WBUDOWANE SYSTEMY OPERACYJNE: UKRYTE ZAGROŻENIE

Wbudowane systemy zawierają własny system operacyjny, zwany „wbudowanym systemem operacyjnym", który jest przedmiotem zainteresowania tego modułu. Wiele osób używa urządzenia GPS (Global Positioning System) lub systemu nawigacyjnego, aby znaleźć bank, aby móc wypłacić gotówkę z bankomatu i nie zdaje sobie sprawy, że zarówno urządzenie GPS, jak i bankomat mogą być wbudowanymi systemami, które wykorzystują wbudowany system operacyjny (OS). Urządzenia podłączone do Internetu (takie jak inteligentne telewizory) są również wbudowanymi systemami i są zwykle określane jako urządzenia IoT. Specjaliści ds. bezpieczeństwa powinni zrozumieć, że każda luka w systemie operacyjnym komputera PC lub serwera może istnieć w przypadku jego wbudowanego odpowiednika. Na przykład wiele wbudowanych systemów operacyjnych zawiera serwer WWW, który jest potencjalnie podatny na ataki. Jeśli oprogramowanie serwera WWW jest wymagane do prawidłowego działania urządzenia, możesz mieć problem. W rzeczywistości problem może być poważniejszy w systemie wbudowanym ze względu na ograniczenia sprzętowe i zgodność oprogramowania. Twórcy oprogramowania często pomijają wiele kontroli bezpieczeństwa w systemach wbudowanych, takich jak walidacja danych wejściowych, aby mogli „zmieścić" kod na chipie. Ponadto presja, aby wprowadzić produkt na rynek tak szybko, jak to możliwe, może skutkować mniej bezpiecznym kodem i ograniczonymi testami bezpieczeństwa. Możesz przeczytać więcej o wyzwaniach związanych z opracowywaniem i zabezpieczaniem systemów wbudowanych w następującym artykule BlackBerry QNX: https://blackberry.qnx.com/en/embeded-system-security/ultimate-guide/. Przeprowadzając testy bezpieczeństwa dla firmy, nie ignoruj systemów wbudowanych. Nie powinieneś pomijać urządzeń, ponieważ są małe, wykonują proste zadania lub nie były eksploatowane w przeszłości. Jako tester bezpieczeństwa, częścią Twojej pracy będzie identyfikacja potencjalnych problemów bezpieczeństwa, a aby to zrobić, musisz myśleć nieszablonowo. W przypadku luk w zabezpieczeniach systemów wbudowanych, być może będziesz musiał zacząć myśleć również „szablonowo".

WPROWADZENIE DO WBUDOWANYCH SYSTEMÓW OPERACYJNYCH

W najprostszej postaci, wbudowany system to dowolny system komputerowy, który nie jest uniwersalnym komputerem PC lub serwerem. Oprócz urządzeń GPS i niektórych bankomatów, wbudowane systemy można znaleźć w szerokiej gamie elektronicznych produktów konsumenckich i przemysłowych: zabawkach, urządzeniach kuchennych, drukarkach, systemach sterowania przemysłowego, statkach kosmicznych i sprzęcie naukowym. Wbudowany system operacyjny (OS) może być małym programem opracowanym specjalnie do użytku z wbudowanymi systemami lub może być uproszczoną wersją systemu operacyjnego powszechnie używanego w komputerach ogólnego przeznaczenia. Wbudowane systemy operacyjne są zazwyczaj projektowane tak, aby były małe i wydajne, więc nie mają niektórych funkcji, które mają uniwersalne systemy operacyjne, szczególnie jeśli specjalistyczne aplikacje, które uruchamiają, nie wykorzystują tych funkcji. Jednym z typów wyspecjalizowanego wbudowanego systemu operacyjnego jest system operacyjny czasu rzeczywistego (RTOS), zwykle używany w urządzeniach takich jak programowalne termostaty, sterowanie urządzeniami, a nawet statki kosmiczne. Jeśli pilotujesz myśliwiec F-35, z pewnością docenisz fakt, że wbudowany system RTOS w Twoim samolocie został zaprojektowany z algorytmem ukierunkowanym na wykonywanie wielu zadań jednocześnie i przewidywalne reagowanie. Systemy RTOS można znaleźć również w wysokiej klasy piekarnikach kuchennych, rozrusznikach serca i niemal każdym nowym pojeździe mechanicznym.

BAJTY BEZPIECZEŃSTWA

Kiedy poznajesz urządzenia wykorzystujące wbudowane systemy operacyjne, musisz myśleć tak, jak atakujący. Jaki system mógłbyś zaatakować, który mógłby wpłynąć na setki systemów? Tysiące systemów? Coś tak prostego, jak atak na system ogrzewania, wentylacji i klimatyzacji (HVAC) firmy — lub nawet termostat — może poważnie zaszkodzić infrastrukturze sieciowej.

Pobieżne przyjrzenie się typowemu budynkowi korporacyjnemu pozwoli Ci znaleźć wiele wbudowanych systemów, w tym zapory sieciowe, przełączniki, routery, urządzenia filtrujące sieć, urządzenia pamięci masowej podłączonej do sieci (NAS), sieciowe przełączniki zasilania, drukarki, skanery, kopiarki, projektory wideo, konsole zasilaczy awaryjnych (UPS), telefony VoIP (Voice over IP) i systemy poczty głosowej, termostaty, systemy HVAC, systemy przeciwpożarowe, systemy telewizji przemysłowej, systemy zarządzania windami, stanowiska i konsole do wideokonferencji oraz systemy interkomowe. Ile wbudowanych systemów potrafisz zidentyfikować w budynku, w którym się znajdujesz?

BAJTY BEZPIECZEŃSTWA

Zhakowanie modelu 3 Tesli było ostatnim testem w corocznym wydarzeniu hakerskim Pwn2Own w 2019 r. Zespół hakerski White Hat Amat Cama i Richard Zhu (występujący pod nazwą Fluoracetate) potrzebował zaledwie kilku minut i kilku linijek kodu, aby zhakować Teslę. Wykorzystali słabość przeglądarki systemu „informacyjno-rozrywkowego" i wkrótce ich polecenia były wyświetlane na ekranie konsoli środkowej Tesli. Fluoracetate wygrał większość wyzwań, w których wziął udział, i opuścił konkurencję z nagrodą pieniężną w wysokości 375 000 $ i zupełnie nową Teslą. Luka w zabezpieczeniach została zgłoszona Tesli, a firma samochodowa wydała łatkę, aby wyeliminować lukę.

Wielu odrzuca temat bezpieczeństwa urządzeń wbudowanych, aby skupić się na bardziej popularnych problemach z bezpieczeństwem. Większość nacisku mediów kładzie się na zagrożenia, które ludzie mogą zrozumieć i z którymi mogą się utożsamić, takie jak najnowszy robak sieciowy, najnowszy atak na system Windows lub cyberatak Colonial Pipeline. Jednak systemy wbudowane znajdują się we wszystkich sieciach i wykonują podstawowe funkcje, takie jak kierowanie ruchem sieciowym i blokowanie podejrzanych pakietów. Wielu uważa, że ponieważ urządzenia korzystają z wbudowanego systemu operacyjnego, nikt nie zawracałby sobie głowy ich atakowaniem ani nie poświęcałby czasu i wysiłku na zrozumienie, jak działają. W rzeczywistości często jest odwrotnie. Na przykład trzech hakerów z San Francisco kupiło kilka parkomatów na eBayu, aby właśnie to zrobić — zrozumieć, jak działają urządzenia. Rozebrali parkomaty, szukając zabezpieczeń i sposobów dostępu do wewnętrznego sprzętu z zewnątrz, takiego jak zewnętrzny port USB lub szeregowy. Próbowali również ustalić, czy ktoś mógłby włożyć kartę lub gumę do żucia, na przykład, do urządzenia, aby je wyłączyć, i zbadali, jaki typ karty inteligentnej można by włożyć, jeśli w ogóle. Ich celem było przekonanie miasta San Francisco, że badanie podatności systemu parkomatów jest warte zachodu. Niedawno badacze ds. bezpieczeństwa byli w stanie dokonać inżynierii wstecznej oprogramowania na chipsecie popularnej zapory sieciowej; oprogramowanie znajdujące się na chipie jest powszechnie określane jako oprogramowanie układowe. Następnie badacze wstawili zmodyfikowane oprogramowanie, aby kontrolować zachowanie zapory sieciowej. Hakerzy, którzy to robią, mogą zmodyfikować zaporę sieciową, aby móc kopiować ruch sieciowy przechodzący przez interfejs i przyznać zewnętrznemu adresowi IP pełny dostęp przez zaporę sieciową. Mogą również skonfigurować zaporę sieciową tak, aby te włamania nie zostały wykryte ani nie wygenerowały pojedynczego wpisu w dzienniku. Wraz ze wzrostem wartości i ilości celów z systemami wbudowanymi atakujący zaczną przenosić swoją uwagę na systemy wbudowane.

Badanie ataków na samochód i telewizor Smart TV

Czas trwania: 30 minut

Cel: Dowiedz się więcej o potencjalnych atakach na systemy wbudowane.

Opisy: W 2013 r. Charlie Miler i Chris Valasek pokazali, że potrafią zdalnie sterować kierownicą i hamulcami pojazdu, do którego byli podłączeni. W 2015 r. udowodnili, że z wygody swojego domu mogą włamać się do Jeepa Cherokee jadącego autostradą. Ten zdalny atak zwrócił uwagę kilku osób w branży i na szczęście został odpowiedzialnie zgłoszony przez Charliego i Chrisa, zanim doszło do jakichkolwiek rzeczywistych szkód. W 2019 r. hakerzy wykorzystali podatne urządzenia Chromecast i Google Home, aby wyświetlać wiadomości na telewizorach konsumenckich promujące znaną gwiazdę YouTube'a PewDiePie. Urodzony w Szwecji komik i komentator gier wideo, którego prawdziwe nazwisko brzmi Felix Kjellberg, został wyzwany przez T-Series, indyjską wytwórnię muzyczną i firmę filmową, o pierwsze miejsce w serwisie YouTube. W tym czasie kanały obu YouTuberów miały około 73 milionów subskrybentów.

1. W systemie Windows uruchom przeglądarkę internetową i przejdź do witryny www.google.com.

2. W polu wyszukiwania wpisz Jeep Hack 2015 i naciśnij Enter.

3. Wybierz wpis z witryny www.wired.com i przeczytaj artykuł. Po zakończeniu użyj strzałki wstecz, aby powrócić do strony z wynikami wyszukiwania.

4. Przewiń wyniki wyszukiwania i poświęć czas na przeczytanie dwóch lub trzech innych artykułów o ataku.

5. Jakiego wektora ataku użyli hakerzy? Czy uważasz, że projektanci mogli coś zrobić, aby zapobiec atakowi?

6. Czy uważasz, że przeczytane artykuły zawierały informacje, których inni mogliby użyć do przeprowadzenia podobnych ataków w przyszłości? Uzasadnij swoją odpowiedź.

7. Co mogliby zrobić hakerzy, gdyby byli złośliwi?

8. Powtórz kroki 1–7, ale tym razem wyszukaj Pewdiepie tv hack i przeczytaj artykuł https://threatpost.com. 9. Po zakończeniu zostaw przeglądarkę internetową otwartą na następną aktywność.

Jak dowiedziałeś się w tej aktywności, praca zaledwie dwóch osób mogła spowodować spustoszenie na autostradach w całym kraju. Praca dwóch innych osób oszukała inteligentne telewizory, aby wyświetlały niechciane wiadomości. Twoim zadaniem jako testera bezpieczeństwa jest próba zapobiegania tego typu atakom.

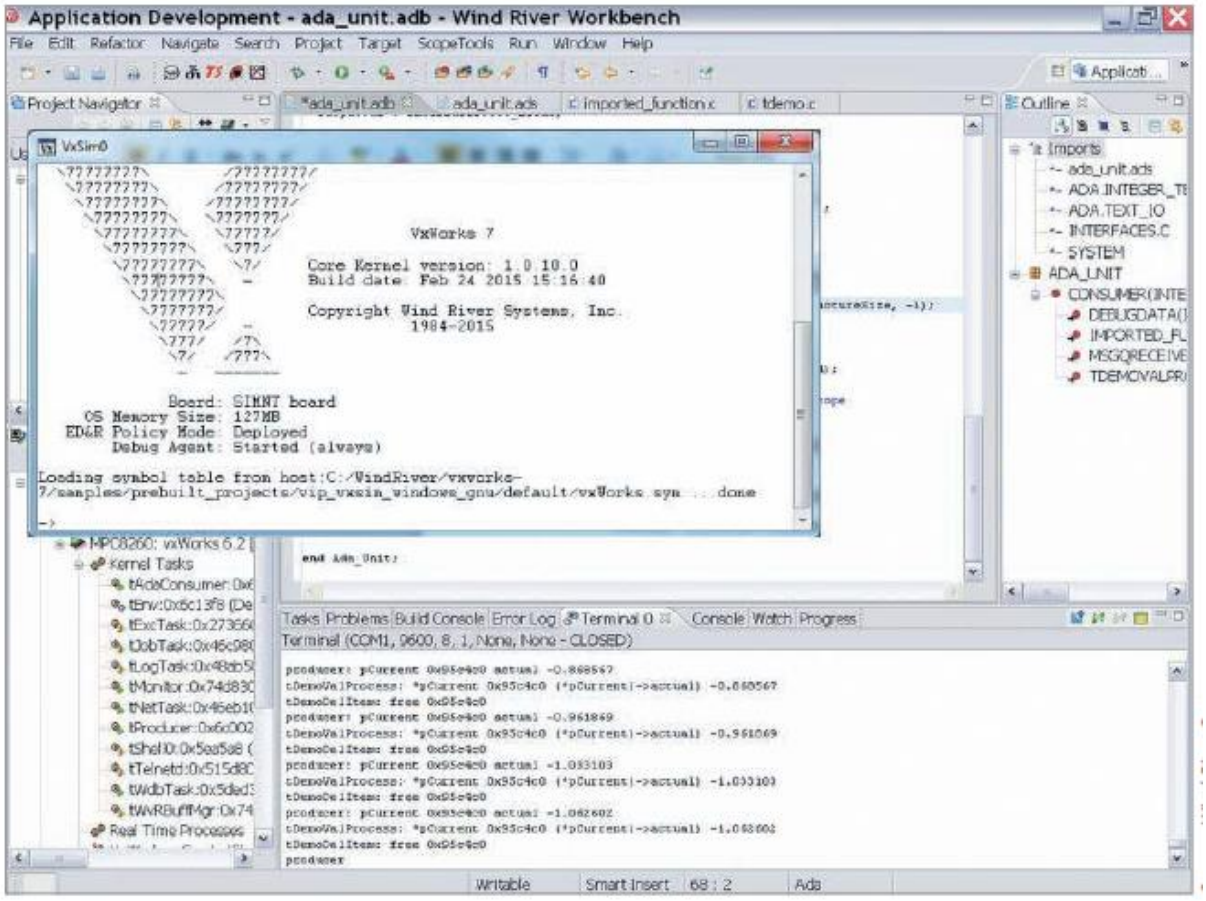
WINDOWS I INNE WBUDOWANE SYSTEMY OPERACYJNE

Recykling wspólnego kodu i ponowne wykorzystywanie technologii to solidne praktyki inżynierii oprogramowania. W końcu, dlaczego miałbyś płacić deweloperowi za wielokrotne pisanie tego samego kodu, skoro możesz go po prostu ponownie wykorzystać? Niestety, takie praktyki wprowadzają typowe punkty awarii w wielu produktach. Wiele wirusów, robaków, trojanów i innych wektorów ataków wykorzystuje współdzielony kod, co zwiększa wpływ, jaki może mieć pojedyncza luka. Już wiesz o lukach w zabezpieczeniach systemów Windows i Linux. Każda luka w zabezpieczeniach tych systemów operacyjnych może również występować w wersji wbudowanej. Na przykład wbudowane wersje systemów Windows 10 i Windows Server 2012 zawierają to samo oprogramowanie i, z niewieloma wyjątkami, działają tak samo jak ich odpowiedniki niewbudowane. Windows XP miał bardzo popularną wersję wbudowaną, z której wiele produktów nadal korzysta nawet po wygaśnięciu rozszerzonego wsparcia w styczniu 2016 r. Windows CE był okrojoną wersją systemu operacyjnego Windows na

komputery stacjonarne i nie należy go mylić z Windows Embedded 8 lub Windows 10 IoT. Część kodu źródłowego Windows CE jest dostępna publicznie, a większość pozostałej części jest dostępna dla dostawców sprzętu, partnerów i deweloperów, w zależności od ich poziomu licencji. Windows CE jest obecnie rzadki, ale nadal warto o nim wiedzieć. Windows Mobile, stary system operacyjny oparty na Windows CE, został zaprojektowany do użytku w produktach takich jak osobiste asystenty danych (PDA) i smartfony. Teraz te starsze urządzenia działają na nieznacznie zmodyfikowanej wersji systemu Windows 10. W przeciwieństwie do Windows CE, Windows 10 IoT zapewnia pełny interfejs API systemu Windows i może wykonywać wiele takich samych zadań, jak wersja na komputery PC, chociaż Windows 10 IoT nie ma interfejsu komputera PC. Jest przeznaczony do użytku na urządzeniach powszechnego użytku, takich jak Raspberry Pi, mały, niedrogi komputer. Oprócz urządzeń powszechnego użytku, Windows 10 IoT może stanowić podstawę każdego z systemów wymienionych wcześniej (tj. GPS-ów, bankomatów i drukarek). Windows 10 IoT został zaprojektowany, aby ułatwić pracę deweloperom. Jak wiadomo, dostępnych jest wiele narzędzi do wykrywania luk w systemach Windows. Niektóre z nich można uruchomić na wbudowanym systemie operacyjnym, a inne można używać zdalnie z sieci, aby wykrywać luki w wbudowanym systemie operacyjnym Windows.

Inne zastrzeżone wbudowane systemy operacyjne

VxWorks to szeroko stosowany wbudowany system operacyjny czasu rzeczywistego opracowany przez Wind River Systems. Jest używany w wielu środowiskach i aplikacjach i został zaprojektowany tak, aby działał wydajnie na minimalnym sprzęcie. W następnej aktywności zbadasz różnorodność systemów obsługiwanych przez VxWorks i inne wbudowane systemy operacyjne. Rysunek przedstawia tworzenie obrazu wbudowanego systemu operacyjnego za pomocą VxWorks Workbench, zestawu narzędzi programistycznych, działającego w wersji Fedora Linux na komputery stacjonarne.



Aby dać ci pojęcie o różnorodności systemów wykorzystujących VxWorks, oto częściowa lista:

• Statek kosmiczny Clementine

• Sonda kosmiczna Deep Impact

• Teleskop kosmiczny Jamesa Webba (w trakcie opracowywania)

• łaziki eksploracji Marsa Spirit i Opportunity

• Lądownik Mars Perseverance

• Lądownik Mars Phoenix

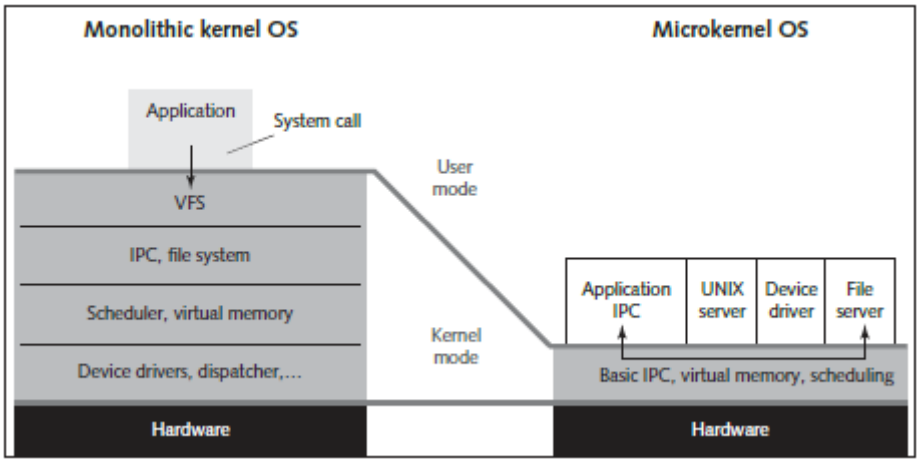
• Orbiter Mars Reconnaissance

• Sprzęt komunikacyjny Radvision 3G

• Statek kosmiczny Stardust

• SAUVIM (zanurzalny statek kosmiczny przeznaczony do operacji na głębokich oceanach)

Green Hill Software produkuje również różnorodne systemy operacyjne. Zaprojektowano system operacyjny dla myśliwca F-35 Joint Strike Fighter, a także system operacyjny certyfikowany do obsługi wielu poziomów klasyfikacji (takich jak niejawny, tajny i ściśle tajny) na tym samym procesorze bez przecieków między poziomami. Ten typ systemu operacyjnego nazywa się wieloma niezależnymi poziomami bezpieczeństwa/ochrony (MILS). Wojsko amerykańskie używa systemów operacyjnych MILS w środowiskach o wysokim poziomie bezpieczeństwa, a inne organizacje, takie jak te kontrolujące elektrownie jądrowe lub miejskie oczyszczalnie ścieków, używają ich, gdy rozdzielenie uprawnień i funkcji jest kluczowe. Green Hill projektuje również kod systemu operacyjnego używanego w drukarkach, routerach, przełącznikach, skanerach kodów kreskowych i radiach. Wspomniane systemy operacyjne używają mikrojądra, które poświęca elastyczność na rzecz prostoty i mniejszych zasobów sprzętowych. QNX, od QNX Software Systems, to komercyjny system operacyjny czasu rzeczywistego używany w routerach o ultrawysokiej dostępności Cisco i w uniwersalnych pilotach Logitech. Innym zastrzeżonym systemem operacyjnym jest Real-Time Executive for Multiprocessor Systems (RTEMS), system operacyjny typu open source używany w systemach kosmicznych, ponieważ obsługuje procesory zaprojektowane specjalnie do pracy w kosmosie. Obecnie działa na Mars Reconnaissance Orbiter wraz z VxWorks. NASA poprawiła przeżywalność tego statku kosmicznego, używając kilku małych systemów operacyjnych dostosowanych do określonych funkcji zamiast ogromnego monolitycznego systemu operacyjnego jądra, który kontroluje każdą funkcję. Jednak używanie wielu systemów operacyjnych zwiększa również powierzchnię ataku. Rysunek ilustruje różnice w rozmiarze i wymaganiach dotyczących zasobów między systemami operacyjnymi z monolitycznym jądrem a systemami operacyjnymi z mikrojądrem.

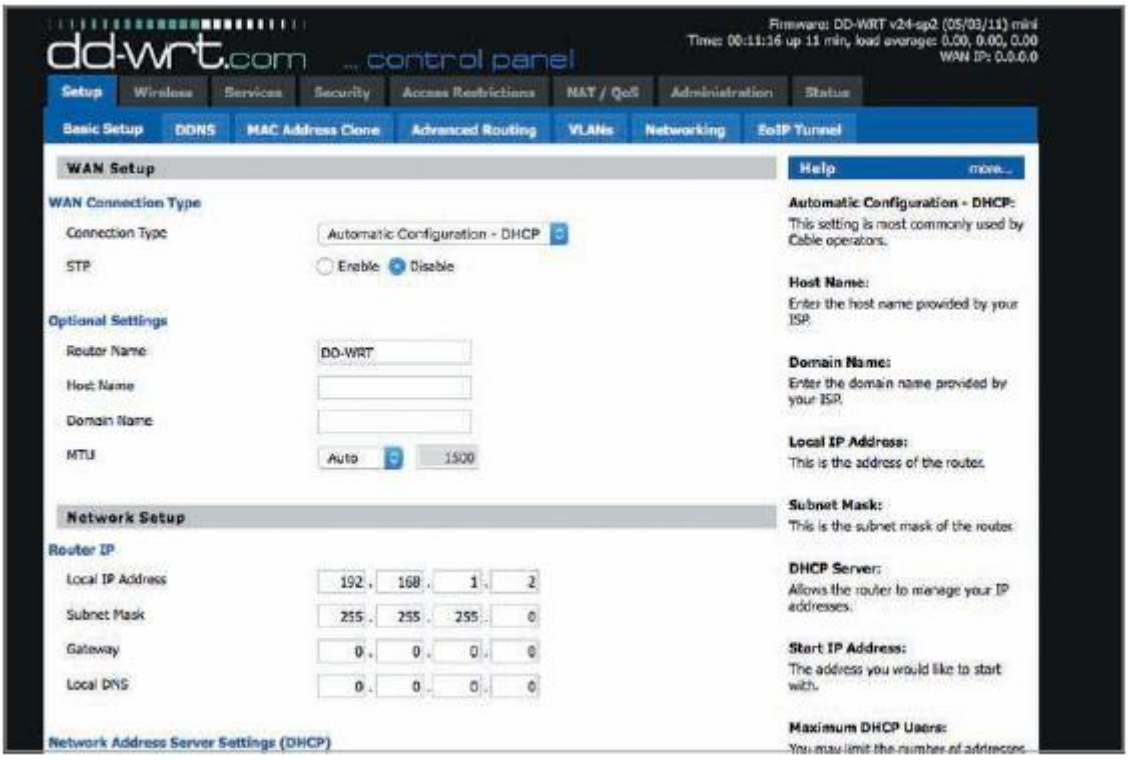


UWAGA

Jeśli chcesz pobawić się systemem RTOS, możesz pobrać kopię FreeRTOS z SourceForge (https://sourceforge.net/projects/freertos/files/FreeRTOS).

***Nix Embedded OS**

Embedded Linux jest przykładem monolitycznego systemu operacyjnego używanego w wielu urządzeniach przemysłowych, medycznych i konsumenckich. Wbudowane wersje Linuksa i innych systemów operacyjnych *nix można dostosować do urządzeń z ograniczoną pamięcią lub pojemnością dysku twardego, takich jak telefony komórkowe. Zaletą monolitycznego jądra jest to, że może obsługiwać najszerszą gamę sprzętu i umożliwia dodawanie funkcji za pomocą dynamicznych modułów jądra. Inne przykłady komercyjnych produktów z wbudowanymi systemami operacyjnymi *nix to przełączniki i routery Cisco, urządzenia GPS TomTom i Garmin, odtwarzacze multimedialne i instrumenty medyczne. Smartfony z Androidem i iPhone'y mają wbudowany system operacyjny *nix w swoich rdzeniach. Oprócz VxWorks, Wind River produkuje system operacyjny Linux dla systemów wbudowanych o nazwie Wind River Linux. Wind River Linux to wariant systemu operacyjnego czasu rzeczywistego Linuksa, który nadaje się do wbudowanych aplikacji wymagających gwarantowanej odpowiedzi w sposób matematycznie przewidywalny. Innym wbudowanym systemem operacyjnym Linux, który można pobrać do użytku domowego, jest dd-wrt (https://dd-wrt.com/). Początkowo zaprojektowany do użytku z bezprzewodowym Linksys WRT54G, ten system operacyjny może być uruchomiony na większości małych routerów biurowych lub domowych. Rysunek pokazuje interfejs konfiguracji.



UWAGA Wbudowane systemy routerów domowych, takie jak Linksys WRT54G, były celem ataku robaka botnet na dużą skalę. Robak ten, zwany psyb0t (lub Network Bluepill), rozprzestrzeniał się, wykorzystując przestarzałe lub źle skonfigurowane systemy operacyjne routerów, które zawierały łatwe do odgadnięcia hasła. Po tym, jak psyb0t zainfekował dziesiątki tysięcy systemów, atakujący użyli go do przeprowadzenia ataków typu DDoS (Distributed Denial of Service) lub wykorzystujących luki w zabezpieczeniach. Jeśli masz w domu router bezprzewodowy, czy wiesz, czy jest on chroniony przed zagrożeniami takimi jak psyb0t?

Jak już widziałeś, wbudowane systemy operacyjne są wszędzie na Ziemi — a w niektórych przypadkach także poza nią. Jako tester bezpieczeństwa musisz wiedzieć o lukach w tych systemach. W następnej aktywności zbadasz niektóre produkty wykorzystujące wbudowane systemy operacyjne i dowiesz się więcej o ich lukach.

Badanie produktów z wbudowanymi systemami operacyjnymi

Czas trwania: 40 minut

Cel: Przeszukanie baz danych luk w celu znalezienia produktów wykorzystujących podatne wbudowane systemy operacyjne.

Opis: Do tej pory większość specjalistów ds. bezpieczeństwa miała niewielką wiedzę na temat wielu produktów wykorzystujących wbudowane systemy operacyjne. W tym ćwiczeniu przeszukasz Narodową Bazę Danych Podatności (NVD) pod kątem produktów wykorzystujących wbudowane systemy operacyjne.

1. W systemie Windows uruchom przeglądarkę internetową, jeśli to konieczne, i przejdź do https://nvd.nist.gov.

2. Kliknij przycisk MENU NVD, a następnie kliknij SZUKAJ.

3. Kliknij przycisk Luki w zabezpieczeniach – CVE, aby wyświetlić stronę Przeszukaj bazę danych luk w zabezpieczeniach.

4. Wpisz vxworks w polu tekstowym Wyszukiwanie słów kluczowych i naciśnij Enter.

5. Przewiń wyniki wyszukiwania i poświęć trochę czasu na czytanie o lukach w zabezpieczeniach urządzeń wykorzystujących systemy operacyjne VxWorks.

6. Kontynuuj swoje badania, wyszukując więcej terminów związanych z systemami operacyjnymi wbudowanymi, takich jak wbudowany Linux, QNX, Netscreen, Lexmark, Jetdirect, Android, drukarki Canon, Linksys, VOIP, dd-wrt, iPhone, Netgear, Foundry, Cisco i Nortel. Zapisz kilka przykładów urządzeń z wbudowanymi systemami operacyjnymi i krótko opisz luki w zabezpieczeniach. Nie poświęcaj więcej niż 20 minut na badanie terminów.

7. Ile urządzeń wbudowanych i luk w zabezpieczeniach udało Ci się znaleźć w ciągu 20 minut? Czy którekolwiek z tych podatnych urządzeń można znaleźć w dużej firmie lub agencji rządowej? A co powiesz na to w domu?

8. Pozostaw przeglądarkę internetową otwartą na czas następnej aktywności.

LUKI WBUDOWANYCH SYSTEMÓW OPERACYJNYCH

Niektórzy specjaliści ds. bezpieczeństwa pamiętają czasy, gdy ataki komputerowe powodowały szkody porównywalne do graffiti na budynku. Obraźliwe, tak, ale nie na tyle szkodliwe, by zaniepokoić większość specjalistów ds. bezpieczeństwa. Jednak skutki ataków stały się poważniejsze, a wbudowane systemy operacyjne nie są wyjątkiem. W Ćwiczeniu powyżej odkryłeś, że wiele wbudowanych systemów operacyjnych ma luki. Witryny takie jak www.exploit-db.com i www.packetstormsecurity.org zawierają informacje o tym, co hakerzy robią z tymi lukami. Wielu hakerów dzisiaj chce czegoś więcej niż tylko rozgłosu; są przestępcami szukającymi sposobów na kradzież pieniędzy. Jednym ze sposobów na czerpanie zysków z hakowania jest atakowanie urządzeń, w których gotówka jest przechowywana i wydawana przez komputer: bankomatów. Bankomaty są podatne na ataki na ich oprogramowanie przeprowadzane lokalnie lub zdalnie, lub na ataki fizyczne, takie jak używanie skimmerów kart, a nawet kradzież maszyn. Podczas konferencji Black Hat w 2010 roku badacz ds. bezpieczeństwa Barnaby Jack z Juniper Networks zasłynął z zademonstrowania luki w zabezpieczeniach popularnych bankomatów, która umożliwiała ataki lokalne i zdalne. Miał na scenie dwa bankomaty, które zhakował, powodując, że wypluwały dziesiątki banknotów. Zhakował jeden bankomat zdalnie przez sieć i podłączył pamięć USB do portu drugiego bankomatu, aby zastosować złośliwe oprogramowanie. Niedawno, w 2021 roku, badacze ds. bezpieczeństwa podnieśli alarm, że czytniki komunikacji bliskiego zasięgu (NFC) w bankomatach są luką w zabezpieczeniach. NFC to wygodna funkcja, która umożliwia dotknięcie lub przesunięcie karty bankowej do czytnika lub w jego pobliżu zamiast wkładania jej do bankomatu. Używając smartfona ze złośliwym oprogramowaniem, można wykorzystać NFC do awarii bankomatu, zablokowania go w ataku ransomware, zhakowania go w celu wydobycia danych karty kredytowej lub wygrania jackpota w bankomacie, aby wypluł pieniądze. Badacie luki w zabezpieczeniach bankomatów w Ćwiczeniu.

BAJTY BEZPIECZEŃSTWA

Jako tester bezpieczeństwa musisz pamiętać, że czasami największym zagrożeniem dla bezpieczeństwa organizacji są jej pracownicy. Administratorzy systemów, menedżerowie sieci i technicy często mają nieograniczony i niemonitorowany dostęp do najważniejszych komponentów IT firmy. Są świadomi wszelkich luk w istniejących procesach bezpieczeństwa i wiedzą, jak ukryć nielegalne działania. Jednak przestrzeganie „zasady najmniejszych uprawnień” może pomóc w zmniejszeniu zagrożenia

wewnętrznego. Zasada ta określa, że personelowi należy przyznać tylko dostęp, którego potrzebuje do wykonywania obowiązków służbowych, i cofnąć dostęp, gdy tylko przestanie być potrzebny.

Badanie luk w zabezpieczeniach bankomatów

Czas trwania: 20 minut

Cel: Zbadanie luk w zabezpieczeniach bankomatów.

Opis: Jako tester bezpieczeństwa musisz być świadomy ataków, które mogą wystąpić na systemy inne niż zwykłe stacje robocze i serwery. Jeśli bank zleci Ci przeprowadzenie testu bezpieczeństwa, a Ty zaniedbasz zbadanie możliwych ataków na bankomaty, możesz znaleźć się w kłopotliwej sytuacji, jeśli poważny atak spowoduje utratę milionów dolarów przez bank. Po przeczytaniu kilku artykułów na temat bankomatów powinieneś lepiej rozumieć metody, których atakujący używają do kradzieży pieniędzy z banków — bez konieczności noszenia masek i broni.

1. W razie potrzeby uruchom przeglądarkę internetową i przejdź do swojej ulubionej wyszukiwarki. Wpisz Hacking ATM Machines z samym tekstem w polu tekstowym wyszukiwania i naciśnij Enter.

2. Artykuł w The Hacker News omawia, w jaki sposób atakujący mogą używać złośliwego oprogramowania i smartfonów, aby bankomaty wypłacały gotówkę. Jaki system operacyjny jest używany? Jakie sugestie przedstawiła firma ochroniarska, aby zmniejszyć te zagrożenia?

3. Kontynuuj wyszukiwanie bardziej aktualnych artykułów na temat włamań do bankomatów i luk w zabezpieczeniach. W szczególności spróbuj znaleźć artykuł na wired.com o odmianie złośliwego oprogramowania WinPot ATM. Na podstawie swoich badań, jakich systemów operacyjnych używa większość bankomatów?

4. Pozostaw przeglądarkę internetową otwartą do następnej aktywności.

Wbudowane systemy operacyjne są wszędzie

Na progu minionego tysiąclecia eksperci ostrzegali przed nieuchronną globalną katastrofą: miliardy wbudowanych systemów z wadą oprogramowania Y2K (od „roku 2000”) nagle zatrzymałyby się lub uległy awarii, gdy zegar wybiłby północ. Te wbudowane systemy znajdowały się wszędzie, w tym w krytycznych elementach infrastruktury sterujących zasilaniem, komunikacją, transportem i nie tylko, więc ogromne ilości czasu i pieniędzy wydano na naprawę wbudowanych systemów, aby zapobiec potencjalnej katastrofie. Obecnie jest o wiele więcej wbudowanych urządzeń, o które należy się martwić, niż w roku 2000. Te wbudowane urządzenia nie mają wady oprogramowania Y2K, ale są atakowane przez hakerów i terrorystów, którzy chcą promować swoje cele finansowe lub polityczne. To nowe zagrożenie jest powodem, dla którego zajęcie się bezpieczeństwem wbudowanych systemów na wczesnym etapie fazy projektowania — a nie traktowanie tego jako czegoś drugorzędnego — jest niezbędne.

Wbudowane systemy operacyjne są połączone w sieć

Ze względów wydajności i oszczędności łączenie wbudowanych systemów z siecią ma swoje zalety. Możliwość zarządzania systemami i udostępniania usług przy jednoczesnym ograniczeniu zasobów ludzkich i wiedzy fachowej do minimum pomaga firmom obniżyć koszty. Zwiększanie wydajności i obniżanie kosztów ma jednak swoją cenę: każde urządzenie dodane do infrastruktury sieciowej zwiększa potencjalne problemy z bezpieczeństwem. Testerzy bezpieczeństwa powinni odpowiadać na następujące pytania dla każdej maszyny lub urządzenia w sieci:

• Jakie urządzenia Peripheral Component Interconnect (PCI) lub USB są obecne?

• Gdzie zostały wyprodukowane? Czy łańcuch dostaw jest godny zaufania?

• Które urządzenia mają wbudowane systemy operacyjne przechowywane w pamięci z możliwością ponownego zapisu (nieulotnej)? Pamięć z możliwością ponownego zapisu można szybko flashować (czyli szybko kasować i nadpisywać).

• Który wbudowany system operacyjny jest obecnie załadowany na każdym urządzeniu?

• Czy możesz upewnić się, że wbudowany system operacyjny nie został uszkodzony lub zmieniony złośliwym kodem? Ta kontrola nazywa się sprawdzaniem integralności wbudowanego systemu operacyjnego

Wbudowane systemy operacyjne są trudne do łatania

Dowiedziałeś się, jak ważne jest aktualizowanie systemów i oprogramowania antywirusowego. W przypadku systemów operacyjnych komputerów PC ogólnego przeznaczenia normalne jest czekanie, aż ktoś zidentyfikuje lukę, pobierze i zainstaluje poprawkę, gdy będzie dostępna, i w razie potrzeby ponownie uruchomi system. Jednak takie podejście nie działa w przypadku wielu systemów operacyjnych wbudowanych, ponieważ muszą one nadal działać niezależnie od zagrożenia, szczególnie w systemach krytycznych, takich jak dystrybucja zasilania, kontrola ruchu lotniczego i podtrzymywanie życia. Łatanie na komputerach ogólnego przeznaczenia jest zwykle proste, ale łatanie systemów operacyjnych wbudowanych może być problemem. Na przykład wielu wykwalifikowanych administratorów systemów wie, jak załatać serwer internetowy dla systemów Linux, Windows lub Solaris UNIX działających na standardowym sprzęcie komputerowym Sun lub x86, ale mogą nie mieć pojęcia, jak załatać serwer internetowy działający na małym chipie (zwanym „16-bitowym mikrokontrolerem”) w plastikowym pudełku wielkości talii kart. Innym problemem jest to, że ataki przepełnienia bufora mogą być skuteczne w systemach operacyjnych wbudowanych, ponieważ niewiele aktualizacji jest wydawanych w celu usunięcia luk. Zazwyczaj producenci wolą, abyś uaktualniał system, a nie wbudowany system operacyjny, więc mogą nie udostępniać aktualizacji, gdy zostaną odkryte luki. Aktualizacja wbudowanego systemu operacyjnego w niektórych systemach jest na tyle trudna, że Twoi klienci prawdopodobnie tego nie zrobią. Bądź przygotowany, aby wyjaśnić swoim klientom najlepszy sposób postępowania. Pamiętaj, że zarówno systemy operacyjne ogólnego przeznaczenia, jak i wbudowane używają sterowników do zarządzania urządzeniami sprzętowymi. W obu typach systemów operacyjnych sterowniki są podatne na wykorzystanie i czasami trzeba je aktualizować lub łatać. Jakiś czas temu luka w sterownikach bezprzewodowego chipsetu Intel umożliwiła zdalne naruszenie bezpieczeństwa urządzeń bezprzewodowych. Luka nie jest zaskakująca. Zaskakujące jest to, że niewielu administratorów systemów aktualizowało te sterowniki, ponieważ nigdy nie pojawiały się one na liście „krytycznych” poprawek systemu operacyjnego w usłudze Windows Update. Jednym z powodów, dla których niektórzy dostawcy wbudowanych systemów operacyjnych częściej używają oprogramowania typu open source, jest to, że koszt opracowania i łatania systemu operacyjnego jest dzielony przez całą społeczność open source, a nie tylko przez garstkę przepracowanych programistów w zapleczu. Do tej pory całkowity koszt godzin pracy programisty na opracowanie i łatanie jądra Linuksa szacuje się na dziesiątki miliardów dolarów. Posiadanie tak dużego doświadczenia programistycznego jest trudne do odrzucenia dla każdej firmy opracowującej systemy wbudowane. Z drugiej strony monolityczne jądro Linuksa zostało zaprojektowane tak, aby oferować największą elastyczność i obsługę zaawansowanych funkcji; z tego powodu jest bardzo duże i ma wiele fragmentów kodu, które mogą wymagać łatania w miarę odkrywania luk. W przypadku wrażliwych systemów wbudowanych, które potrzebują tylko ułamka funkcji jądra Linuksa, ryzyko potencjalnych luk może przeważyć nad korzyściami. W tej sytuacji bardziej odpowiednie może być zastrzeżone jądro. Jako tester bezpieczeństwa możesz zidentyfikować drobne

luki w zabezpieczeniach wbudowanych systemów operacyjnych, których naprawa jest niezwykle kosztowna. Jednak ilość czasu i wiedzy, jakiej atakujący potrzebowałby, aby wykorzystać tę niewielką lukę, jest również niezwykle wysoka. W przypadku tego typu luk musisz rozważyć koszt naprawy luki w stosunku do ważności informacji kontrolowanych przez wbudowany system. Możesz zalecić nienaprawianie luki, ponieważ jest ona wystarczająco bezpieczna w stosunku do niewielkiego ryzyka.

BAJTY BEZPIECZEŃSTWA

Monitory pracy serca i urządzenia MRI to przykłady systemów, które działają na wbudowanych systemach operacyjnych Windows. Często tych systemów nie można załatać, ponieważ są certyfikowane na określonym poziomie rewizji lub producent nigdy nie udostępnił metody łatania. Problem ten stał się widoczny, gdy robak Conficker zainfekował wiele systemów medycznych na całym świecie. Nawet w systemach wbudowanych, które nie były bezpośrednio podłączone do Internetu, wersje Confickera rozprzestrzeniały się za pośrednictwem nośników wymiennych. Prosty transfer danych za pomocą dysków USB może być ryzykowny.

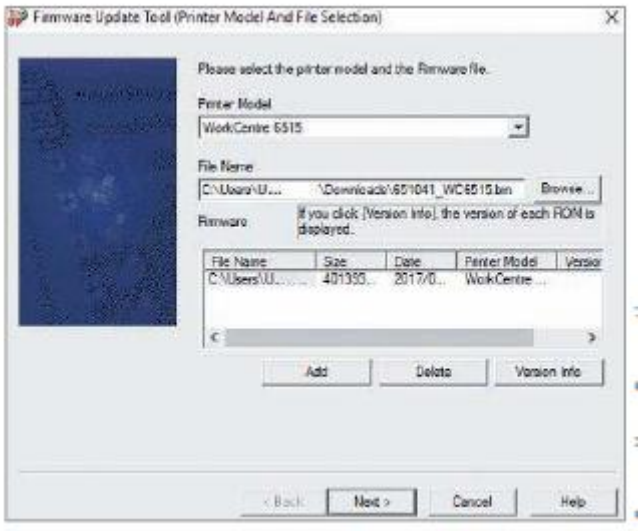
Wbudowane systemy operacyjne znajdują się w urządzeniach sieciowych

Urządzenia sieciowe, takie jak routery i przełączniki, zazwyczaj mają oprogramowanie i sprzęt przeznaczone do przesyłania informacji przez sieci. Pierwotnie do routingu i przełączania używano komputerów ogólnego przeznaczenia, ale obecnie szybkie sieci wykorzystują specjalistyczny sprzęt i wbudowane systemy operacyjne. W przeszłości Cisco używało głównie zastrzeżonego kodu w swoich wbudowanych systemach. Jednak dzięki wykorzystaniu większej ilości kodu open source Cisco może szybciej udostępniać nowe funkcje produktów. Cisco używa jąder Linux w swoich najnowszych urządzeniach VoIP Call Manager i zaporze Adaptive Security Appliance (ASA). Inne wbudowane systemy operacyjne dla urządzeń sieciowych to zmodyfikowane systemy operacyjne *nix. Na przykład systemy operacyjne Juniper i Extreme Networks są oparte na systemie UNIX. Możesz się zastanawiać, dlaczego ktokolwiek miałby zawracać sobie głowę hakowaniem routerów lub innych urządzeń sieciowych, ponieważ nie zawierają one tajemnic korporacyjnych i nie mają dużej przestrzeni dyskowej ani mocy obliczeniowej, które mogłyby zostać skradzione. Krótka odpowiedź brzmi, że gdy atakujący naruszą bezpieczeństwo hosta, to wszystko, co mogą uzyskać: pojedynczy host. Gdy włamią się do routera, mogą kontrolować każdego hosta w sieci. Z routera atakujący mogą mapować całą sieć, modyfikować pakiety do i z hostów, przekierowywać ruch do i z innych hostów lub sieci, atakować inne sieci, do których można uzyskać dostęp z włamanego routera, i wykonywać bezpłatne połączenia telefoniczne za pomocą VoIP, jeśli jest skonfigurowany. Krótko mówiąc, kontrolowanie routera może dać atakującym pełny dostęp do zasobów sieciowych. Aby włamać się do całej sieci za pośrednictwem routera, atakujący stosują zwykłe metody odciskania śladu, skanowania i enumerowania celu. Wbudowane systemy operacyjne w routerach są często podatne na wiele takich samych ataków, które nękają systemy operacyjne ogólnego przeznaczenia, od prostego zgadywania hasła po wyrafinowane ataki przepełnienia bufora. Częstą podatnością routerów i innych urządzeń sieciowych ze wbudowanymi interfejsami zarządzania siecią jest podatność na obejście uwierzytelniania. Atakujący mogą przejąć kontrolę nad urządzeniem sieciowym lub zbierać z niego poufne informacje, uzyskując dostęp do urządzenia za pomocą specjalnie spreparowanego adresu URL, który omija normalny mechanizm uwierzytelniania. Po ominięciu uwierzytelniania atakujący mogą przeprowadzić inne ataki sieciowe, wykorzystując dostęp uzyskany dzięki włamaniu się do routera.

Wbudowane systemy operacyjne znajdują się w urządzeniach peryferyjnych sieciowych

Urządzenia peryferyjne w sieci organizacji mogą obejmować drukarki, skanery, kopiarki i sieciowe urządzenia faksowe. Urządzenia wykonujące więcej niż jedną z tych funkcji nazywane są urządzeniami wielofunkcyjnymi (MFD), drukarkami wielofunkcyjnymi (MFP) lub kopiarkami wielofunkcyjnymi (MFC).

Zazwyczaj administratorzy systemów lub sieci myślą o urządzeniach MFD tylko wtedy, gdy rozwiązują problemy lub dodają je do sieci. Przez resztę czasu te urządzenia peryferyjne sieciowe są zapominane. Rzadko są skanowane pod kątem luk w zabezpieczeniach lub konfigurowane pod kątem bezpieczeństwa. Urządzenia MFD mają jednak wbudowane systemy operacyjne, a wiele poufnych informacji jest wysyłanych do tych urządzeń przez sieć, co czyni je atrakcyjnymi celami dla hakerów. Administratorzy sieci i systemów muszą zwracać uwagę na luki w zabezpieczeniach tych urządzeń i podejmować kroki w celu załatania lub zmniejszenia ryzyka. Informacje drukowane, kopiowane, skanowane i faksowane mogą być podatne na kradzież i modyfikację. Na przykład zainfekowane urządzenie wielofunkcyjne może zostać użyte do zbierania informacji i odsyłania ich z powrotem do atakującego za pośrednictwem wbudowanego w system FTP lub systemu przekazywania poczty e-mail. Niektóre zaawansowane drukarki działają na wbudowanych systemach operacyjnych Windows, więc mogą zostać zainfekowane przez powszechne złośliwe oprogramowanie. Urządzenia wielofunkcyjne i serwery wydruku z dyskami twardymi mogą być z pewnością używane do rozprzestrzeniania złośliwego oprogramowania, jeśli mają udziały dostępne w sieci. W 2018 roku fani gwiazdy YouTube PewDiePie zhakowali drukarki na całym świecie i zdalnie spowodowali, że drukarki drukowały plakaty popierające PewDiePie. Później powtórzyli ten wyczyn, ale dołączyli wiadomość wzywającą ofiary do poprawy bezpieczeństwa. W wielu starszych drukarkach wszystkie dostępne protokoły sieciowe są domyślnie włączone. Jeśli drukarka jest zabezpieczona za pomocą adresu IP, atakujący mogą po prostu połączyć się z nią za pomocą innego protokołu, takiego jak IPX lub AppleTalk. Ponieważ te drukarki mają również domyślne nazwy użytkowników i hasła administratora, nieautoryzowani użytkownicy mogą się z nimi połączyć jako administratorzy. Obecnie większość drukarek ma włączony tylko protokół TCP/IP, ale niestety domyślne nazwy użytkowników i hasła administratora są nadal skonfigurowane. Przed podłączeniem drukarek do sieci należy je ponownie skonfigurować. Wreszcie atakujący mogą użyć technik socjotechnicznych, aby podszyć się pod techników pomocy technicznej, aby uzyskać fizyczny dostęp do urządzeń wielofunkcyjnych i wymienić dysk twardy drukarki lub wbudowany system operacyjny na taki, który zawiera złośliwy kod. Złośliwi insiderzy mogą również wymienić oprogramowanie układowe (wbudowany system operacyjny) na specjalnie zmodyfikowane oprogramowanie układowe, jak pokazano na rysunku.



BAJTY BEZPIECZEŃSTWA

Kilka lat temu klient pracujący dla dużej korporacji z siedzibą na Hawajach skontaktował się z działem pomocy technicznej Xerox Corporation. Jego skarga? Zadania drukowania zajmowały teraz nieproporcjonalnie dużo czasu. Po zaledwie kilku minutach rozwiązywania problemów technik ustalił,

że wszystkie zadania drukowania wysyłane do lokalnej drukarki były również kierowane do Europy Wschodniej.

Identyfikowanie luk w zabezpieczeniach drukarek

Czas trwania: 30 minut

Cel: Zbadanie luk w zabezpieczeniach drukarek.

Opis: W miarę jak specjaliści ds. bezpieczeństwa stają się coraz bardziej kompetentni w zabezpieczaniu systemów komputerowych i sieciowych, atakujący muszą być kreatywni w znajdowaniu innych słabości, które dają im dostęp do systemów. Internet jest cennym źródłem wiedzy na temat metod, których atakujący używają obecnie. Jako tester zabezpieczeń poświęcisz dużo czasu na tego typu badania.

1. W razie potrzeby uruchom przeglądarkę internetową i przejdź do swojej ulubionej wyszukiwarki. Wpisz exploity sterowników drukarek w polu tekstowym wyszukiwania, a następnie naciśnij Enter.

2. Przeczytaj artykuł pod linkiem www.zdnet.com/article/hp-patches-vulnerable-printer-driver-impacting-millions-ofdevices. Czy od czasu napisania tego artykułu wprowadzono jakieś ulepszenia mające na celu rozwiązanie problemów związanych z wbudowanymi systemami operacyjnymi?

3. Podaj krótki opis luk i możliwych ataków wymienionych w artykule.

4. Przeczytaj artykuł pod linkiem www.darkreading.com/vulnerabilities-threats/significant-vulnerabilities-found-in- 6-common-printer-brands. Jakie są powody, dla których drukarki są podatne? Które marki miały najwięcej luk, a które najmniej? Jakie rozwiązania sugerują badacze?

5. Zamknij przeglądarkę internetową.

Systemy kontroli nadzorczej i gromadzenia danych

Systemy kontroli nadzorczej i gromadzenia danych (SCADA) są używane do monitorowania sprzętu w dużych gałęziach przemysłu, takich jak roboty publiczne i zakłady użyteczności publicznej, generatory i tamy, systemy transportowe (takie jak wieże kontrolne FAA), produkcja — wszędzie tam, gdzie automatyzacja ma kluczowe znaczenie. Systemy SCADA czasami mają wiele wbudowanych systemów jako komponenty, które mogą być podatne na ataki ze względu na dane przesyłane do nich i z nich lub poprzez wbudowane systemy operacyjne. W każdym razie nie będzie przesadą stwierdzenie, że bezpieczeństwo niektórych systemów SCADA jest kwestią życia i śmierci. Z tego powodu systemy SCADA kontrolujące krytyczną infrastrukturę są zwykle oddzielone od Internetu „przerwą powietrzną". Czy hakerzy nadal mogą się dostać? Aby przetestować tę możliwość, Departament Bezpieczeństwa Krajowego rozpoczął projekt Aurora, aby symulować zdalny atak sieciowy na duży generator dieslowsko-elektryczny używany w wielu amerykańskich elektrowniach. Projekt Aurora był w stanie wykorzystać lukę w zabezpieczeniach systemu SCADA i spowodować, że generator o wartości 1 miliona dolarów rozpadł się. Wyobraź sobie niszczycielski wpływ skoordynowanego ataku, który mógłby zniszczyć setki generatorów w elektrowniach na całym świecie. W grudniu 2015 r. atak na ukraińską elektrownię pozostawił około 700 000 osób w ciemności na kilka godzin. Później odkryto, że fragment złośliwego kodu o nazwie „Black-Energy" został wprowadzony w celu zainfekowania systemów w elektrowni. Ten sam złośliwy kod został użyty przeciwko Gruzji w 2008 r. Nadal istnieje pewne zamieszanie co do tego, w jaki sposób atakujący spowodowali przerwę w dostawie prądu, ale zakłada się, że weszli w interakcję z systemem SCADA, aby przerwać przepływ energii. W maju 2021 r. cyberatak ransomware zmusił amerykańskiego operatora rurociągów Colonial Pipeline do tymczasowego wstrzymania wszystkich operacji rurociągowych. Colonial Pipeline dostarcza około 45

procent całego paliwa na wschodnie wybrzeże USA. Atak doprowadził do niedoborów paliwa i wzrostu cen paliwa. Colonial Pipeline zapłacił hakerom okup w wysokości około 5 milionów dolarów, aby ich okupowane systemy i dane zostały ujawnione.

Telefony komórkowe, smartfony i technologia noszona

Podsłuchiwanie tradycyjnej linii telefonicznej wymagało kiedyś dużo czasu, drogiego sprzętu technicznego i nakazu. Nawet wtedy można było jedynie podsłuchiwać rozmowę. Co zaskakujące, wiele osób ma takie same oczekiwania co do bezpieczeństwa telefonów komórkowych i smartfonów. Luki w zabezpieczeniach telefonów komórkowych obejmują podsłuchiwanie rozmów telefonicznych, używanie telefonu jako mikrofonu i „klonowanie" karty SIM telefonu w celu wykonywania nielegalnych połączeń międzynarodowych. Korzystając z tych metod, atakujący mogą znaleźć informacje przydatne do uzyskania dostępu do komputera (lub sieci firmy), a nawet mogą ukraść tajemnice handlowe lub bezpieczeństwa narodowego. Smartfony, takie jak urządzenia z systemem Android i iPhone'y, łączą funkcje tego, co kiedyś nazywano PDA, i telefonu komórkowego. Badacze ds. bezpieczeństwa i atakujący stworzyli wirusy oparte na Javie, a także kod, który może zainfekować telefony z systemem Google Android, Windows Mobile i Apple iPhone OS (iOS). Wraz ze wzrostem liczby funkcji dostępnych w smartfonach granica między systemami operacyjnymi wbudowanymi a ogólnego przeznaczenia zaciera się. Te systemy operacyjne, podobnie jak Windows i Red Hat, mają luki, które mogą zagrozić bezpieczeństwu smartfona. Noszona technologia, taka jak inteligentne zegarki i trackery fitness, również zawiera wbudowane systemy operacyjne, które mogą być podatne na ataki. Często technologie noszone wchodzą w interakcję ze smartfonami za pomocą Bluetooth. Ta interakcja zwiększa liczbę sposobów, w jakie można zaatakować smartfon (powierzchnia ataku), czyniąc go bardziej podatnym na ataki. W 2020 r. konferencja Blackhat ujawniła nowy łańcuch exploitów o nazwie TiYunZong, który może zdalnie zrootować szeroką gamę urządzeń z systemem Android opartych na systemie Qualcomm. (Zrootowanie urządzenia z systemem Android oznacza zmianę jego systemu operacyjnego przy użyciu uprawnień administratora). W lipcu 2015 r. podczas konferencji Blackhat w Las Vegas ujawniono luki Stagefright w systemie Android. Poważniejsze z tych luk można wykorzystać za pomocą złośliwej wiadomości MMS (Multimedia Messaging Service). Telefon ofiary automatycznie pobierał złośliwą wiadomość MMS, a atakujący mógł przejąć kontrolę nad urządzeniem. Inna luka, również ujawniona w 2015 r., umożliwiła atakującym zebranie odcisków palców wykorzystywanych ofiar. Podczas gdy dane odcisków palców są przechowywane w bezpiecznej lokalizacji, atak może odczytać informacje z samego czujnika odcisków palców, ujawniając atakującemu osobiste, biometryczne informacje. Trojany stały się również dużym problemem w sklepach z aplikacjami mobilnymi, takich jak Google Play Store i Apple App Store. Aplikacja może wydawać się przydatna, ale kraść informacje lub moc obliczeniową ze smartfona. Na przykład w marcu 2021 r. Google usunęło 10 aplikacji ze sklepu Play, które zawierały droppery dla trojanów finansowych. Dropper to złośliwe oprogramowanie używane do dostarczania (upuszczania) innych ładunków złośliwego oprogramowania. Niektóre z usuniętych aplikacji to Cake VPN, Pacific VPN, BeatPlayer, QR/Barcode Scanner MAX i QRecorder. Te aplikacje omijały standardowe zabezpieczenia Google, pobierając złośliwe oprogramowanie z GitHub po instalacji. Jeśli atakującym jest sama firma telefoniczna, niewiele można zrobić. W 2009 r. krajowa firma telekomunikacyjna w państwie Zatoki Perskiej nakazała wszystkim swoim klientom BlackBerry zainstalowanie aplikacji „w celu zapewnienia ciągłej jakości usług". Klienci, którzy nie zastosowali się do tego, byli zagrożeni rozłączeniem. Późniejsza analiza wykazała, że ta aplikacja była wyrafinowanym programem szpiegującym, który umożliwiał podsłuchującym firmy telefoniczne przechwytywanie wszystkich połączeń do i z BlackBerry z zainstalowaną tą aplikacją.

Rootkity

Rootkity istnieją dla systemów Windows i *nix, więc wersje wbudowane tych systemów są na nie podatne. Rootkity mogą modyfikować części systemu operacyjnego lub instalować się jako moduły jądra, sterowniki, biblioteki, a nawet aplikacje. Narzędzia do wykrywania rootkitów i niektóre programy antywirusowe mogą wykrywać rootkity i zapobiegać ich instalacji. Jednak problem staje się trudniejszy, jeśli system operacyjny został już naruszony. Zainstalowanie tych narzędzi w zainfekowanym systemie zwykle nie powoduje wyświetlenie alertów, ponieważ rootkity mogą monitorować system operacyjny pod kątem narzędzi antyrootkitowych i je neutralizować. Rootkity, które stanowią największe zagrożenie dla każdego systemu operacyjnego (wbudowanego lub ogólnego przeznaczenia), to te, które infekują oprogramowanie układowe urządzenia. Są bardziej niebezpieczne, ponieważ mają tendencję do bycia niezwykle małymi, są ładowane w pamięci masowej niskiego poziomu, do której narzędzia antyrootkitowe nie mają łatwego dostępu, i mogą przetrwać nawet po ponownym sformatowaniu dysku twardego. Obrona przed rootkitami niskiego poziomu obejmuje użycie Trusted Platform Module (TPM), kryptograficznego procesora sprawdzającego rozruch oprogramowania sprzętowego zainstalowanego w wielu ostatnich systemach komputerowych. TPM zapewnia, że system operacyjny nie został podważony ani uszkodzony, na przykład przez rootkit oprogramowania sprzętowego. TPM jest obecnie standardem ISO ISO/IEC 11889. Aby uzyskać więcej informacji na temat tego standardu, odwiedź stronę www.iso.org. Komputer może mieć kilka megabajtów pamięci flash ROM na płycie głównej i kartach kontrolera, takich jak kontroler Ethernet. Rootkity oprogramowania sprzętowego są trudne do wykrycia, ponieważ kod oprogramowania sprzętowego często nie jest sprawdzany pod kątem możliwych uszkodzeń. Włamania wewnętrzne są trudniejsze do wykrycia, gdy złośliwy kod jest ukryty w pamięci flash systemu. Niezadowoleni pracownicy mogliby na przykład zainstalować rootkita opartego na systemie BIOS w pamięci flash komputerów firmowych, zanim opuszczą firmę. Następnie mogliby użyć tego rootkita BIOS-u, który przetrwałby po ponownej instalacji systemu operacyjnego, aby uzyskać dostęp do sieci korporacyjnej później.

BAJTY BEZPIECZEŃSTWA

W celach demonstracyjnych naukowcy z Microsoftu i University of Michigan opracowali rootkita na poziomie BIOS-u dla komputerów PC, zwanego SubVirt, który może przetrwać wymianę dysku twardego i ponowną instalację systemu operacyjnego. SubVirt modyfikuje sekwencję rozruchową i ładuje się przed systemem operacyjnym, dzięki czemu może działać poza systemem operacyjnym i pozostać ukryty przed wieloma narzędziami do wykrywania rootkitów. Wykorzystując technologię wirtualizacji sprzętu od producentów procesorów, SubVirt może załadować oryginalny system operacyjny jako maszynę wirtualną, a następnie przechwytywać wywołania systemu operacyjnego do sprzętu.

Co się stanie, jeśli używany przez Ciebie system zostanie naruszony jeszcze przed jego zakupem? Przestępcy w Europie manipulowali urządzeniami do obsługi kart kredytowych, gdy te były jeszcze w łańcuchu dostaw. Naruszone urządzenia nadal działają jak normalne czytniki kart kredytowych, z jednym godnym uwagi wyjątkiem: kopiują informacje o kartach kredytowych klientów i przesyłają je przestępcom za pośrednictwem sieci telefonii komórkowej. Jedynym sposobem na pozbycie się tego typu infekcji jest flashowanie (ponowne zapisanie) BIOS-u znaną czystą kopią, wyczyszczenie dysku twardego i ponowne załadowanie systemu operacyjnego z czystego nośnika instalacyjnego. Te zadania mogą być bardzo kosztowne pod względem czasu i pieniędzy, ale przynajmniej istnieje metoda usuwania złośliwego oprogramowania. Popularna usługa odzyskiwania laptopów po kradzieży, LoJack for Laptops, ma pewne luki na poziomie projektu, które mogą być wykorzystywane przez rootkity. Naukowcy z Core Security Technologies przekonfigurowali LoJack za pomocą niestandardowego rootkita BIOS, który wykorzystuje luki LoJack. Ponieważ infekcja znajduje się w BIOS-ie komputera, utrzymuje się nawet po ponownej instalacji systemu operacyjnego lub wymianie dysku twardego.

Bardziej niepokojące dla specjalistów ds. bezpieczeństwa jest to, że agent BIOS LoJack jest przechowywany w części BIOS-u, która nie jest nadpisywana podczas flashowania. Agent BIOS LoJack okresowo „dzwoni do domu" do centralnego organu monitorującego w celu uzyskania instrukcji w przypadku zgłoszenia kradzieży laptopa. Mechanizm połączenia domowego pozwala organowi monitorującemu nakazać agentowi BIOS LoJack wyczyszczenie wszystkich informacji jako środek bezpieczeństwa lub śledzenie lokalizacji skradzionego systemu. Ponieważ tak wiele laptopów ma zainstalowanego tego agenta i nie można go usunąć, jest on atrakcyjnym celem dla atakujących.

Identyfikowanie luk w zabezpieczeniach urządzeń IoT

Czas trwania: 30 minut

Cel: Przeskanuj urządzenie IoT w celu wykrycia otwartych portów.

Opis: Urządzenia IoT częściej znajdują się w domach, ale można je również podłączyć do sieci przedsiębiorstw. Wielu użytkowników łączy się zdalnie z sieciami służbowymi z domu, więc zainfekowane urządzenie IoT w domu może stanowić zagrożenie dla sieci służbowej. Odkrycie urządzeń IoT i otwartych portów to dobry początek zwiększania bezpieczeństwa urządzeń IoT i sieci.

1. Określ adres IP urządzenia IoT w sieci (np. telewizora Smart TV). Możesz użyć Nmap lub Zenmap, aby określić adresy IP i producentów urządzeń w sieci. Jeśli jesteś w pracy lub w klasie, koniecznie poproś o pozwolenie na skanowanie sieci za pomocą Nmap i je otrzymaj, ponieważ w przeciwnym razie możesz zostać wykryty jako atakujący.

2. Po znalezieniu celu IoT wykonaj intensywne skanowanie Nmap tylko na tym docelowym adresie IP. Nie skanuj całej sieci, zwłaszcza jeśli jesteś podłączony do sieci szkolnej lub służbowej.

3. Jakie porty znalazłeś otwarte? Na podstawie otwartych portów, jakie usługi możesz przypuszczać, że są uruchomione na urządzeniu IoT? Na podstawie odkrytych informacji, na jakie ataki urządzenie IoT może być podatne? Krótko udokumentuj swoje odkrycia i omów je z kolegą z klasy, przyjacielem lub członkiem rodziny.

Teraz, gdy lepiej rozumiesz luki w zabezpieczeniach systemów operacyjnych, czytaj dalej, aby dowiedzieć się, jak możesz poprawić ich bezpieczeństwo.

Najlepsze praktyki ochrony systemów wbudowanych

Dowiedziałeś się, że Twoim zadaniem jako testera bezpieczeństwa jest odkrywanie i dokumentowanie luk w zabezpieczeniach oraz zalecanie sposobów ich naprawy. Teraz, gdy wiesz, że systemy wbudowane mają luki w zabezpieczeniach podobne do luk w systemach ogólnego przeznaczenia, a także dodatkowe wyzwania związane z bezpieczeństwem, co możesz zrobić?

• Zidentyfikuj wszystkie systemy wbudowane w organizacji.

• Nadaj priorytet systemom lub funkcjom, które są od nich zależne.

• Postępuj zgodnie z zasadą najmniejszych uprawnień w celu uzyskania dostępu do systemów wbudowanych.

• Używaj szyfrowania przesyłu danych, jeśli to możliwe, do komunikacji systemów wbudowanych.

• Konfiguruj systemy wbudowane tak bezpiecznie, jak to możliwe, i postępuj zgodnie z zaleceniami producentów.

• Jeśli to możliwe, używaj środków kryptograficznych, takich jak TPM, do uruchamiania systemów wbudowanych, zwłaszcza gdy utrata danych lub zmiana w zachowaniu systemu stanowi poważne ryzyko.

• Zainstaluj poprawki i aktualizacje, jeśli są dostępne, aby rozwiązać problemy z lukami w zabezpieczeniach. Upewnij się jednak, że jest to możliwe w systemie wbudowanym, z którym pracujesz; niektóre systemy wbudowane nie mogą mieć przestoju na instalowanie aktualizacji i poprawek.

• Zmniejsz potencjalne luki w zabezpieczeniach, ograniczając dostęp do sieci tylko do adresów IP, które muszą komunikować się z systemami wbudowanymi i zmniejszając powierzchnię ataku systemów wbudowanych, wyłączając lub blokując niepotrzebne usługi.

• Uaktualnij lub wymień systemy wbudowane, których nie można naprawić lub które stanowią niedopuszczalne ryzyko.

PODSUMOWANIE MODUŁU

• System wbudowany to dowolny system komputerowy, który nie jest serwerem ogólnego przeznaczenia ani komputerem PC. Wbudowany system operacyjny i jego sprzęt to główne komponenty systemu wbudowanego.

• RTOS to wyspecjalizowany wbudowany system operacyjny zaprojektowany z algorytmami mającymi na celu wykonywanie wielu zadań jednocześnie i przewidywalne reagowanie; jest używany w urządzeniach takich jak programowalne termostaty, sterowanie urządzeniami, samoloty i statki kosmiczne.

• Większość sieci korporacyjnych i budynków ma liczne wbudowane systemy, takie jak routery i przełączniki, zapory sieciowe, kopiarki, drukarki, faksy, telefony cyfrowe, systemy HVAC, domofony i systemy przeciwpożarowe.

• Microsoft oferuje kilka wbudowanych systemów operacyjnych. Windows 10 IoT, najnowocześniejszy z tych systemów, jest podobny do starszych wersji Windows Embedded Standard. Windows CE był wbudowanym systemem operacyjnym zaprojektowanym dla urządzeń mobilnych, a Windows Embedded Standard był przykładem systemu operacyjnego Windows PC zmodyfikowanego do użytku w systemach wbudowanych.

• Wbudowane systemy operacyjne Microkernel, takie jak QNX, GreenHills i VxWorks, wymieniają elastyczność na większe bezpieczeństwo i prostotę i są często używane, gdy bezpieczeństwo i ochrona są kluczowe.

• *Wbudowane systemy operacyjne oparte na Nix są często używane w urządzeniach, w których wymagana jest elastyczność i szeroki zakres funkcji oraz obsługi sprzętu, takich jak GPS-y, PDA i iPhone'y.

• Wbudowane systemy operacyjne są teraz bardziej powszechne niż w czasie światowej paniki spowodowanej luką Y2K. Fakt, że są wszędzie, podkreśla znaczenie włączania zabezpieczeń do fazy projektowania wbudowanego systemu operacyjnego.

• Wbudowane systemy operacyjne są zwykle połączone w sieć w celu zwiększenia wydajności. Jednak trudno je załatać, co może zwiększyć koszty ich zabezpieczania. Luki w zabezpieczeniach wbudowanych systemów operacyjnych są często takie same, jak w systemach operacyjnych ogólnego przeznaczenia.

Wykorzystywanie wbudowanych systemów operacyjnych, takich jak bankomaty, może być opłacalne dla przestępców.

• Systemy wbudowane znajdują się w urządzeniach sieciowych i urządzeniach peryferyjnych w niemal każdej sieci, a w porównaniu z systemami komputerowymi ogólnego przeznaczenia, ich podatności są często pomijane.

• Systemy SCADA są używane w systemach infrastruktury krytycznej, takich jak wytwarzanie i dystrybucja energii, kontrola ruchu lotniczego i kolei, zapory i roboty publiczne oraz ciężki przemysł. Uszkodzenie tych systemów wbudowanych może mieć katastrofalne skutki.

• Smartfony są przykładami stale rozwijającego się systemu wbudowanego, który może zostać wykorzystany do kradzieży poufnych informacji korporacyjnych i osobistych.

• Smartfony mogą zostać zainfekowane złośliwym oprogramowaniem trojańskim i wykorzystane tak jak systemy Windows i Linux.

• Rootkity oprogramowania układowego stanowią największe zagrożenie dla systemu operacyjnego wbudowanego. Kryptograficzna ochrona rozruchu, taka jak ta zapewniana przez TPM, może pomóc w obronie przed rootkitami oprogramowania układowego.

• Przestrzeganie najlepszych praktyk, takich jak identyfikacja wszystkich systemów wbudowanych, stosowanie poprawek, gdy jest to możliwe, przestrzeganie zasady najmniejszych uprawnień i ograniczanie dostępu, jest ważne dla zapewnienia bezpieczeństwa systemów wbudowanych.