konta root to pierwszy krok na drodze do dostosowania urządzenia.

FABRYCZNE NARZĘDZIA DO ZASTĘPOWANIA OPROGRAMOWANIA

W niektórych urządzeniach przy pierwszym rootowaniu trzeba wykorzystać fabryczne narzędzia diagnostyczne lub do zastępowania oprogramowania. Po zastąpieniu firmware'u i uzyskaniu dostępu do konta root zwykle do wprowadzania dalszych zmian używa się niestandardowego programu do przywracania systemu.

Dostęp do konta root często można uzyskać tylko przez zastąpienie kompletnego podpisanego pakietu firmware'u za pomocą fabrycznych narzędzi. Jeśli dane narzędzie wymaga zewnętrznego programu (innego niż wbudowane narzędzia z pakietu SDK Androida, czyli ADB — ang. *Android Debug Bridge* — i Fastboot), aby po raz pierwszy zapisać nowy firmware, potrzebny będzie kompletny podpisany pakiet firmware'u. Pierwsza technika rootowania Droida 1 polega na zastosowaniu narzędzia serwisowego RSDLite Motoroli w celu załadowania niestandardowego programu rozruchowego do sekcji rozruchowej systemu plików. Podobnie w wielu urządzeniach z procesorem NVIDIA Tegra 2 trzeba używać programu NVFlash, a w urządzeniach Samsunga — narzędzia ODIN.

Zdobywanie wiedzy

Bardzo ważne jest to, aby zapoznać się z wszystkimi dostępnymi informacjami na temat używanego urządzenia. Przeczytaj wstępne instrukcje na temat rootowania i wszystkie przyklejone wpisy. Przejrzyj cały wątek dotyczący rootowania danego urządzenia. Poświęć kilka dni na samo przeczytanie doświadczeń innych osób, które rootowały i romowały to urządzenie lub zmieniały w nim kompozycję. Większości błędów popełnianych przez początkujących można łatwo uniknąć, potrzebne są jednak cierpliwość i zapoznanie się z wszystkimi materiałami na temat danego urządzenia. Hakerzy są samoukami i bardzo cierpliwymi stworzeniami.

Ponieważ bierzesz na siebie ryzyko i odpowiedzialność związane z uszkodzeniem sprzętu (lub jego usprawnieniem), uczestnictwo w społeczności hakerów oraz użytkowników rootujących urządzenia powinieneś traktować bardziej jak maraton niż sprint. Dużo czytaj, a pytania zadawaj dopiero po tym, jak nie uda Ci się znaleźć odpowiedzi za pomocą funkcji wyszukiwania na forum XDA.

Szczególnie ważne jest, aby przed rozpoczęciem rootowania nauczyć się, jak przywrócić do stanu używalności uszkodzone urządzenie (jeśli w ogóle jest to możliwe). W tym celu wpisz w wyszukiwarce na forum XDA słowo „unbrick" wraz z nazwą swojego urządzenia.

Czasem jedynym sposobem na przywrócenie uszkodzonego urządzenia do stanu używalności jest zastosowanie fabrycznych narzędzi do zastępowania oprogramowania.

Oto zalety stosowania takich narzędzi:

- są one zwykle stosunkowo bezpieczne i proste w użyciu;
- proces obejmuje niewielką liczbę prostych kroków.

Korzystanie z fabrycznych narzędzi ma też wady:

- niektóre z nich bywają trudne w użyciu lub do zrozumienia; w najlepszym razie mają ubogi interfejs, w najgorszym — interfejs jest w niezrozumiałym języku;
- fabryczne narzędzia diagnostyczne są trudne do zdobycia (i trudno znaleźć ich aktualną wersję).

EXPLOITY

W systemach operacyjnych występują słabe punkty (lub luki), które hakerzy mogą wykorzystać, pisząc exploity. Istnieje wiele rodzajów i postaci exploitów. Jedną z pierwszych metod rootowania urządzenia EVO 4G było wykorzystanie luki w zabezpieczeniach aplikacji Adobe Flash.

W świecie linuksowych systemów operacyjnych wykorzystywanie luk jest po części nauką, po części sztuką, a w dużym stopniu opieraniem się na intuicji wynikającej z doświadczenia. Znalezienie słabego punktu, który można wykorzystać, jest pierwszym celem społeczności programistów po pojawieniu się nowego urządzenia. Zaawansowani hakerzy i geekowie ścigają się ze sobą, aby znaleźć w kodzie lukę, która pozwoli odblokować zabezpieczenia. Na forum XDA wątki z analizą różnych możliwości obejmują czasem tysiące wpisów.

Korzystanie z exploitów to jeden z najprzyjemniejszych sposobów rootowania urządzeń z Androidem. Mniej więcej w połowie rootowania mojego pierwszego urządzenia HTC Thunderbolt za pomocą exploita ASH (opracowanego przez Scotta Walkera) pomyślałem: „Nieźle, naprawdę hakuję urządzenie. Czuję się jak postać z *Mission Impossible*". Exploit `psneuter` Scotta Walkera (pseudonim scotty2walker w społeczności hakerów Androida) to dobry przykład prostego exploita, który wykonuje ciekawe operacje w celu uzyskania dostępu do konta root. Scott wykorzystał to, że program ADB (zobacz rozdział 3.) w sytuacji, kiedy nie może ustalić wartości opcji `S-ON` i `S-OFF`, przyjmuje tę drugą oraz domyślnie montuje system plików w trybie do odczytu i zapisu przy zdalnym dostępie do powłoki niezrootowanego urządzenia. Ten prosty exploit można wykorzystać do nadpisania zwykle niedostępnych fragmentów systemu plików, na przykład sekcji rozruchu i przywracania systemu.

Nie mam wystarczającego doświadczenia ani odpowiednich umiejętności programistycznych, aby napisać exploit `psneuter`, jednak Scott Walker udostępnił swój kod społeczności Androida. Dlatego mogę go wykorzystać do odblokowania mojego urządzenia z Androidem. Nigdy nie bawiłem się lepiej niż w czasie nauki hakowania nowych urządzeń z Androidem z pomocą społeczności z forum XDA.

Oto zalety stosowania exploitów:

- umożliwiają dostęp do ściśle zabezpieczonych urządzeń;
- ich używanie jest ciekawe (można się poczuć jak haker);
- dla producentów zwykle trudne jest przygotowanie poprawek zabezpieczających przed exploitami;
- każdy może je stosować, wykorzystując wiedzę zawartą w tej książce.

A oto wady korzystania z exploitów:

- proces ich stosowania jest złożony — wymaga wiedzy i umiejętności;
- łatwo jest popełnić błąd;
- istnieje duże prawdopodobieństwo uszkodzenia sprzętu.

ZASTĘPOWANIE OPROGRAMOWANIA ZA POMOCĄ WBUDOWANEGO NARZĘDZIA FASTBOOT

Jeśli urządzenie nie jest zablokowane (lub nie można go zablokować), można przejść do trybu Fastboot i uruchamiać w nim polecenia. Fastboot umożliwia wykorzystanie całego zestawu plików lub systemu plików spakowanego do jednego pliku (tak zwanego obrazu) i zapisanie go w wybranych obszarach systemu plików, na przykład w katalogu *boot* lub *system*.

Większość „google'owych" urządzeń pierwszej generacji, na przykład Nexus One, Xoom czy Nexus S, ma programy rozruchowe, których nie można zablokować, co pozwala wyłączyć zabezpieczenia (opcja `S-OFF`) — zwykle odbywa się to za pomocą polecenia Fastboota. Jednak nie wszystkie urządzenia mają wbudowaną obsługę tego protokołu. Oznacza to, że jeśli producent nie uwzględnił możliwości wywoływania poleceń Fastboota z poziomu komputera, nie można z nich korzystać. Polecenia tego protokołu i jego możliwości omówiono w rozdziale 3.

Poniżej wymieniono zalety korzystania z Fastboota:

- instrukcje są proste do zrozumienia i dość łatwo jest je wykonać;
- technika ta jest prosta i stosunkowo bezpieczna.

Oto wady stosowania Fastboota:

- nie wszystkie urządzenia go obsługują;
- potrzebna jest umiejętność korzystania z wiersza poleceń;
- odblokowywanie za pomocą fabrycznego narzędzia Fastboot powoduje usunięcie danych z partycji */data* urządzenia.

Dyskusje na temat rootowania za pomocą skryptów i narzędzi uruchamianych jednym kliknięciem

W społeczności skupionej wokół Androida wciąż trwa dyskusja dotycząca skryptów i technik uruchamianych jednym kliknięciem. Niektórzy programiści obawiają się, że producenci zaczną utrudniać stosowanie tych technik. Inni twierdzą, że ułatwienie rootowania obniży poprzeczkę dla potencjalnych hakerów. Im łatwiej będzie zrootować urządzenia, tym więcej osób zacznie uszkadzać je i próbować wymienić na gwarancji. Doprowadzi to do tego, że producenci zaczną utrudniać rootowanie nowych urządzeń.

TECHNIKI OPARTE NA SKRYPTACH I JEDNYM KLIKNIĘCIU

Jest to pojemna kategoria, obejmująca zarówno bardzo zaawansowane techniki (na przykład metodę rootowania unRevoked), jak i proste skrypty dla narzędzia ADB. W metodach opartych na skryptach użytkownik musi zwykle wykonać znacznie mniej operacji niż przy stosowaniu wieloetapowych metod rootowania z wykorzystaniem ADB lub narzędzi fabrycznych. Dlatego omawiane tu podejście jest zwykle prostsze i mniej zawodne. Niestandardowe techniki elektroniczne, takie jak unRevoked, opierają się na zastrzeżonym połączeniu USB lub wymagają uruchomienia aplikacji bezpośrednio w urządzeniu. Jednak także te zastrzeżone metody wykonują podstawowe operacje — zastępują w systemie plików program rozruchowy lub program do przywracania systemu.

Ważną zaletą stosowania technik skryptowych i wymagających tylko jednego kliknięcia jest znaczne uproszczenie pracy. Ponadto efekt jest osiągany bez długich okresów frustracji.

A oto wady korzystania z opisywanych tu metod:

- haker ma mniejszą kontrolę nad procesem;
- takie techniki są dostępne dla ograniczonej liczby urządzeń.

ROOTOWANIE DWÓCH KONKRETNYCH URZĄDZEŃ

W tym podrozdziale porównano dwie metody rootowania o różnym poziomie trudności, przeznaczone dla dwóch telefonów. Nexus One to telefon dla programistów. Zaprojektowano go pod kątem łatwego rootowania i dostosowywania. Do zrootowania tego urządzenia służy Fastboot. Zrootowanie telefonu Thunderbolt jest trudniejsze. Służy do tego exploit `psneuter`.

Nie martw się, jeśli nie zrozumiesz niektórych pojęć. Poznasz je w trakcie dalszej lektury.

NEXUS ONE

W tym punkcie opisano odblokowywanie i rootowanie telefonu Nexus One. Google umieścił w programie rozruchowym usuwalną blokadę, dlatego najpierw należy odblokować urządzenie, używając narzędzia dla programistów, Fastboota. Po odblokowaniu telefonu można go łatwo zhakować i zrootować. Jeśli producent umożliwia społeczności odblokowanie urządzenia, wykonywanie wszystkich późniejszych operacji jest prostsze.

1. Podłącz telefon Nexus One do komputera za pomocą kabla USB.
2. Przełącz telefon w tryb Fastboot. W tym celu uruchom urządzenie, przyciskając odpowiednią kombinację klawiszy (dla poszczególnych urządzeń jest ona różna). Tryb Fastboot powoduje obsługę przez telefon poleceń Fastboota.
3. W oknie wiersza poleceń na komputerze uruchom następującą instrukcję, aby odblokować program rozruchowy:

   ```
   fastboot OEM unlock
   ```
4. Ponownie uruchom telefon w trybie Fastboot.
5. Uruchom skrypt, aby zainstalować w urządzeniu program rozruchowy superboot.

Na tym etapie telefon Nexus One jest w pełni zrootowany.

HTC THUNDERBOLT

Trudniejszy proces rootowania przedstawiono na przykładzie telefonu Thunderbolt firmy HTC. Firma ta zablokowała program rozruchowy i bardzo utrudniła dostęp do systemu plików poprzez konto root. W omówieniu widać, że zablokowany program rozruchowy zwiększa złożoność procesu rootowania. Tu przedstawiono poszczególne kroki w ogólny sposób. Szczegóły znajdziesz w rozdziale 9.

1. Podłącz telefon Thunderbolt do komputera za pomocą kabla USB.
2. Wykorzystaj narzędzie programistyczne ADB do umieszczenia na karcie SD następujących plików:
   - skryptu z exploitem `psneuter`,
   - narzędzia BusyBox,
   - pliku obrazu nowego programu rozruchowego.
3. Za pomocą poleceń powłoki narzędzia ADB zmień uprawnienia dla skryptu `psneuter` i narzędzia BusyBox, tak aby można wykonywać ich kod.
4. Za pomocą poleceń powłoki narzędzia ADB uruchom skrypt z exploitem `psneuter`, aby uzyskać tymczasowy dostęp do systemu plików z poziomu konta root.
5. Uruchom polecenie MD5SUM narzędzia BusyBox, aby się upewnić, że plik obrazu jest identyczny z oryginałem.
6. Wywołaj polecenie DD narzędzia BusyBox, aby zapisać plik obrazu w sekcji pamięci, gdzie znajduje się program rozruchowy.

7. Za pomocą poleceń powłoki narzędzia ADB zapisz na karcie SD starszy firmware podpisany przez producenta.
8. Ponownie uruchom telefon i zainstaluj podpisany starszy firmware.
9. Za pomocą narzędzia programistycznego ADB zapisz na karcie SD następujące pliki:
   - skrypt z exploitem `psneuter`,
   - narzędzie BusyBox,
   - skrypt `wpthis`.
10. Ustaw odpowiednie uprawnienia dla skryptu `psneuter` i uruchom go, aby uzyskać dostęp do konta root z poziomu powłoki narzędzia ADB.
11. Ustaw uprawnienia dla skryptu `wpthis` i uruchom go, aby uzyskać dostęp do zablokowanego programu rozruchowego.
12. Za pomocą narzędzia ADB umieść obraz nowego programu rozruchowego na karcie SD.
13. Zastąp domyślny program rozruchowy pierwszego poziomu nowym programem rozruchowym.
14. Wywołaj instrukcję MD5SUM, aby się upewnić, że skrót nowego programu rozruchowego jest zgodny z plikiem obrazu.
15. Jeśli instrukcja MD5SUM informuje o niezgodnym skrócie, powtarzaj kroki 12. – 14. do czasu uzyskania zgodności.
16. Zapisz nowy, niepodpisany i niestandardowy firmware systemu na karcie SD.
17. Ponownie uruchom telefon. Nowy program rozruchowy wczyta teraz niestandardowy firmware.

Na tym etapie w telefonie Thunderbolt działa program rozruchowy z opcją `S-OFF`. Potrzebnych jest dziesięć dalszych kroków, aby zainstalować aplikację SuperUser i uzyskać trwały dostęp do konta root. Jak widać, rootowanie urządzenia z zablokowanym fabrycznie programem rozruchowym jest znacznie trudniejsze niż rootowanie odblokowanego urządzenia. Hakowanie zablokowanego sprzętu, tak aby uzyskać w pełni odblokowany telefon, daje tak dużo satysfakcji, że kiedy uda Ci się uzyskać pożądany efekt, zaczniesz szukać innych urządzeń do zrootowania.

ROOTOWANIE TO DOPIERO POCZĄTEK

Zrootowanie urządzenia to dopiero początek. Aby zainstalować niestandardowy firmware, tak zwany ROM, potrzebny jest dostęp do konta root. Jest on konieczny także w celu usunięcia bloatware'u, czyli dodatkowego oprogramowania umieszczanego w urządzeniu przez producenta lub operatora.

Bloatware

Jak wspomniano w rozdziale 1., operatorzy i producenci pobierają od usługodawców oraz twórców oprogramowania opłaty za umieszczanie aplikacji w urządzeniu z Androidem. Pozwala to obniżyć cenę urządzenia (lub zwiększyć premie menedżerów).

Niezależnie od przyczyn instalowania tych aplikacji nie da się ich usunąć bez zrootowania urządzenia. Przypomina to zakup komputera, w którym zainstalowanych jest tylko 19 programów, przy czym producent uniemożliwia użytkownikowi usunięcie 5 zbędnych aplikacji. Tego typu bloatware zajmuje ograniczoną pamięć urządzenia i czasem uruchamia usługi, których dana osoba nie potrzebuje lub nie chce używać. Prowadzi to do zużycia energii i pamięci.

Firma AT&T uniemożliwiła instalowanie w swoich urządzeniach aplikacji spoza sklepu. Dopiero po zrootowaniu można było instalować dowolne aplikacje na standardowo ograniczanych przez operatora telefonach.

W niektórych tańszych tabletach i telefonach nie można nawet instalować aplikacji z oficjalnego sklepu Google Apps Marketplace. Po zrootowaniu takich urządzeń można instalować takie programy, a także uzyskać dostęp do wszystkich opcji z droższych telefonów.

Widać więc, że zrootowanie urządzenia z Androidem otwiera drogę do przejęcia kontroli nad sprzętem. Pozwala znieść blokady narzucone przez operatorów i inne ograniczenia, które mogą skłaniać do zakupu nowych urządzeń.

SKOROWIDZ

B

C

D

E

F

H

J

K

L

M

N

O

P

R

S

T

U

V

W

X

Z

Naucz swój telefon nowych, fantastycznych sztuczek!

System operacyjny Android ma rzeszę fanów. Zdobył ich dzięki swoim niezwykłym możliwościom, imponującej elastyczności oraz ogromowi dostępnych aplikacji. System ten łączy w sobie prostotę ważną dla początkujących użytkowników z możliwościami rozwoju i ingerencji istotnymi dla tych zaawansowanych. Jeżeli masz pomysł, jak ulepszyć Twój system operacyjny, jeżeli chcesz dostosować go do swoich potrzeb, trafiłeś na właściwą książkę!

Dzięki niej dowiesz się, jak skutecznie zrootować Twoje urządzenie i przejąć nad nim pełną kontrolę. To jest pierwszy i najważniejszy krok. Gdy go wreszcie uczynisz, świat pełen różnych wersji ROM-ów, modyfikacji i atrakcyjnych funkcjonalności stanie przed Tobą otworem. W trakcie lektury nauczysz się modyfikować wygląd i styl Twojego Androida, tworzyć pełną kopię bezpieczeństwa oraz wydłużać życie baterii. Znajdziesz tu również szczegółowe informacje na temat rootowania konkretnych modeli telefonów oraz tabletów. Książka ta jest idealną pozycją dla wszystkich chcących wycisnąć jeszcze więcej z telefonów z systemem Android.

Dzięki tej książce:

- przygotujesz środowisko pracy
- zrootujesz swój telefon
- dostosujesz wygląd systemu
- zainstalujesz niestandardowy ROM

WILEY

helion.pl
księgarnia internetowa

Nr katalogowy: 11954

Księgarnia internetowa
http://helion.pl

Zamówienia telefoniczne:
0 801 339900
0 601 339900

Helion

Sprawdź najnowsze promocje:
http://helion.pl/promocje
Książki najchętniej czytane:
http://helion.pl/bestsellery
Zamów informacje o nowościach:
http://helion.pl/nowosci

Helion SA
ul. Kościuszki 1c, 44-100 Gliwice
tel.: 32 230 98 63
e-mail: helion@helion.pl
http://helion.pl

Informatyka w najlepszym wydaniu

ISBN 978-83-246-5682-0

Cena 39,90 zł