Sposoby zabezpieczania urządzeń elektronicznych przed występowaniem w nich ukrytych funkcji

Mgr inż. Paweł Koszut
Prof. dr hab. inż. Zbigniew Kotulski

Instytut Telekomunikacji
Politechnika Warszawska
15 październik 2009 r.

Streszczenie: Niniejsza praca porusza problematykę występowania ukrytych funkcji w urządzeniach elektronicznych oraz oprogramowaniu. Jest szczególnie ważne, by urządzenia o znaczeniu strategicznym, np. urządzenia przetwarzające informacje niejawne lub urządzenia istotne dla funkcjonowania infrastruktury telekomunikacyjnej, zabezpieczone były przed zagrożeniami związanymi z występowaniem w nich dodatkowych, ukrytych funkcji. W celu prawidłowego, tj. opartego na rzetelnej ocenie zagrożeń, zabezpieczenia tych urządzeń należy przede wszystkim uwzględnić współczesne metody ataków i włamań, a także sposoby utrudniania wykrycia celowo zaimplementowanych ukrytych funkcji. W niniejszej publikacji, będącej rezultatem analizy trendów w tej dziedzinie bezpieczeństwa, przedstawiono niektóre aspekty dotyczące współczesnych zagrożeń, które warto uwzględnić podczas oceny aktualnej lub wyboru nowej polityki bezpieczeństwa teleinformatycznego. Skoncentrowano się szczególnie na komponencie software'owym urządzeń.

W zależności od potrzeb, wymagany stopień bezpieczeństwa badanych urządzeń elektronicznych oraz poziom zaufania w prawidłowość ich działania, może być różny. Dążąc jednak do zapewnienia możliwie najwyższego poziomu bezpieczeństwa w tych przypadkach, kiedy jest to szczególnie ważne, należy analizować zarówno metody ochrony przed współczesnymi zagrożeniami, jak i najnowsze metody ataków i przełamywania zabezpieczeń. Takie podejście jest konieczne, by nie pozostawać „krok za” włamywaczami.

Urządzenia elektroniczne, w tym tak istotne dla bezpieczeństwa teleinformatycznego urządzenia sieciowe, szyfratory, środki łączności bezprzewodowej, są urządzeniami, na których bezpieczeństwo można spojrzeć z punktu widzenia dwóch istotnych komponentów : ich architektury sprzętowej oraz ich oprogramowania.

W naszej pracy skupimy się szczególnie na drugim z tych aspektów. Wcześniej jednak, warto wspomnieć, że czynników ważnych dla bezpieczeństwa teleinformatycznego jest więcej, i nie wszystkie

są czynnikami technicznymi. Np. :

- stopień zaufania do producenta – przykładowo, dla urządzeń niejawnych wymaga się, by ich producent posiadał ważne poświadczenie bezpieczeństwa przemysłowego, wydane przez właściwą Służbę Ochrony Państwa (ABW lub SKW).
- relacje handlowe z innymi firmami, w szczególności zagranicznymi – dostawcy podzespołów elektronicznych, potrzebnych do budowy urządzeń, mogą stanowić potencjalne źródło zagrożeń.

Dalsza część pracy dotyczy technicznych aspektów bezpieczeństwa. Przedstawione zostaną niektóre metody używane do przeprowadzania ataków, przełamywania zabezpieczeń i ukrywania dodatkowych funkcji w systemach i urządzeniach elektronicznych. Zapoznanie się z tymi metodami umożliwia lepszy dobór i skuteczniejsze zastosowanie środków zaradczych.

Oprogramowanie stanowi istotny element wpływający na bezpieczeństwo urządzeń telekomunikacyjnych. Routery, switche, firewall'e, szyfratory VPN, i inne urządzenia posiadają swoje oprogramowanie – jest na nich zainstalowany system operacyjny. Niektórzy producenci tworzą własny system operacyjny, np. system Cisco IOS stosowany w urządzeniach sieciowych firmy Cisco, a inni korzystają z jednego z dostępnych już systemów, np. Linux, OpenBSD i modyfikują go na potrzeby budowanego sprzętu – np. Linux w urządzeniach sieciowych firmy Barracuda. Bezpieczeństwo oprogramowania jest również istotne dla wielu zwykłych użytkowników komputerów osobistych PC.

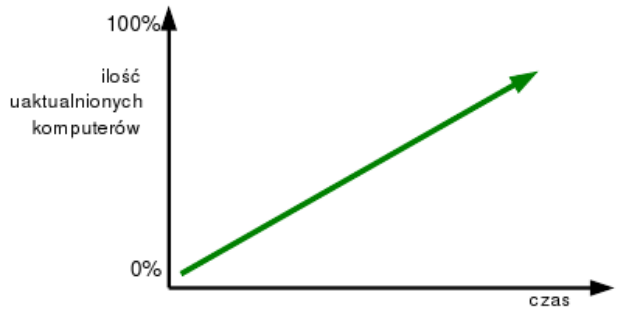
W sferze bezpieczeństwa oprogramowania, coraz istotniejszym problemem staje się wpływ tzw. zero-dniowych luk bezpieczeństwa (ang. zero-day security vulnerabilities). Poniżej zjawisko to zostanie bliżej przedstawione, dla lepszego jego zrozumienia.

Powszechnie uważa się, że w celu ochrony np. swojego komputera osobistego PC, należy regularnie uaktualniać oprogramowanie i wprowadzać udostępniane przez producenta łatki systemowe. Uaktualnianie komputera ma chronić przed znajdowanymi dziurami bezpieczeństwa. Rzeczywiście jest to dobry nawyk i podwyższa on poziom bezpieczeństwa. Pójdźmy jednak dalej za ideą przyświecającą napisaniu tej publikacji i przeanalizujmy jakie konsekwencję dla atakującego pociąga za sobą taki stan obowiązujących dziś praktyk w dziedzinie bezpieczeństwa IT. Zadajmy sobie więc pytanie czym teraz atakujący mogą nas zaskoczyć? Przede wszystkim warto zwrócić uwagę na kilka prostych spostrzeżeń dotyczących wspomnianej praktyki uaktualniania oprogramowania. Mianowicie, licząc od czasu, gdy

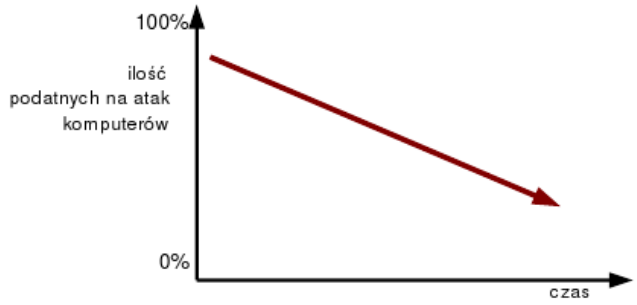
opublikowana została informacja o występowaniu krytycznej luki bezpieczeństwa, użytkownicy danego oprogramowania uaktualniają je, a zatem :

1) ilość zabezpieczonych komputerów zwiększa się w miarę upływającego czasu (rys. nr 1),

2) ilość komputerów podatnych na włamanie zmniejsza się (rys. nr 2),

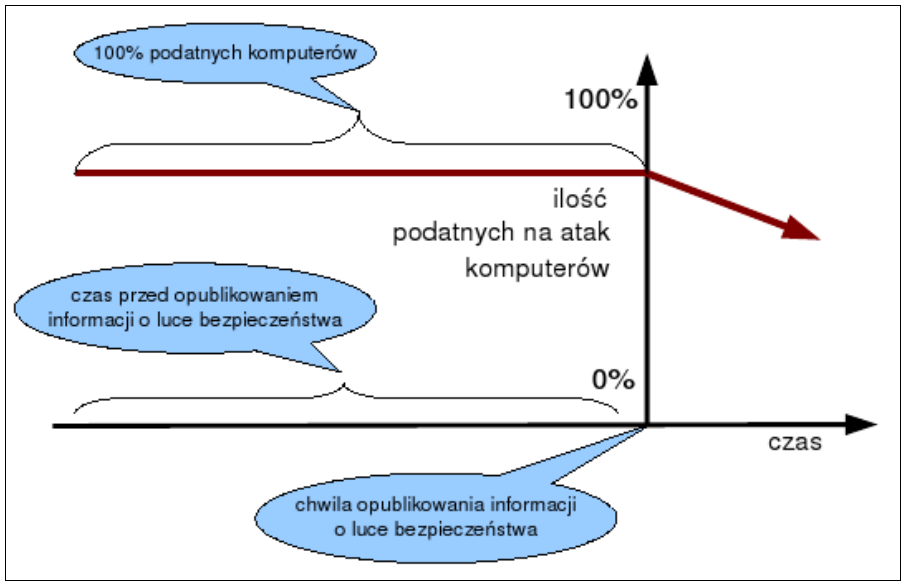


Rysunek 1



Rysunek 2

3) przed chwilą czasu, gdy opublikowana została informacja o luce systemowej, ilość podatnych komputerów wynosiła 100% (rys. nr 3).



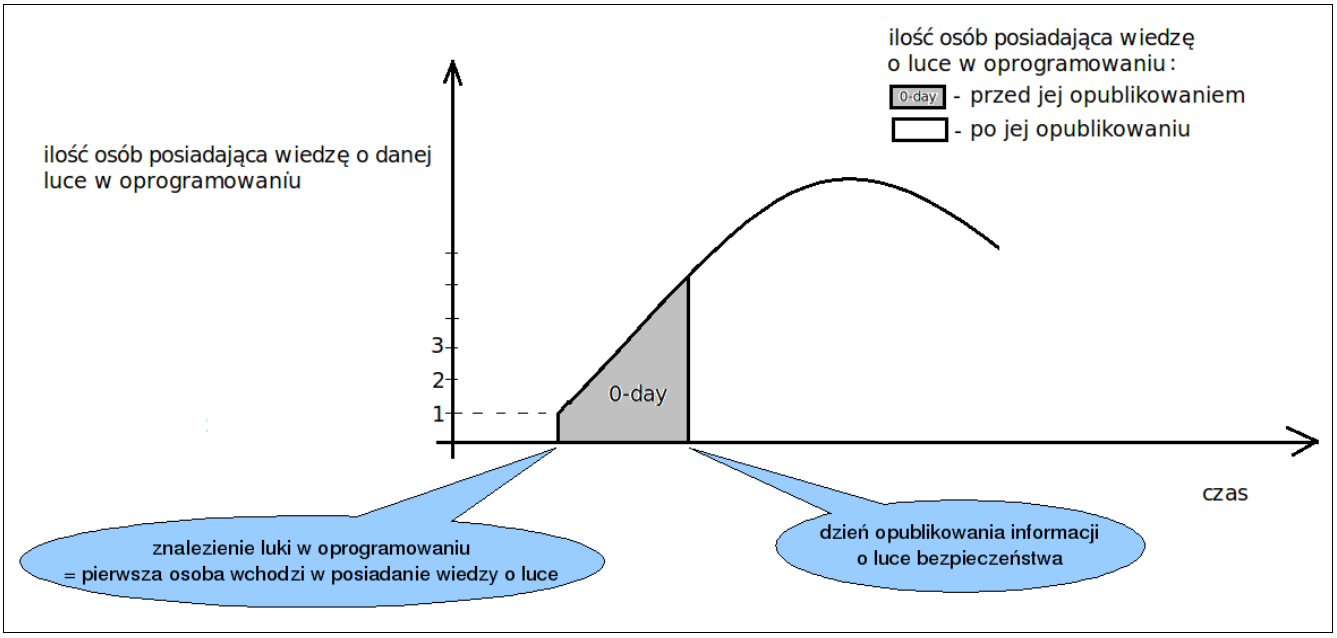
Rysunek 3

Dla atakującego, ze spostrzeżeń nr 1 i 2 wynika, że posiadana przez niego informacja o danej luce w oprogramowaniu jest tym groźniejsza (tym skuteczniejsza), im mniej czasu upłynęło od momentu jej

opublikowania. Ze spostrzeżenia nr 3 wynika, że najcenniejsze dla atakującego i zarazem najgroźniejsze dla użytkowników są te luki, które jeszcze nie zostały opublikowane*. Są to właśnie tzw. luki zero-dniowe.

Innymi słowy, jeżeli informacja o krytycznej luce pojawiła się np. 15 marca 2009, to następnego dnia, tj. 16 marca 2009 krytyczna luka jest bardziej groźna niż miesiąc później, tj. 15 kwietnia 2009 r. lub rok później tj. 15 marca 2010. Natomiast najbardziej niebezpieczna jest ona (i jest ona jednocześnie wtedy luką zero-dniową) przed dniem 14 marca 2009 r., a zatem przed dniem jej opublikowania.

Ważnym pytaniem jakie należy sobie więc zadać jest : jakie grupy osób mają dostęp do tych istotnych informacji o krytycznych lukach zero-dniowych?



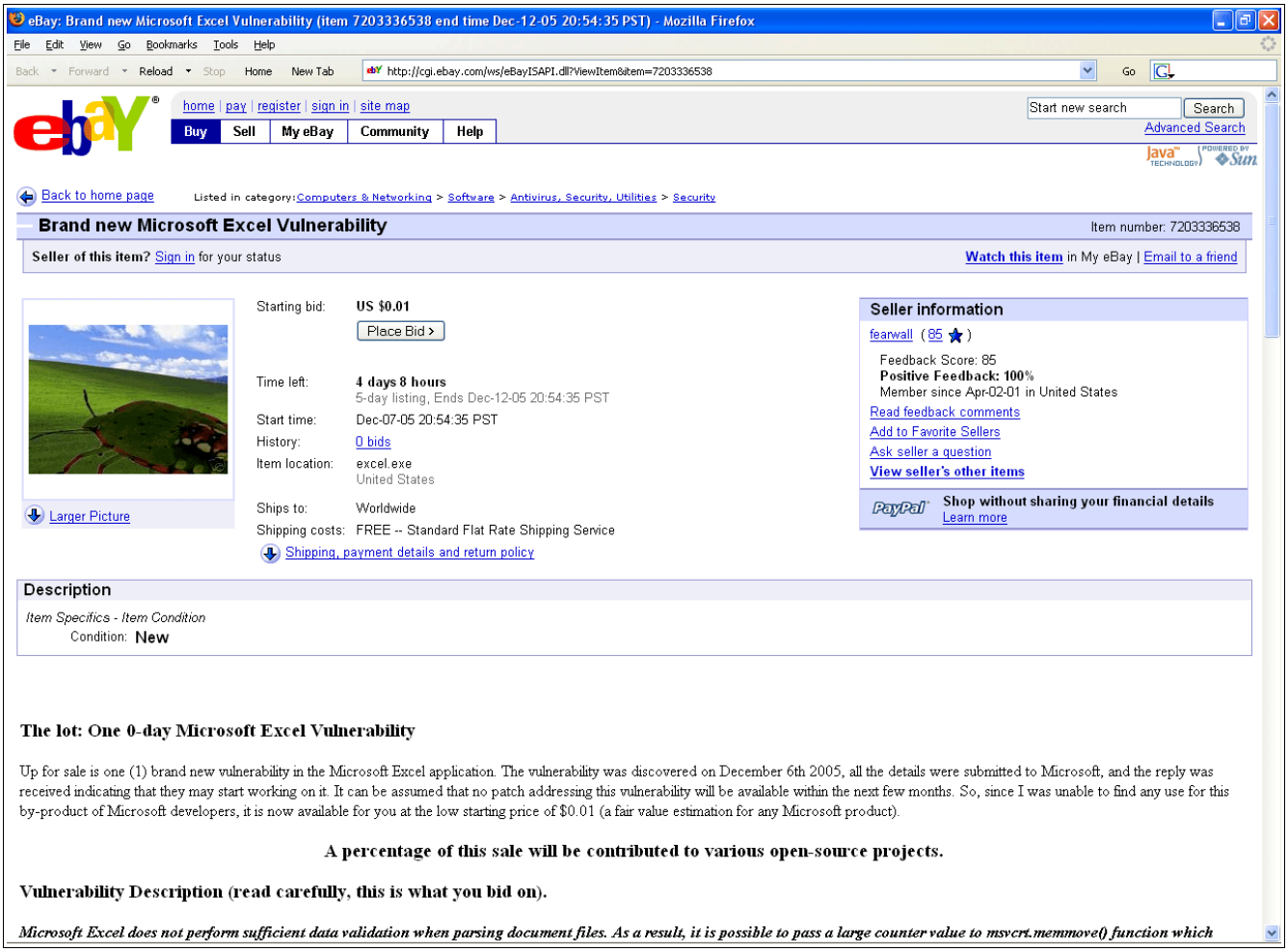
Rysunek 4

Jako oczywistą grupę osób, posiadających tę wiedzę można wymienić programistów zatrudnionych u producenta oprogramowania/urządzenia, którzy poprawiają wspomniane błędy. Aby mogli oni załatać dziurę poprzez napisanie i udostępnienie odpowiedniej łatki, muszą oni znać szczegóły dotyczące tej luki.

* W sensie ścisłym nie chwila opublikowania luki jest istotna, a chwila udostępnienia łatki przez producenta lub uaktualnienia bazy sygnatur ataków w posiadanym przez użytkowników oprogramowaniu zabezpieczającym.

Innymi osobami, oprócz osób związanych z producentem oprogramowania/urządzenia, są eksperci, którzy legalnie zgłaszają producentom znalezione przez siebie luki w oprogramowaniu. Producenci urządzeń i oprogramowania coraz częściej nagradzają takich znalazców finansowo, a następnie poprawiają wykryte przez nich błędy zanim staną się one groźne dla ich klientów. W ten sposób dążą do poprawy bezpieczeństwa swoich produktów. Na stronie internetowej www.zerodayinitiative.com znaleźć można jeden z takich programów, gdzie można zgłaszać znalezione przez siebie luki. Dzięki takim zgłoszeniom, nie tylko producenci oprogramowania/urządzeń zawierających niebezpieczne luki mogą je poprawiać, ale także inne firmy, które sprzedają oprogramowanie zabezpieczające i antywirusowe mogą w swoich produktach zamieszczać sygnatury nowych ataków chroniąc swoich klientów nawet wtedy, gdy producent zagrożonego systemu/urządzenia nie zdąży zabezpieczyć swoich produktów.

Naturalnie wśród osób znajdujących luki bezpieczeństwa należy się także spodziewać osób, które wykorzystują swoją wiedzę niezgodnie z prawem. Luki bezpieczeństwa, w tym także szczególnie niebezpieczne luki zero-dniowe, są wykorzystywane przez cyber-przestępców jako narzędzie do włamań. Wiedza, potrzebna do opracowania działającego narzędzia do włamania, może być zaczerpnięta z różnych źródeł. Informacje o lukach zero-dniowych niekoniecznie trzeba zdobyć samemu. Można je np. kupić – rysunek nr 5 przedstawia aukcję na eBay, która została zablokowana przez administratorów ze względu na łamanie regulaminu. Niedoszły sprzedawca wystawił na licytację lukę zero-dniową, występującą w programie Microsoft Excel. Kilka miesięcy później w biuletynie bezpieczeństwa Microsoft Security Bulletin MS06-012 - „Vulnerabilities in Microsoft Office Could Allow Remote Code Execution”[1] firma podała informację, że pakiet MS Office zawiera krytyczny błąd, który można wykorzystać do zdalnego wykonania kodu.



źródło: http://osvdb.org/ref/blog/ebay-bug.gif

Rysunek 5

Zagadnienia związane z funkcjonowaniem rynku informacji o lukach bezpieczeństwa zostały przedstawione w publikacji pt. „The Legitimate Vulnerability Market, Inside the Secretive World of 0-day Exploit Sales" napisanej przez dr Charlie Miller'a [2].

Zdobyta wiedza o lukach zero-dniowych potrzebna do dokonania skutecznego włamania, może pochodzić także z samych urządzeń zabezpieczających i oprogramowania antywirusowego. Jak wspomniane było wcześniej, niektórzy producenci oprogramowania antywirusowego i przemysłowych urządzeń zabezpieczających chcąc poprawić wykrywalność ataków, a tym samym skuteczność swoich produktów, umieszczają w nich bazę sygnatur najnowszych ataków – w tym także ataków wykorzystujących luki zero-dniowe. Zatem poprzez demontaż urządzeń i analizę informacji

znajdujących się na nośnikach w urządzeniach zabezpieczających, można uzyskać sygnatury ataków zero-dniowych, co umożliwia uzyskanie wiedzy potrzebnej do przeprowadzenia danego ataku. Mimo, iż baza sygnatur w jednym z analizowanych urządzeń była zabezpieczona kryptograficznie, autorzy publikacji „A Simpler Way of Finding 0day" [3] wykazali, iż możliwe jest wydostanie tych cennych informacji z urządzenia przez zastosowanie tzw. metod inżynierii wstecznej (ang. reverse engineering).

Jak widać krytyczne luki bezpieczeństwa mogą być uzyskiwane w różnoraki sposób a ich nielegalne wykorzystanie może stanowić zagrożenie. Dla bezpieczeństwa urządzeń, których znaczenie jest szczególnie ważne dla funkcjonowania krytycznej infrastruktury telekomunikacyjnej lub ochrony informacji niejawnych, warto zauważyć, iż nie da się wykluczyć możliwości celowego pozostawienia luki bezpieczeństwa. Takie zjawisko polegałoby na celowym tworzeniu ukrytej funkcji w urządzeniu lub oprogramowaniu, która nie byłaby wykrywalna przez metody bazujące na przeglądaniu kodu źródłowego. Przeglądanie kodu źródłowego może jedynie skutecznie wykryć klasyczną implementację dodatkowej ukrytej funkcji (pod warunkiem, że kod został przeanalizowany ze zrozumieniem), natomiast nie zapobiegnie implementacji, w której wykorzystuje się te same mechanizmy, na których bazują luki zero-dniowe. Innymi słowy, te same metody zaradcze, które regularnie nie sprawdzają się przy wykrywaniu luk w bezpieczeństwie naszego oprogramowania codziennego użytku, także nie ochronią skutecznie urządzeń elektronicznych o specjalnym znaczeniu przed ukrytymi funkcjami zaimplementowanych celowo. Pod względem technicznym zero-dniowe luki bezpieczeństwa zaimplementowane celowo nie różnią się od tych, pozostawianych przez niedopatrzenie podczas zwykłego procesu technologicznego wytwarzania oprogramowania.

Analizując bezpieczeństwo urządzeń elektronicznych warto więc liczyć się z możliwościami, jakie dają takie sposoby wniesienia zagrożeń do badanych systemów i uwzględnić je podczas planowania polityki bezpieczeństwa. Warto także pamiętać, że oprogramowanie stanowi jeden z dwóch kluczowych komponentów takich urządzeń. Drugim jest ich architektura sprzętowa, gdzie również możliwe jest zagnieżdżenie ukrytej funkcji w sposób trudno wykrywalny. Ukryte funkcje mogą także występować w więcej niż jednym miejscu w danym systemie/urządzeniu (zarówno zaimplementowane w sprzęcie, jak i w oprogramowaniu) oraz mogą być zaprojektowane tak, by dopiero współpracując ze sobą tworzyły funkcjonalnie jedną całość. Takie podejście dodatkowo utrudnia ich wykrycie. Środki zaradcze zatem, które mają na celu wyeliminowanie lub ograniczenie wspomnianych zagrożeń powinny opierać się na dogłębnej analizie, uwzględniającej w swoich założeniach jakie środki ofensywne może

zastosować atakujący, by przełamać nasze zabezpieczenia i procedury ochronne. Takie podejście jest konieczne, by możliwe było podjęcie odpowiednich kroków defensywnych w celu możliwie najskuteczniejszego zabezpieczenia rozpatrywanych urządzeń.

[1] Microsoft Security Bulletin MS06-012 - „Vulnerabilities in Microsoft Office Could Allow Remote Code Execution" - http://www.microsoft.com/technet/security/Bulletin/MS06-012.mspx

[2] dr Charlie Miller, „The Legitimate Vulnerability Market, Inside the Secretive World of 0-day Exploit Sales", 2007

[3] Robert Graham, David Maynor „A Simpler Way of Finding 0day" Errata Security.