Bezpieczeństwo systemów komputerowych

Tomasz Lewicki

WWSIS, Wrocław

kwiecień 2007

Bezpieczeństwo – co to znaczy?

- Zespół zasad, jakimi należy się kierować projektując i wykorzystując system komputerowy, by w każdych okolicznościach dostęp do niego był zgodny z założeniami
- Projektując zasady bezpieczeństwa trzeba uwzględnić środowisko (otoczenie), w jakim działa system komputerowy
- Szybki rozwój komunikacji w sieciach różnego typu wymusza nowe spojrzenie na bezpieczeństwo

Motto na dziś

„Bezpieczeństwo to proces, a nie produkt”

Bruce Schneier

Dlaczego chronimy systemy komputerowe?

Musimy być przygotowani na naruszenia bezpieczeństwa **przypadkowe** (awarie sprzętu, zaniki zasilania, błędy ludzkie, zdarzenia losowe) i **celowe** (odczytywanie danych i/lub ich modyfikacja bez upoważnienia, złośliwe utrudnienie i/lub uniemożliwienie działania systemu w „normalny" sposób).

Paradoks: **łatwiej chronić przed naruszeniami przypadkowymi**!

Przykłady:

- nadmiarowość zabezpiecza przed skutkami awarii sprzętu
- systemy zasilania awaryjnego zabezpieczają przed skutami utraty zasilania w sieci elektrycznej
- automatyczne systemy dozoru zabezpieczają przed skutkami niektórych zdarzeń losowych (kradzież, pożar, zalanie)

Bezpieczeństwo – jak to „ugryźć”?

Na bezpieczeństwo systemu komputerowego należy patrzeć **kompleksowo** i wielotorowo, starając się przewidzieć różne scenariusze.

Nie można przewidzieć wszystkiego $\Longrightarrow$ **osiągnięcie pełnego bezpieczeństwa jest niemożliwe**, można jedynie **obniżać ryzyko**.

Najsłabszym punktem w systemie zabezpieczeń jest **człowiek**.

Poziomy bezpieczeństwa

Zagadnienie ochrony systemu komputerowego możemy podzielić na kilka poziomów:

Fizyczny
Zabezpieczenie systemu komputerowego przed fizycznym dostępem osób niepowołanych (weryfikacja personelu, systemy alarmowe, . . .) oraz przed awariami sprzętu i zdarzeniami losowymi

Ludzki
Edukowanie użytkowników i operatorów systemu o zakresie ich uprawnień, uczulanie ich na metody socjotechniczne stosowane przez potencjalnych napastników

Poziomy bezpieczeństwa – c.d.

System operacyjny
Wybranie SO odpowiedniego do potrzeb; zaprojektowanie SO w taki sposób, by sam mógł chronić się przed naruszeniami bezpieczeństwa o różnej genezie

Sieciowy
Zabezpieczenie danych przesyłanych za pośrednictwem różnych mediów transmisyjnych i zapewnienie ich poufności oraz integralności; wykluczenie możliwości przechwycenia transmisji

Uwierzytelnianie (autentykacja)

Jest to jeden z podstawowych sposobów ograniczania dostępu do systemu komputerowego do kręgu zaufanych użytkowników.

Najpopularniejszą metodą sprawdzania tożsamości użytkowników jest stosowanie haseł (właściwie par *identyfikator/hasło*).

Nowoczesne systemy operacyjne nie przechowują haseł użytkowników w postaci jawnej (niezaszyfrowanej). Przy każdorazowej próbie dostępu do chronionych zasobów systemu hasło wprowadzone przez użytkownika jest szyfrowane i porównywane z tzw. *hash*-em, czyli skrótem kryptograficznym obliczanym według pewnego algorytmu.

Uwierzytelnianie za pomocą haseł

Zalety:

- Łatwe do wdrożenia i proste w stosowaniu
- Użytkownicy są przyzwyczajeni do systemów, w których stosowane są różne rozwiązania oparte na hasłach

Wady:

- Hasło może zostać skompromitowane (złamane, odgadnięte, podejrzane, przechwycone, wyjawione celowo lub przypadkowo)
- Użytkownicy są z natury „leniwi”, tzn. mają tendencję do stosowania nieskomplikowanych haseł, powielania haseł i ich beztroskiego ujawniania
- Ludzie są podatni na socjotechnikę

Utwardzanie haseł

- Stosowanie odpowiednio silnych algorytmów kryptograficznych
- Wymóg stosowania haseł długich i skomplikowanych, wykorzystujących wszystkie znaki dostępne z klawiatury (a...z, A...Z, 0...9, znaki specjalne)
- Regularne zmiany haseł i uniemożliwienie ich powtarzania
- Uniemożliwienie stosowania haseł słownikowych
- Ograniczenie ilości niedanych prób logowania w połączeniu z czasową blokadą konta
- Okresowe badanie odporności haseł stosowanych przez użytkowników

Szybko, łatwo i. . . niebezpiecznie

- Niech hasło będzie takie jak login
- Niech hasłem będzie imię Twoje, Twojej żony/dziecka/psa itd.
- Niech Twoje hasło brzmi jak marka Twojego samochodu/telefonu itd.
- Niech Twoje hasło będzie łatwe jak data urodzenia/PESEL/NIP itd.
- Niech hasłem będzie prosta sekwencja klawiszy (`qwerty`, `qaz123` itp.)

Przykłady bardziej „wymyślnych" haseł:
`vv!OsHA` (*wiosna*)
`@L1cjaWKC` (*Alicja w Krainie Czarów*)
`W6MzkpgsVW` (*W sobotę Maciek zabił kota przejeżdżając go swoim Volkswagenem*)

Metody biometryczne

Polegają na analizie indywidualnych, niepowtarzalnych cech żywych organizmów i wykorzystaniu tej wiedzy np. do identyfikacji poszczególnych osobników. W przypadku systemów komputerowych pozwalają na dokładniejszą kontrolę dostępu do tychże systemów.

Cechy biometryczne można podzielić na **fizyczne** oraz **behawioralne** (związane z zachowaniem). W celu dokładniejszej identyfikacji można łączyć pomiary różnych cech jednej osoby.

Pomiar cech biometrycznych powinien być szybki, dokładny i nie wymagający zbyt wielkiego zaangażowania ze strony weryfikowanej osoby.

Potencjalna niedogodność: cechy biometryczne ulegają zmianom z biegiem czasu i/lub przypadkowo!

Nieco futurologii

Fizyczne cechy biometryczne

- Układ linii papilarnych
- Geometria twarzy
- Geometria dłoni
- Wzór tęczówki lub siatkówki oka
- Układ naczyń krwionośnych
- Kształt ucha
- Mapa temperaturowa określonych części ciała
- Układ zębów
- Zapach
- Kod genetyczny

Nieco futurologii – c.d.

Behawioralne cechy biometryczne

- podpis odręczny
- głos (tembr głosu, szybkość mówienia, akcent)
- chód (długość kroku, nacisk na podłoże, rozłożenie masy ciała)
- sposób pisania na klawiaturze (szybkość pisania, siła nacisku na klawisze, odstęp między kolejnymi naciśnięciami klawiszy)
- reakcja mózgu na znany bodziec

Złośliwe oprogramowanie – kategorie zagrożeń

Złośliwe oprogramowanie (*malicious software*, in. *malware*) występuje w licznych odmianach:

- wirus – program lub kod powielający się dzięki dołączeniu do innego programu lub makra (tzw. nosiciela)
- robak – samodzielny program rozprzestrzeniający się najczęściej za pośrednictwem sieci
- koń trojański – program lub kod ukryty w pliku systemowym, w programie użytkowym lub zakamuflowany w inny sposób
- *backdoor* (tylne wejście) – luka w SO lub oprogramowaniu użytkowym, która pozwala nieuprawionym osobom na obejście zabezpieczeń systemu komputerowego
- *spyware* – oprogramowanie śledzące poczynania użytkownika; często występuje w połączeniu z innymi rodzajami złośliwego oprogramowania

Złośliwe oprogramowanie – c.d.

- *keylogger* – program rejestrujący sekwencje naciskanych klawiszy; również urządzenie o takiej nazwie
- *rootkit* – zespół programów umożliwiających włamania do systemów komputerowych; ukrywa pliki i procesy uruchomione przez napastnika
- *exploit* – program lub kod wykorzystujący błędy w oprogramowaniu; często służy do przeprowadzania zdalnych ataków
- bomba logiczna – program lub kod uruchamiający się po spełnieniu pewnych warunków logicznych
- bomba czasowa – program lub kod uruchamiający się w ściśle określonej chwili (można ją uznać za szczególny przypadek bomby logicznej)
- królik/bakteria – program namnażający się bez ograniczeń i zajmujący zasoby SO (najczęściej pamięć operacyjną i przestrzeń dyskową)
- *joke* (żart) – program zazwyczaj nie wyrządzający szkód, wywołujący strach lub zaskoczenie u użytkownika

Najczęstsze działania ze strony malware'u

- Zmiana ustawień sieci (np. filtrowanie określonych rodzajów ruchu sieciowego, zmiana listy znanych hostów, kierowanie zapytań DNS przez serwer atakującego)
- Deaktywacja oprogramowania ochronnego (antywirusowego i antyspyware'owego)
- Wyłączanie „Centrum zabezpieczeń" i automatycznych aktualizacji systemu Windows
- Instalowanie *rootkit*ów utrudniających wykrycie przez użytkownika
- Instalacja fałszywych certyfikatów w przeglądarkach
- Pobieranie z Internetu innych szkodliwych programów
- Logowanie sekwencji znaków wpisywanych z klawiatury
- Monitorowanie odwiedzanych stron WWW, wpisów z formularzy i wykonywanie zrzutów ekranu

Najczęstsze działania ze strony malware'u – c.d.

- Skryte uruchamianie mikrofonu i/lub kamery podłączonej do komputera
- Podszywanie się pod pożyteczne oprogramowanie
- Dodawanie reklam generowanych lokalnie do stron WWW
- Uczynienie z zaatakowanego systemu serwera SMTP w celu rozsyłania *spamu*
- Przekształcenie zaatakowanego systemu w *zombie* – element *botnetu*
- Wykradanie ważnych dokumentów firmowych lub ich szyfrowanie w oczekiwaniu na okup
- Instalacja *sniffera* do podsłuchiwania ruchu w sieci, której częścią jest zaatakowany komputer

Wektory ataków

Mianem **wektora ataku** określa się drogę, technikę lub zabiegi użyte do uzyskania nieautoryzowanego dostępu do systemu komputerowego lub urządzenia sieciowego w celu przejęcia nad nim kontroli lub uzyskania zgromadzonych w nim informacji.

Przykłady:

- wirusy, robaki, *spyware*
  Niektórzy uważają wirusy i robaki za „ładunek", a nie za wektor ataku
- poczta elektroniczna
- specjalnie spreparowane strony WWW i ich zawartość (np. filmy)
- „wyskakujące okna" (*pop-up*'s)
- wstrzykiwanie kodu (*code injection*)
- *cross site scripting* (XSS)

Wektory ataków – c.d.

Przykłady – c.d.:

- makra w dokumentach tekstowych lub arkuszach kalkulacyjnych
- komunikatory internetowe
- kanały IRC (*Internet Relay Chat*)
- czaty (*chats*)
- sieci P2P (*peer-to-peer*)
- protokoły komunikacyjne (np. Bluetooth)
- kompilatory (szczególnie perfidna metoda)
- socjotechnika (inżynieria socjalna, *social engineering* – bardzo skuteczna, często stosowana w powiązaniu z innymi metodami)

Klasyfikacja ataków

Ataki na systemy informatyczne można przypisać do jednej z kilku grup, np. ze względu na:

- skutki ataku (ujawnienie lub sfałszowanie informacji, naruszenie integralności danych, aplikacji lub systemu, **zajęcie lub kradzież zasobów**, zmniejszenie lub zablokowanie dostępności usługi, bezprawne zwiększenie uprawnień)
- cel ataku (**sieć**/pojedyńczy host, **konto systemowe**, dane, proces)
- sieć docelową (wewnętrzna lub zewnętrzna; **sieć firmowa**, edukacyjna, rządowa, *ISP*)
- źródło ataku (w obrębie atakowanej sieci lub poza nią; sieci korporacyjne, edukacyjne, **osoby prywatne** (za pośrednictwem *ISP*s))

Klasyfikacja ataków – c.d.

- profil atakującego (**haker**, **zawodowy przestępca**, szpieg, terrorysta, „podglądacz” (*voyeur*), nieuczciwy pracownik, wandal, *script kiddie*)
- zamiar (celowy lub nieświadomy; **uzyskanie korzyści finansowej**, propagandowej, politycznej, wzmocnienie *ego* napastnika)
- wykorzystanie słabych punktów atakowanych systemów (**luki w konfiguracji**, luki w implementacji, luki w projekcie)
- narzędzie ataku (**samodzielny agent**, skrypt lub program, *rootkit*, polecenie użytkownika)
- technika ataku [informacje na kolejnych slajdach]

Klasyfikacja ataków według CERT

- Próbkowanie (*probing*) – próba dostępu do obiektu przez zbadanie jego charakterystyki
- Skanowanie (*scanning*) – próba dostępu do wielu obiektów naraz poprzez ustalenie obiektu z oczekiwaną charakterystyką
- Przepełnienie (*flooding*) – dostęp do obiektu poprzez nagłe przepełnienie jego możliwości przetwarzania
- Uwierzytelnienie (*authenticating*) – przedstawienie się jako osoba uprawniona oraz w razie konieczności przekazanie informacji potrzebnej do poprawnego uwierzytelnienia
- Ominięcie (*bypassing*) – ominięcie procesu zabezpieczającego poprzez zastosowanie alternatywnej drogi osiągnięcia obiektu
- Podszywanie (*spoofing*) – przedstawianie się w trakcie połączenia sieciowego jako użytkownik posiadający prawo dostępu do zasobów

Klasyfikacja ataków według CERT – c.d.

- Czytanie (*reading*) – dostęp z prawami czytania do informacji przez osobę nieuprawnioną
- Kopiowanie (*copying*) – dostęp z możliwością kopiowania do informacji przez osobę nieuprawnioną
- Kradzież (*stealing*) – przejęcie zasobów przez osobę nieuprawnioną bez pozostawienia kopii w uprawnionej lokalizacji
- Modyfikacja (*modyfing*) – zmiana zawartości lub charakterystyki obiektu ataku
- Usunięcie (*deleting*) – usunięcie (zniszczenie) obiektu ataku

Ochrona sieci przed naruszeniami bezpieczeństwa

Sieci są szczególnie wrażliwe na naruszenia bezpieczeństwa i ataki, zarówno na szkielet sieci, jak i poszczególnie hosty. Atak może pochodzić zarówno z zewnątrz, jak i z wnętrza sieci. Często wysiłki administratorów skupiają się na zabezpieczeniu sieci lokalnej od strony Internetu, pomijany jest natomiast aspekt zabezpieczeń przed intruzami z własnej sieci.

Ochrona sieci nie powinna skupiać się wyłącznie na zagrożeniach czysto sieciowych i programowych. Należy pamiętać o tak prozaicznych zagadnieniach jak zabezpieczenie infrastruktury przed fizycznym wtargnięciem czy odpowiednia edukacja użytkowników na każdym poziomie.

Edukacja użytkowników sieci

Edukacja użytkowników jest bardzo ważnym elementem **polityki bezpieczeństwa**. Ludzie są podatni na tzw. inżynierię społeczną (ang. *social engineering*), czyli techniki manipulacji ze strony innych osób. Człowiek okazuje się być często najsłabszym ogniwem systemu komputerowego. Zabezpieczenie sieci za pomocą wymyślnych urządzeń, list kontroli dostępu, *firewalli* może okazać się nic nie warte, jeśli napastnikowi uda się zdobyć zaufanie osób mających dostęp do sieci.

Intruz może „zmieniać skórę" zależnie od sytuacji i od tego, z kim aktualnie rozmawia. Oczywiście im lepiej uświadomiony użytkownik, tym mniejsza szansa napastnika na zdobycie interesujących go informacji. W sieciach korporacyjnych edukację użytkowników należy przeprowadzać począwszy od pracowników najniższego szczebla, poprzez „zwykłych" użytkowników, na administratorach sieci i kadrze kierowniczej kończąc.

Zapory ogniowe

Firewall zwany również zaporą lub ścianą ogniową jest jednym z najpopularniejszych i najskuteczniejszych sposobów ochrony sieci przed atakami i nieautoryzowanym dostępem. Jego rolą jest oddzielenie sieci zaufanej od niezaufanej, np. firmowej sieci lokalnej od Internetu lub wewnętrznej sieci firmowej od tzw. strefy zdemilitaryzowanej (*DMZ*), w której uruchomione są usługi dostępne dla klientów (np. serwer WWW z informacjami o przedsiębiorstwie).

Zapora może chronić zarówno całą sieć (wtedy będzie uruchomiona na routerze lub moście sieciowym), jak i pojedyńcze hosty, np. szczególnie ważne serwery.

Filtracja pakietów

Ochronę sieci za pomocą *firewalli* realizuje się na różne sposoby. Jednym z nich jest **filtrowanie pakietów**, polegające na analizie pakietów sieciowych przechodzących przez zaporę w obu kierunkach i przepuszczania tylko dozwolonego ruchu. Analiza jest przeprowadzana zazwyczaj na podstawie protokołu komunikacyjnego i/lub portu, na jakim nadaje/nasłuchuje dana usługa.

Filtrowanie pakietów jest realizowane programowo (np. za pomocą programu *iptables* dostępnego w Linuksie, *pf* w systemie OpenBSD lub *ipfw* z systemu FreeBSD) bądź na dedykowanych urządzeniach, które oprócz filtrowania i kontroli poprawności pakietów mogą wykonywać również inne zadania (np. ochronę antywirusową czy odsiewanie *spamu*).

Serwery pośredniczące (proxy)

Innym środkiem ochrony sieci jest stosowanie **serwerów pośredniczących** (*proxy*). Ich działanie polega na tym, że użytkownik chcący uzyskać dostęp do pewnego zasobu lub usługi najpierw łączy się z pośrednikiem, który w imieniu użytkownika łączy się ze zdalnym hostem i dopiero wtedy udostępnia żądany zasób użytkownikowi. Ma to tę zaletę, że użytkownik może dostać zawartość odfiltrowaną według reguł zdefiniowanych przez administratora *proxy* (tzw. *content filtering*).

Serwery *proxy* są zazwyczaj kojarzone z przyspieszaniem ładowania stron WWW poprzez magazynowanie w pamięci podręcznej elementów najczęściej pobieranych przez użytkowników. Mają również zdolność do ukrywania prawdziwego adresu IP użytkownika, podstawiając w jego miejsce adres IP serwera *proxy*.

Ochrona pojedynczych hostów

Pojedyncze stanowiska komputerowe można chronić na wiele sposobów. Jednym z nich jest oczywiście *firewall* w postaci programu, często zintegrowany z ochroną antywirusową i anty*spyware*'ową. Prostym sposobem zapobiegania kradzieży wrażliwych danych lub uzyskania nieautoryzowanego dostępu do systemu operacyjnego przez intruza lub nieuczciwego pracownika jest uniemożliwienie korzystania z napędów wymiennych (stacji dysków, odtwarzaczy i nagrywarek płyt oraz pamięci *flash*) poprzez zablokowanie takiej możliwości na poziomie SO lub BIOS bądź przez zwyczajne wyjęcie napędu z obudowy.

Śledzenie zdarzeń

Śledzenie i rejestrowanie zdarzeń zachodzących w systemie informatycznym są jednymi z najważniejszych zadań administracyjnych. Analiza dzienników systemowych (logów) pozwala na wychwycenie prób naruszenia bezpieczeństwa, daje informację o częstotliwości i powtarzalności tych prób, umożliwia stwierdzenie, czy próby te są przypadkowe i niezamierzone czy podejmowane z premedytacją i wymierzone w konkretny punkt systemu. Zapisy w logach pozwalają również na ustalenie źródeł ewentualnych ataków i prób naruszenia bezpieczeństwa. Niekiedy można na ich podstawie stwierdzić, jakich narzędzi używa intruz.

W skrajnych przypadkach mogą stać się ważnym dowodem prawnym przeciwko napastnikowi.

Wykrywanie ataków sieciowych

Systemy wykrywania włamań (*Intrusion Detection Systems, IDS*) mają na celu wykrycie włamania lub innego naruszenia bezpieczeństwa i zebranie śladów tego zdarzenia do dalszej analizy lub jako dowód dla organów ścigania. Występują jako rozwiązania sieciowe (*Network IDS, NIDS*), składające się z czujników wykrywających zdarzenia, silnika zbierającego dane z czujników i generującego alarmy oraz konsoli administracyjnej wyświetlającej dane z czujników i alarmy bądź jako rozwiązania hostowe (*Host IDS, HIDS*), zabezpieczające pojedyncze systemy.

Wykrywanie ataków sieciowych – c.d.

Systemy wykrywania włamań bazują na dwóch podstawowych metodach:

Wykrywanie w oparciu o sygnatury IDS sprawdza, czy ruch w sieci lub dostęp do systemu da się przypisać do znanych, ściśle określonych wzorców (sygnatur) będących oznakami ataku. Sygnaturą mogą być np. powtarzające się nieudane próby logowania.

Wykrywanie anomalii IDS sprawdza, czy sieć lub system informatyczny zachowuje się normalnie (trzeba zdefiniować „normalne zachowanie”!), np. czy poziom ruchu sieciowego nie wzrasta zbyt gwałtownie i bez uzasadnienia.

Plusy i minusy systemów IDS

Zalety

- wykrywanie ataków mających źródło poza siecią lokalną (*NIDS*) oraz wewnątrz LAN (*HIDS*)
- dobra skalowalność (szczególnie w przypadku *NIDS*)
- zarządzanie z centralnej konsoli
- mogą koegzystować z *firewallami* i pracować transparentnie
- mogą analizować dane na bieżąco i wstecz

Wady

- nie powstrzymują ataków, tylko je rejestrują
- mogą generować fałszywe trafienia (*false positives*) i usypiać czujność lub pomijać pewne typy ataków
- muszą być stale dostrajane (uzupełnianie sygnatur ataków)
- w szybkich i rozległych sieciach mogą powodować opóźnienia

Zapobieganie atakom sieciowym

Systemy wykrywania włamań są z definicji **pasywne** – pomagają w stwierdzeniu samego faktu włamania, ale nie potrafią zapobiegać atakom w trakcie ich trwania.

Tę niedogodność usuwają **systemy zapobiegania włamaniom** (*Intrusion Prevention Systems, IPS*) – są rozwiązaniami **aktywnymi**, dynamicznie reagującymi na naruszenia bezpieczeństwa. Sieciowy *IPS* to w praktyce *NIDS* z analizą ruchu *inline* (tzn. bezpośrednio na łączu sieciowym) i możliwością dynamicznego podejmowania określonych działań w odpowiedzi na wykryty atak (np. modyfikacja danych w warstwie aplikacji lub zmiana reguł list dostępu). Hostowy *IPS* to *HIDS* sprzężony z *firewallem* aplikacyjnym (*proxy*). *IPS* potrafią działać na poziomie aplikacji (warstwa 7 modelu OSI), czyli analizować protokoły przeznaczone dla konkretnych aplikacji (np. HTTP, SMTP, FTP).

Miejsce IPS w systemie

System zapobiegania włamaniom działający w trybie *inline* można umieścić na routerze lub moście sieciowym (tryb*inline*) lub na konkretnym hoście. Rozwiązanie sieciowe ma tę zaletę, że analizuje ruch przeznaczony dla wszystkich hostów jednocześnie, dzięki czemu oszczędza się zasoby indywidualnych maszyn. *NIPS* mają jednak trudności z obsługą ruchu szyfrowanego, gdyż na deszyfrowanie zużywane jest sporo zasobów. Analiza ruchu szyfrowanego to zadanie dla *HIPS*.

Wadą *NIPS* jest to, że awaria systemu wpiętego *inline* pociąga za sobą brak ochrony całej sieci. Niewątpliwą zaletą *NIPS* jest natomiast scentralizowane zarządzanie.

Pułapki na intruzów

Oprócz wykrywania włamań i zapobieganiu im nie jesteśmy ograniczeni tylko do bycia ofiarą. Stosunkowo łatwo możemy zamienić się rolami z napastnikiem. Podglądanie jego działań i wysiłków oraz analiza używanych technik i narzędzi daje nam pojęcie o poziomie umiejętności intruza, a często informuje o jego zamiarach (zabawa, chęć sprawdzenia się, próba kradzieży danych, próba przejęcia sieci...). Zwabienie włamywacza w pułapkę daje nam również cenny czas na ewentualne wprowadzenie dodatkowych zabezpieczeń na poziomie sieci lub pojedynczych hostów.

Rozwiązania mające na celu zwabienie potencjalnego intruza w pułapkę określa się nazwą **honeypot** (garnek miodu) lub po prostu **przynętą**.

Rodzaje przynęt

Honeypoty można podzielić na dwie grupy w zależności od zastosowania:

Produkcyjne
Mają odciągnąć uwagę intruza od ważnych zasobów poprzez sprawianie wrażenia bycia istotnym punktem w strukturze sieci (np. dzięki nadaniu odpowiednio „poważnej" nazwy). Ich celem jest obniżenie ryzyka ataku na kluczowe cele. Mogą służyć również do zbierania dowodów włamania.

Badawcze
Ich zadaniem jest zbieranie jak największej ilości informacji o technikach i narzędziach stosowanych przez różne grupy intruzów. Dzięki analizie tych danych badacze mogą odpowiednio dostosowywać narzędzia obrony implementowane w systemach produkcyjnych.

Umiejscowienie przynęty

Honeypot można umieścić w różnych miejsach sieci: na styku LAN z niezaufaną siecią (Internetem lub DMZ), przed siecią lokalną lub wewnątrz niej. Można również zastosować kilka przynęt rozstawionych w różnych miejscach. Każde z powyższych ustawień ma określone konsekwencje i pozwala na zebranie odmiennych danych na temat ataku i napastnika.

Honeypot można ustawić w tej samej podsieci, w której istnieją maszyny produkcyjne bądź wydzielić osobną podsieć, symylując istnienie w niej wielu hostów udostępniających rozmaite usługi. Im dokładniej przynęta potrafi symulować sieć i działające w niej serwery oraz usługi, tym mniejsza szansa, że intruz zorientuje się, iż został wpuszczony w przysłowiowe maliny...

Kryptografia

Często chcemy ukryć pewne informacje, by nie zostały odczytane przez osoby postronne. Z pomocą przychodzi nam **kryptografia**. W największym uproszczeniu mianem kryptografii określamy techniki zapisu informacji w sposób niejawny, czyli **zaszyfrowany**. Założenie kryptografii (z greckiego *ukryte pismo*) jest zatem takie, że nikt nie powinien mieć dostępu do ukrytej informacji, jeśli nie ma wiedzy o metodzie, jakiej użyto dla uczynienia tej informacji nieczytelną. Kryptografia służy również do zapewnienia autentyczności przekazu informacji.

W obecnych czasach termin *kryptografia* lub równoważne mu pojęcie *szyfrowanie* jest używany praktycznie tylko w odniesieniu do komputerów i sieci komputerowych. Kryptografia opiera się na tzw. *kluczach*, czyli informacjach niezbędnych do zaszyfrowania, odszyfrowania, podpisania, sprawdzenia poprawności podpisu pewnej porcji danych.

Kryptografia – c.d.

Dwa główne powody, dla których stosuje się techniki kryptograficzne, to:

- **chęć zapewnienia poufności** — zawężenie kręgu **odbiorców** komunikatu lub danych do zaufanych osób lub określonych aplikacji, będących w posiadaniu klucza. W tym znaczeniu szyfrowanie jest komplementarne do uwierzytelniania
- **potwierdzenie autentyczności** — zawężenie kręgu potencjalnych **nadawców** komunikatu lub danych do zaufanych osób dysponujących kluczem (główne zastosowanie: podpisy cyfrowe)

Do tych cech można jeszcze dodać **integralność**, czyli zapewnienie, że informacja lub dane nie uległy zmianie w czasie przesyłania.

Integralność nie jest tożsama z potwierdzeniem autentyczności nadawcy informacji!

Kryptografia – kilka pojęć

- **Szyfrowanie** — zastosowanie pewnego *algorytmu kryptograficznego* do ukrycia przekazu
- **Odszyfrowywanie** — zastosowanie algorytmu kryptograficznego do odczytania zaszyfrowanego przekazu
- **Wiadomość jawna** — informacja przed poddaniem jej procesowi szyfrowania; inaczej: tekst otwarty
- **Kryptogram** — informacja w postaci zaszyfrowanej; inaczej: tekst zaszyfrowany

Skuteczność kryptografii

Skuteczność kryptografii zależy od zastosowanego algorytmu kryptograficznego, długości klucza szyfrującego i czasu potrzebnego na złamanie tego klucza. Nie powinno być możliwe odgadnięcie klucza bezpośrednio z zaszyfrowanej wiadomości. W żadnym wypadku algorytm używany do szyfrowania i deszyfrowania informacji nie powinien być tajny, tzn. mieć zamkniętej specyfikacji, gdyż stwarza to ryzyko nadużyć.

W obecnych czasach termin *kryptografia* lub równoważne mu pojęcie *szyfrowanie* jest używany praktycznie tylko w odniesieniu do komputerów i sieci komputerowych. Kryptografia opiera się na tzw. *kluczach*, czyli informacjach niezbędnych do zaszyfrowania, odszyfrowania, podpisania, sprawdzenia poprawności podpisu pewnej porcji danych.

Sposoby szyfrowania

Istnieją dwie podstawowe gałęzie szyfrów:

- **symetryczne** — istnieje tylko jeden klucz, używany zarówno do szyfrowania, jak i odszyfrowywania informacji
  Przykłady algorytmów: DES, 3DES, AES, Blowfish, IDEA
- **asymetryczne** — istnieje para kluczy (prywatny i publiczny), z których jeden jest używany do szyfrowania informacji, a drugi do jej odszyfrowania.
  Przykłady algorytmów: RSA, DSA, ECIES, ECDSA

Szyfry symetryczne

Te rodzaje szyfrów można używać wyłącznie do zapewniania poufności, czyli do „klasycznego” szyfrowania. Przy stosowaniu kluczy symetrycznych nie da się oddzielić poufności od autentyczności. Szyfry symetryczne są szybkie w sensie obliczeniowym.

Szyfry asymetryczne

Stosowane od lat siedemdziesiątych XX wieku. Można oddzielić poufność od autentyczności dzięki stosowaniu pary kluczy: prywatnego oraz publicznego. Zasada jest następująca: jeśli jednym z kluczy zaszyfrowano lub podpisano wiadomość, to tylko drugim można dokonać operacji odwrotnej.

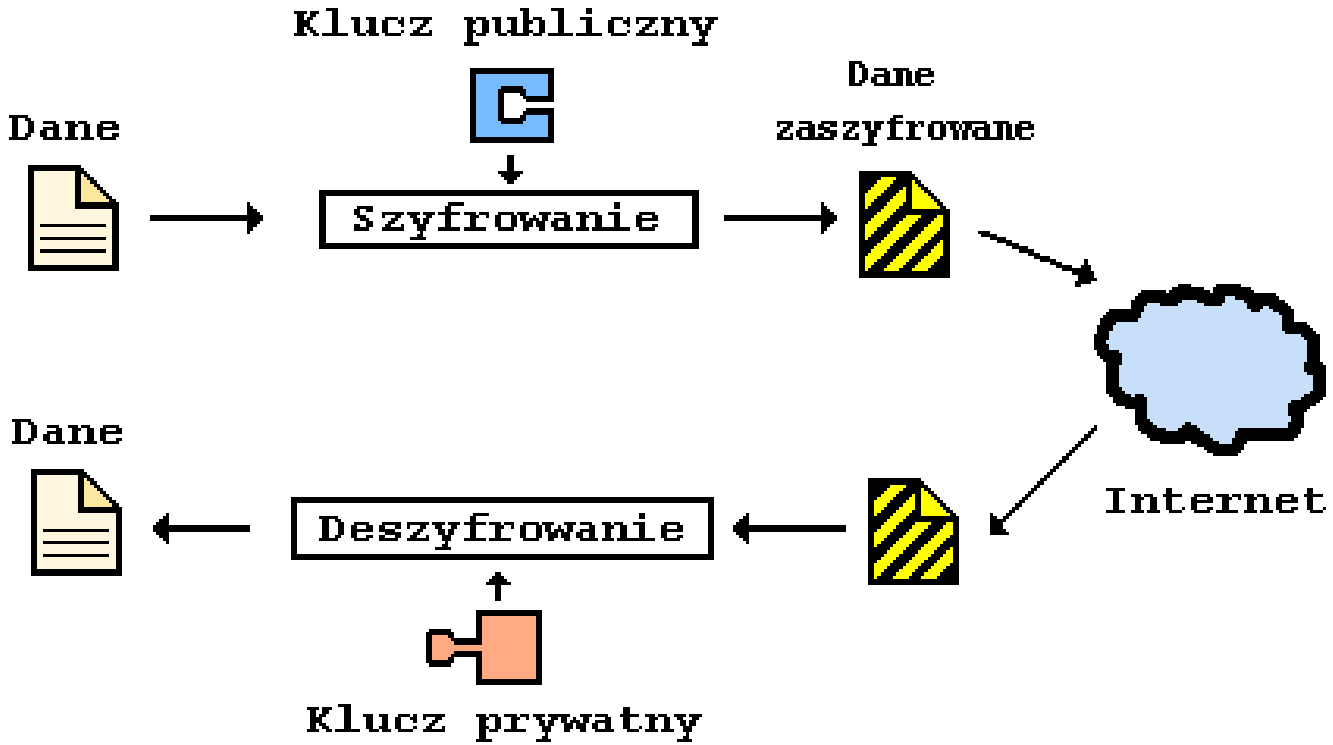
Klucz publiczny można stosunkowo łatwo wyznaczyć z klucza prywatnego, ale przeprowadzenie odwrotnego procesu w odpowiednio krótkim czasie i przy rozsądnym nakładzie środków powinno być – przy dobrym algorytmie – bardzo trudne. Klucz prywatny powinien być chroniony i znany wyłącznie jego właścicielowi, natomiast klucz publiczny może być dowolnie rozpowszechniany (również niezaufanymi kanałami informacyjnymi, takimi jak Internet) i udzielany wszystkim zainteresowanym.

Szyfry asymetryczne są wolniejsze w sensie obliczeniowym od szyfrów symetrycznych.

Szyfry asymetryczne w praktyce

Ze względu na „powolność” kluczy asymetrycznych, szczególnie do szyfrowania dużych ilości danych, stosuje się następujące podejście: dane szyfruje się „szybkim” algorytmem symetrycznym z wykorzystaniem losowego klucza, a następnie ten losowy klucz szyfruje się „wolnym” szyfrem asymetrycznym. Adresat wiadomości najpierw używa klucza z pary kluczy asymetrycznych (prywatnego lub publicznego) do odzyskania klucza symetrycznego, a później tego właśnie symetrycznego klucza używa do rozszyfrowania właściwych danych.

Zasada działania szyfru asymetrycznego



Źródło: Wikipedia

Poufność i autentyczność

Poufność
Informacja jest zaszyfrowana pewnym kluczem publicznym. Dla jednego klucza publicznego istnieje tylko jeden odpowiadający mu klucz prywatny, dlatego też tylko posiadacz odpowiedniego klucza prywatnego będzie mógł odszyfrować wiadomość.

Autentyczność
Nadawca szyfruje wiadomość swoim kluczem prywatnym i przesyła ją osobie, która posiada klucz publiczny nadawcy. Skoro wiadomo, że tylko posiadacz odpowiedniego klucza prywatnego był w stanie wygenerować taki kryptogram, który da się odszyfrować pasującym do tego klucza prywatnego kluczem publicznym, można przyjąć, że wiadomość pochodzi od konkretnego zaufanego nadawcy.

Funkcja skrótu

Inaczej nazywana *funkcją haszującą*, *funkcją mieszającą* lub *haszem* (z ang. *hash*). Pozwala z informacji o dowolnej długości utworzyć skrót (zwany również streszczeniem, *digest*) w postaci ciągu znaków o stałej długości i unikalnej wartości.

Dobra funkcja skrótu powinna charakteryzować się trzema własnościami:

- pozwalać na szybkie i efektywne obliczenie wartości skrótu dla dowolnej informacji
- uniemożliwiać lub co najmniej znacznie utrudniać próbę wygenerowania identycznego skrótu dla dwóch różnych informacji
- uniemożliwiać wnioskowanie co do zawartości wiadomości, dla której znany jest skrót. W praktyce znaczy to, że zmiana wiadomości wejściowej powinna drastycznie zmieniać skrót tej wiadomości

Najpopularniejsze funkcje skrótu to MD5, SHA-1, RIPEMD-160, NTLM.

Podpis cyfrowy

Służy do dodatkowego potwierdzenia autentyczności pochodzenia i/lub integralności wiadomości lub pliku.

W praktyce procedura opatrywania informacji podpisem cyfrowym wygląda następująco: autor informacji wylicza skrót wiadomości i szyfruje ów skrót swoim kluczem prywatnym. Potencjalny odbiorca wiadomości odszyfrowuje skrót kluczem publicznym autora informacji, samodzielnie wylicza skrót wiadomości i porównuje go z uprzednio odszyfrowanym skrótem. Jeśli wyniki są identyczne, można uznać, że wiadomość jest autentyczna i nie uległa zmianie podczas przesyłania.

Do podpisywania cyfrowego stosuje się najczęściej algorytmy RSA, ElGamal i DSA.

Weryfikacja kluczy

Z używaniem kluczy prywatnych i publicznych wiąże się problem potwierdzenia ich autentyczności – nie chcemy bowiem sytuacji, że potencjalny napastnik podstawi własny klucz publiczny jako oryginalny klucz publiczny osoby lub instytucji. Innymi słowy: chcemy przekonać się, czy posiadany przez nas klucz publiczny nadawcy jest wygenerowany na podstawie klucza prywatnego będącego w jego posiadaniu.

W celu weryfikacji kluczy stosuje się dwa rozwiązania: odcisk palca (*fingerprint*) klucza publicznego lub certyfikaty wydawane przez godne zaufania instytucje certyfikacyjne.

Najważniejsze zastosowania kryptografii

- zapewnienie poufności i integralności danych na nośnikach magnetycznych i optycznych
- ochrona informacji przesyłanych przez niezaufane sieci i media transmisyjne
  - ochrona prywatności korespondencji elektronicznej (PGP)
  - ochrona dostępu do zdalnych systemów informatycznych (SSH)
  - ochrona transakcji *on-line*: zakupów, płatności, przelewów itp. (SSL)
- poświadczanie tożsamości osób oraz autentyczności i integralności dokumentów (podpis cyfrowy)
- poświadczanie certyfikatów cyfrowych

Przydatne adresy

- http://www.securityfocus.com
- http://www.cert.org, http://www.cert.pl i http://arakis.cert.pl
- http://www.networkintrusion.co.uk
- http://www.sans.org i http://www.incidents.org
- http://www.onlamp.com/security
- http://www.packetstormsecurity.org
- http://www.windowsecurity.com
- http://www.treachery.net
- http://www.neohapsis.com
- http://www.narf.shl.pl
- http://www.hack.pl
- http://www.hacking.pl
- http://www.ipsec.pl
- http://www.hakin9.org