BIULETYN INSTYTUTU AUTOMATYKI I ROBOTYKI
NR 26, 2009

Ponad barierami - łączenie sieci o różnych klauzulach[1]

Marek BRUDKA, Janusz FURTAK

Filbico Sp. z o.o., ul. Wyszyńskiego 7, 05-220 Zielonka,
Instytut Teleinformatyki i Automatyki WAT, ul. Gen. S. Kaliskiego 2, 00-908 Warszawa

STRESZCZENIE: Opracowanie jest zwięzłym przeglądem możliwych sposobów wymiany danych pomiędzy sieciami o różnych poziomach ochrony poufności. Określono potrzeby i zagrożenia związane z łączeniem sieci chronionych, a także wskazano obszary aktywności badawczych i standaryzacyjnych z tym zakresie. Opisano podstawowe komponenty bezpieczeństwa styków systemów teleinformatycznych i sposób ich wykorzystania przy tworzeniu bram międzysystemowych. W podsumowaniu wymieniono kilka bram międzysystemowych oraz wskazano istotne dla osiągania zdolności sieciocentrycznych przez SZ RP kierunki rozwoju rozwiązań typu CDS.

SŁOWA KLUCZOWE: bramy międzysystemowe, bezpieczeństwo wielopoziomowe, dioda danych

1. Wprowadzenie

Podstawy do tworzenia bezpiecznych systemów teleinformatycznych, a w szczególności obowiązkowe mechanizmy kontroli dostępu bazujące na modelach Bella-La Paduli (BLP), Clarka-Wilsona, czy Biby [2], [5], [6] powstały kilkadziesiąt lat temu, gdy komputer nie był urządzeniem powszechnie używanym, a dzisiejsza globalna sieć informacyjna pojawiała się głównie w śmiałych futurystycznych wizjach. Modele te wpłynęły na regulacje prawne i standardy doprowadzając do utworzenia rekomendacji i wymogów np. TCSEC (Trusted Computer System Evaluation Criteria), czy Common Criteria, umożliwiając tworzenie i ocenę bezpiecznych systemów teleinformatycznych, w tym systemów wielopoziomowych MLS (ang. Multilevel Security) [16].

[1] Zagadnienia poruszane w opracowaniu były prezentowane na konferencji CYBERSPACE 2009, która odbyła się w Warszawie w dniu 15.10.2009

Dyskusje dotyczące wagi i znaczenia tych rozwiązań toczone są na forach eksperckich od lat i prowadzą do powstania nowych modeli oraz rozwiązań technicznych i organizacyjnych w dziedzinie ochrony. Zapewniają one dobrą bazę do zabezpieczenia poufności i integralności przetwarzanych danych stwarzając nawet możliwości formalnego dowodzenia poprawności projektowania i testowania. Z drugiej strony rozwój, a następnie akredytacja lub certyfikacja urządzeń i systemów tego typu jest trudna technicznie, kosztowna i czasochłonna [19]. W konsekwencji ceny urządzeń są wysokie, a oferta rynkowa jest spóźniona względem potrzeb.

Potrzeby użytkowników w kontekście rozwoju zdolności sieciocentrycznych (ang. *Network Enabled Capabilities*) sił zbrojnych [1] wynikają z porównania możliwości obecnych systemów militarnych z możliwościami systemów dostępnych w sieci Internet. Technicznie część z tych potrzeb mogłaby zostać prawie natychmiast zastosowana, jednak oczywista konieczność zapewnienia ustawowej ochrony informacji [22], [24] oraz względy proceduralno-formalne prowadzą do swoistej cyberdeprywacji (ang. *cyber deprivation*). Zasadniczym powodem tego stanu rzeczy wydaje się być separacja sieci o niekompatybilnych poziomach ochrony skutkująca zablokowaniem szeregu kanałów wymiany danych [9]. Nie jest trudno się zgodzić ze spostrzeżeniem [7], że tzw. *air gap* daje poczucie poprawy ochrony poufności kosztem utraty możliwości wymiany informacji.

Sytuacja ta w obliczu narastającego znaczenia wojny informacyjnej, gwałtownego rozwoju cyberprzestępczości i cyberterroryzmu wymaga zdecydowanych działań. Blokady wszystkich kanałów danych szczególnie istotnie wpływają na współpracę systemów automatycznie wymieniających dane, w tym systemów automatyzacji dowodzenia – znany jest tzw. „*sensor-shooter problem*" [17]. Konieczność wymiany informacji pomiędzy systemami wymusza ewolucję ich architektur w kierunku stref bezpieczeństwa o różnych poziomach ochrony stykających się za pośrednictwem bram międzysystemowych [21]. O wadze zasygnalizowanego problemu niech świadczy fakt, że zagadnienia z nim związane były tematem wiodącym szeregu prób, eksperymentów i ćwiczeń interoperacyjności sił zbrojnych np. CWID[2] i JWID[3] [14], [18]. W szczególności, dla opracowania wytycznych w zakresie bezpieczeństwa systemów tworzonych w oparciu o metodykę SOA (ang. *Service Oriented Architecture*), powołano grupę roboczą NATO/RTO IST-061 [23], w której aktywną rolę odegrały polskie podmioty [15].

Współczesne opracowania związane z łączeniem systemów o różnych klauzulach są odzwierciedleniem pewnego trendu w rozumieniu zabezpieczeń

[2] CWID - Coalition Warrior Interoperability Demonstrations
[3] JWID - Joint Warrior Interoperability Demonstration

teleinformatycznych, a mianowicie silniejszego akcentowania znaczenia zarządzania ryzykiem w systemach połączonych w stosunku do wymogu całkowitej eliminacji ryzyka w sieciach izolowanych. Prowadzi to do ustalania innego kompromisu polegającego na zwiększeniu dostępu do danych kosztem zwiększenia ryzyka utraty ich poufności i integralności. Jest to podejście praktyczne, które wprawdzie nie stoi w sprzeczności z uznanymi modelami kontroli dostępu i zabezpieczenia systemów teleinformatycznych, ale też nie jest przez nie mocno wspierane [16].

Metody łączenia systemów o różnych poziomach ochrony określone zostały łącznie, jako CDS (ang. *Cross Domain Solutions*) i są intensywnie rozwijane w krajach NATO. Na przykład w 2006 roku w Stanach Zjednoczonych powołano biuro UCDMO (ang. *Unified Cross Domain Management Office*) odpowiedzialne za scentralizowaną koordynację i nadzorowanie wszystkich inicjatyw związanych z wymianą informacji pomiędzy chronionymi systemami teleinformatycznymi ministerstwa obrony, służb wywiadu, ministerstwa sprawiedliwości i innych instytucji rządowych.

Warto w tym miejscu odróżnić CDS od tworzenia połączeń przez strefy o niższym poziomie ochrony. Typowym przykładem przypadku drugiego jest połączenie chronionego terminala zdalnego z serwerem systemu dowodzenia za pośrednictwem sieci niechronionej. Do właściwego, z punktu widzenia obowiązujących wytycznych i standardów, zabezpieczenia takiej konfiguracji [11], [13], [22], [24] należy wykorzystać ochronę kryptograficzną, np. w postaci szyfratora lub routera obsługującego sieci VPN. Jeśli jednak do serwera systemu dowodzenia (przetwarzającego dane poufne) należy doprowadzić położenie pojedynczych jednostek odczytywane z GPS, które są danymi niżej klasyfikowanymi, to musi nastąpić komunikacja pomiędzy systemami o różnym poziomie ochrony, a zatem właściwe jest stosowanie rozwiązań typu CDS.

Rozwiązania CDS dostarczają funkcji, które można ująć w następujących grupach [4]:

- dostarczanie danych (ang. *push data*) - dostarczanie danych np. do repozytoriów, baz danych, importowanie i eksportowanie, strumienie danych;
- współpraca (ang. *collaboration*) za pomocą poczty elektronicznej, komunikatorów, konferencji audio i video, czy współdzielonych miejsc pracy;
- scentralizowane zarządzanie IT (ang. *centralized IT management*) obejmujące m.in. scentralizowane usługi np. DNS, DHCP, LDAP, scentralizowanie zabezpieczanie i odtwarzanie danych, scentralizowany audyt, zdalna administracja systemami IT i CDS;
- inspekcja zawartości i sposobu rozpowszechniania (ang. *content inspection and release*) polegająca na sprawdzeniu zawartości w celu

wykrycia złośliwego oprogramowania, identyfikacji ukrytej treści, kontroli dostępu bazującą na atrybutach, wymuszeniu przestrzegania reguł bezpieczeństwa, czy proceduralnej kontroli danych przez operatora;

- zdalnie dostępne scentralizowane repozytoria i inne zasoby (ang. *remote access centralized repository and other*) pozwalające na dzielenie aplikacji, dostęp do baz MLS, czy redukcję liczby stacji roboczych i sieci np. za pomocą maszyn wirtualnych.

W dalszej części opracowania przedstawione zostaną niektóre z gotowych komponentów bezpieczeństwa wykorzystywane do budowy rozwiązań CDS. Część z nich posiada certyfikaty potwierdzające spełnienie wymagań określonego poziomu EAL lub stosowne akredytacje. Należy jednak podkreślić, że z faktu wykorzystania w specyficznej konstrukcji certyfikowanych urządzeń nie wynika akredytacja całości rozwiązania. Zabezpieczenie połączenia wymaga stosowania wielu komplementarnych i redundantnych komponentów współpracujących w kierunku ochrony pożądanych, specyficznych i ściśle zdefiniowanych w dokumentacji bezpieczeństwa funkcji i danych.

2. Komponenty do ochrony systemów

Przy opisie zabezpieczeń wykorzystany zostanie model BLP [5], w którym informację D i system S opisuje się klauzulami SL w postaci par < *klasyfikacja K, zakres Z* >. Klasyfikacja K o wartościach ze zbioru uporządkowanego {*jawne, zastrzeżone, poufne, tajne, ściśle tajne*} wykorzystywana jest do określenia wymaganego poziomu ochrony informacji D, a w odniesieniu do systemu S oznacza minimalny, zapewniony przez system S poziom ochrony przetwarzanych w nim informacji. Zakres Z opisuje zbiór kategorii, do których należy informacja D lub zbiór kategorii informacji przetwarzanych przez system S. W zbiorze klauzul określona jest częściowo porządkująca relacja dominacji LLS ≤ HLS pomiędzy klauzulą wyższą HLS, a klauzulą niższą LLS. Relacja ta jest spełniona wtedy, gdy K(LLS) ≤ K(HSL) i Z(HSL) ⊇ Z(LLS). Przykładem klauzuli LLS dla systemu przetwarzającego dane jawne i wykorzystującego Internet może być < *jawne, imię i nazwisko* >, a przykładem klauzuli HSL niech będzie < *zastrzeżone, dane osobowe* > dla informacji zastrzeżonych z zakresu danych osobowych. Z kolei w dziedzinie militarnej, przykładem LLS może być < *tajne, dane mobilizacyjne* > i HLS - < *tajne, wyposażenie w sprzęt* >. System LLS nazywany będzie również systemem z niższym poziomem ochrony albo krótko niższym, natomiast HLS systemem z wyższym poziomem ochrony albo wyższym.

Warto w tym miejscu zwrócić uwagę na praktyczne znaczenie zakresu przetwarzanych danych w relacji dominacji. Otóż możliwa jest sytuacja, w której jeden z dwóch systemów akredytowanych do przetwarzania informacji opisanych tą samą klasyfikacją jest systemem wyższym, a drugi niższym z uwagi na szerszy zakres informacji przetwarzanych przez HLS. Przykładem takiej sytuacji może być baza położenia wojsk własnych HLS opisana klauzulą < *poufne, baza położeń* > oraz elementy systemu kierowania walką zainstalowane w wozie bojowym opisane klauzulą < *poufne, położenie wozu* >. Innym interesującym przypadkiem jest brak relacji dominacji pomiędzy systemem < *tajne, wyposażenie w sprzęt* >, a < *zastrzeżone, dane osobowe* > z uwagi na rozłączność zakresów przetwarzanych informacji. W obydwu wymienionych przypadkach połączenie pomiędzy systemami wymaga rozważenia stosowania rozwiązań CDS.

2.1. Środki defensywne

Do grupy środków defensywnych należy zaliczyć wszystkie komponenty w postaci aktywnych, bądź pasywnych urządzeń sieciowych, które ukierunkowane są na zapobieganie atakom intruzów lub złośliwego oprogramowania na system chroniony. Bezpośrednim przeznaczeniem tych rozwiązań nie jest zabezpieczanie poufności informacji, niemniej pośrednio, z uwagi na możliwość ścisłego zdefiniowania i kontroli przepływów informacji, pozwalają one zmniejszyć ryzyko ujawnienia danych chronionych. Do najważniejszych środków z tej grupy należy zaliczyć routery, zapory sieciowe (ang. *firewall*), serwery pośredniczące (ang. *proxy*), systemy zapobiegania włamaniom IPS (ang. *Intrusion Prevention System*), przy czym bogactwo dostępnych urządzeń łączących w sobie różne funkcje istotnie utrudnia właściwą ich klasyfikację.

Najpopularniejszym środkiem ochrony styków międzysystemowych są zapory filtrujące (ang. *packet filter*) odpowiadające za blokowanie wszelkiego niepożądanego ruchu sieciowego na poziomie sieciowym i transportowym według modelu ISO/OSI. Z uwagi na podwyższone wymagania bezpieczeństwa zapory takie często łączone są szeregowo, przy czym zwykle przestrzegana jest zasada "doboru sprzętu od różnych producentów" np. Check Point i Cisco. Redundancja zapór zmniejsza podatności systemu chronionego na ataki wynikające z niewłaściwej konfiguracji i błędów w oprogramowaniu. Często spotykaną, właściwą raczej routerom, choć ważną w kontekście bezpieczeństwa funkcjonalnością zapór, jest translacja adresów sieciowych (ang. *Network Address Translation*) pozwalająca na ukrycie adresów systemu chronionego.

Specyficznym rodzajem zapór są zapory warstwy aplikacyjnej i usługi

(serwisy) pośredniczące operujące na poziomie warstwy aplikacji modelu ISO/OSI. Ich rolą jest nadzorowanie i pośredniczenie w realizacji usług systemu chronionego tak, aby komputery systemu LLS nigdy nie kontaktowały się bezpośrednio z systemem HLS. W ten sposób serwisy chronione pozostają anonimowe, część z ataków zakłóci funkcjonowanie raczej zapory, niż systemu docelowego, a nadzór na transmisją umożliwia detekcję i zapobieganie naruszeniom standardów specyfikacji protokołów komunikacyjnych opisywanych na przykład w dokumentach RFC (ang. *Request for Comment*).

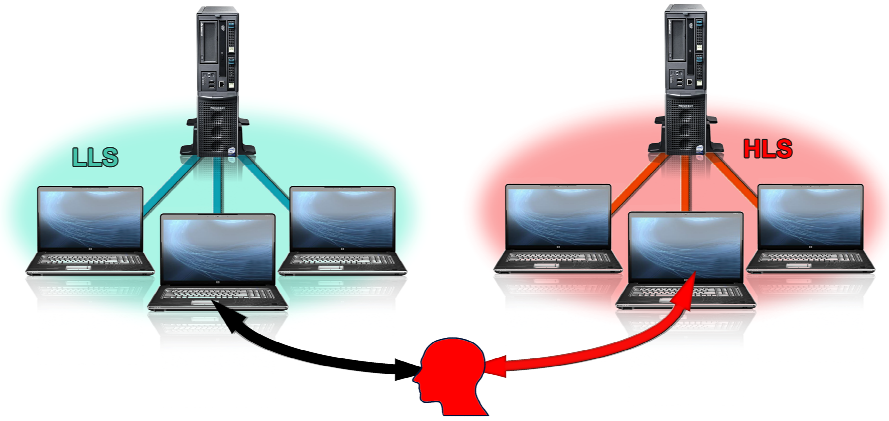
Systemy wykrywania i zapobiegania włamaniom IDS/IPS (ang. *Intrusion Detection/Prevention System*) oferują funkcje podobne do funkcji zapór warstwy aplikacyjnej. Systemy IDS/IPS jednak, w przeciwieństwie do zapór pośredniczących, są całkowicie niewidoczne zarówno z od strony systemu niższego poziomu, jak i chronionego systemu wyższego poziomu. Systemy wykrywania włamań IDS analizują i sygnalizują wykryte incydenty polegające na wystąpieniu w przepływającym przez nie ruchu sieciowym zachowań pasujących do sygnatur charakterystycznych dla prób ataku, np. źle skonstruowane ramki, czy też próby połączeń przez zakazane porty. Systemy IPS dodatkowo zapobiegają włamaniom korygując bądź blokując podejrzany ruch sieciowy.

2.2. Pełna separacja sieci

Podstawowym i powszechnie wykorzystywanym sposobem ochrony poufności systemów niejawnych jest wspomniana już *air gap*, czyli całkowita separacja sieci systemu wyższego poziomu od sieci systemu niższego poziomu (rys. 1). Rozwiązanie to oferuje najwyższy możliwy poziom ochrony przed wypływem informacji chronionych z systemu wyższego do systemu niższego. Jedynym sposobem transferu informacji w takich sieciach, o ile jest to uwzględnione w procedurach bezpiecznej eksploatacji, jest przenoszenie danych za pomocą dyskietek, płyt CD/DVD, pamięci pen-drive, wydruków, czy w wyniku przepisywania danych przez operatora.

Najważniejszym zagrożeniem dla takich sieci jest możliwość wprowadzenia oprogramowania złośliwego, bądź utrata poufności w wyniku pomyłkowego skopiowania danych chronionych. Jeśli jednak do tworzenia systemu wykorzystano rozwiązania MLS z etykietami bezpieczeństwa, to przy właściwej jego konfiguracji ryzyko takiej pomyłki jest minimalne, bowiem nośniki zewnętrzne mogą zostać opisane klauzulą niższą, niż dane podlegające ochronie. Z reguły w odniesieniu do sieci o wyższych klauzulach procedury bezpiecznej eksploatacji oraz konfiguracja sprzętowa wykluczają możliwość wykorzystania jakichkolwiek nośników danych. Odseparowane systemy nie mogą automatycznie wymieniać żadnych informacji, a zatem odgrywają niewielką rolę w infrastrukturze sieciocentrycznej, a jedynym źródłem

i odbiorcą danych jest uprawniony użytkownik.



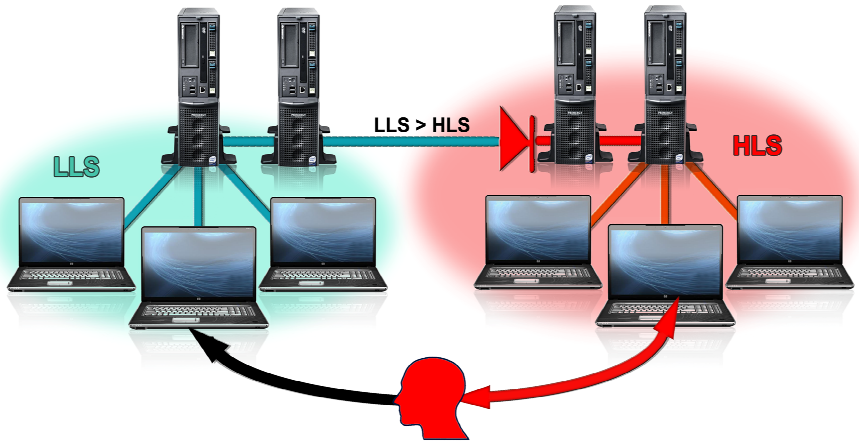
Rys. 1. Sieci odseparowane

2.3. Komunikacja jednokierunkowa

Większe możliwości wymiany pomiędzy systemami (rys. 2) stwarza wykorzystanie jednokierunkowych traktów komunikacyjnych w postaci diody danych (ang. *data diode*). Jednokierunkowość przepływu danych od systemu LLS do HLS zapewniana jest na poziomie warstwy fizycznej przez separator światłowodowy bazujący na karcie Ethernet FX z odłączonym jednym kierunkiem komunikacji. Funkcjonalnie, dioda jest rodzajem zapory filtrującej o sprzętowej regule akceptacji ruchu sieciowego tylko w jednym kierunku. Diody danych oferowane są na świecie przez kilku producentów m.in. Tenix (obecnie BAE Systems), NC3 Agency [20], OWL Inc., a w Polsce przez Filbico Sp.z o.o. [26].

Wykorzystanie światłowodowych rozwiązań sprzętowych w diodzie prowadzi do wzbogacenia jej w porównaniu z klasyczną zaporą o kombinację unikalnych i krytycznych dla bezpieczeństwa własności. Łącze światłowodowe rozwiązuje problem ulotu elektromagnetycznego praktycznie uniemożliwiając prowadzenie podsłuchu transmisji w miejscu połączenia systemów. W klasycznej, pojedynczej zaporze filtracja ruchu odbywa się zwykle we wnętrzu urządzenia na poziomie oprogramowania, bądź reguł zaimplementowanych w układach scalonych. Rozwiązanie takie prowadzi do trudności w zapewnieniu właściwego ekranowania urządzeń, eliminacji przesłuchów oraz nie separuje systemów galwanicznie. Podział diody na dwie

części: nadawczą i odbiorczą, w sposób przejrzysty określa granicę fizyczną pomiędzy systemem niższym, a chronionym, jako miejsce dołączenia światłowodu do części odbiorczej separatora. Wyznaczenie takiej granicy jest trudne w odniesieniu do pojedynczej zapory pakietowej, a jednocześnie jest niezbędne z uwagi na konieczność ochrony fizycznej HLS i separacji przestrzennej HLS od LLS.



Rys. 2. Komunikacja jednokierunkowa z LLS do HLS

Konstrukcja diody uniemożliwia jakąkolwiek utratę poufności informacji przetwarzanej w HLS np. z powodu niewłaściwej konfiguracji lub też przez tylne drzwi (ang. *backdoor*) utworzone przez złośliwe oprogramowanie, bądź w wyniku działań intruza[4]. System HLS jest "niewidoczny" z poziomu LLS, dlatego też nie jest również możliwa żadna forma skanowania elementów infrastruktury HLS w poszukiwaniu miejsc wrażliwych.

Najważniejszą trudnością techniczną stosowania diod jest brak możliwości automatycznej kontroli transmisji, w szczególności jednokierunkowe transfery datagramowe nie zapewniają wiarygodności przesyłania danych. W praktyce jednak stopa błędów transmisji światłowodowych jest na tyle niska, że nie prowadzi to do zakłócenia pracy systemów, a spowodowane utratą pakietów interwencje administratora styku są rzadkie. Innym istotnym niedostatkiem stosowania diod jest brak możliwości wykorzystywania usług używających protokołu TCP.

[4] Pod warunkiem wyeliminowania możliwości użycia nośników zewnętrznych w systemie HLS

Rozwiązania CDS bazujące na pojedynczej diodzie wraz z dodatkowymi komponentami zabezpieczającymi pozwalają na realizację wszystkich funkcji związanych z transferami danych z systemu LLS do systemu HLS. Do szczególnie interesujących zastosowań można zaliczyć:

- jednokierunkowe transmisje audio i wideo np. z kamer obserwacyjnych,
- pomiary z sieci sensorów np. informacja radiolokacyjna,
- składanie meldunków i zgłaszanie zapotrzebowań np. za pomocą ADatP-3,
- przekazywanie strumieni informacyjnych np. RSS,
- import danych do baz systemu HLS.

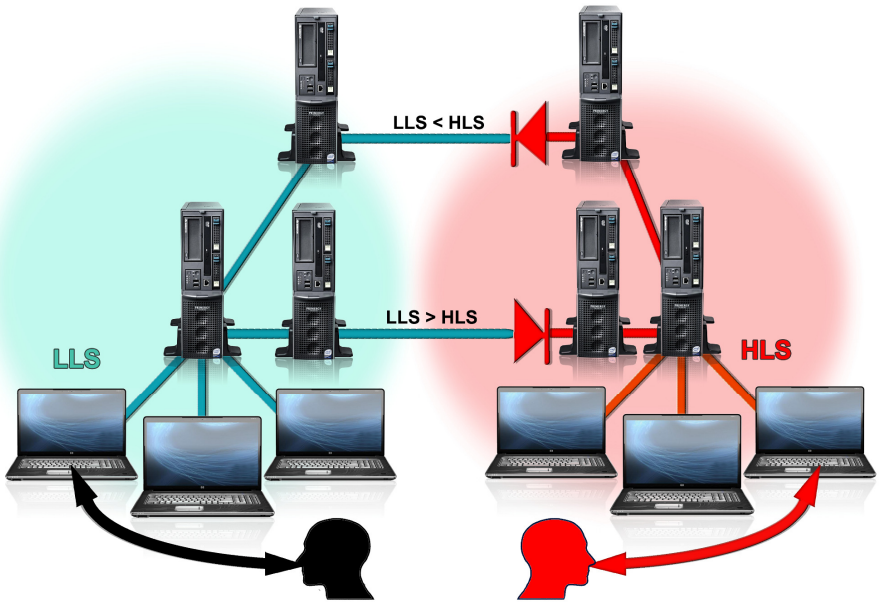
Wprowadzenie danych do HLS prowadzi do pojawienia się typowych zagrożeń dla integralności bądź dostępności systemu chronionego związanych z możliwością infekcji oprogramowaniem złośliwym lub przeprowadzeniem ataku typu DoS (ang. *Denial of Service*). Z powodu tych zagrożeń dioda zwykle łączona jest szeregowo z innymi teleinformatycznymi środkami ochrony takimi jak zapory, skanery zawartości, czy też systemy detekcji i zapobiegania włamaniom.

2.4. Komunikacja za pomocą układu dwóch diod

Wykorzystanie układu dwóch diod (UDD) dla niezależnych traktów komunikacyjnych umożliwia dwukierunkową wymianę informacji pomiędzy LLS i HLS (rys. 3). Funkcjonalnie konfiguracja ta jest równoważna dwóm niezależnym zaporom akceptującym jednokierunkowy ruch datagramowy, ale działającym w przeciwnych kierunkach. UDD posiada wszystkie zalety diody pojedynczej związane z ochroną fizyczną i ochroną przed ulotem elektromagnetycznym. Rozdzielenie traktów komunikacyjnych zmniejsza znaczenie pomyłek administratora oraz istotnie utrudnia utworzenie tylnych drzwi do systemu HLS. UDD nie realizuje protokołów połączeniowych, a zatem mniejsze są możliwości ataków polegających na przejęciu bądź podsłuchaniu sesji. Dodatkowo sprzętowe rozdzielenie kierunków transmisji narzuca twórcom specyficznych systemów korzystających z UDD wymianę informacji w oparciu o komunikaty (ang. *message based*) oraz ścisłe stosowanie się do zasady podziału odpowiedzialności (ang. *separation of concerns*).

Teoretycznym przykładem zastosowania UDD może być połączenie systemu < *jawne, wszystko* > z systemem HLS o klauzuli < *zastrzeżone, dane osobowe* > w celu umożliwienia pobierania za pomocą poczty elektronicznej rekordów pojedynczych osób z bazy danych osobowych (przy założeniu, że pojedyncze dane osobowe są jawne). Zapytanie w postaci sformatowanego listu przekazywane jest przez diodę LLS>HLS (rys. 3) do systemu HLS.

Specjalizowane oprogramowanie po stronie HLS pobiera z bazy danych osobowych wymagany rekord, tworzy list-odpowiedź opisaną klauzulą <*jawne, rekord danych osobowych*> i przez diodę LLS<HLS (rys. 3) przesyła go do pytającego.



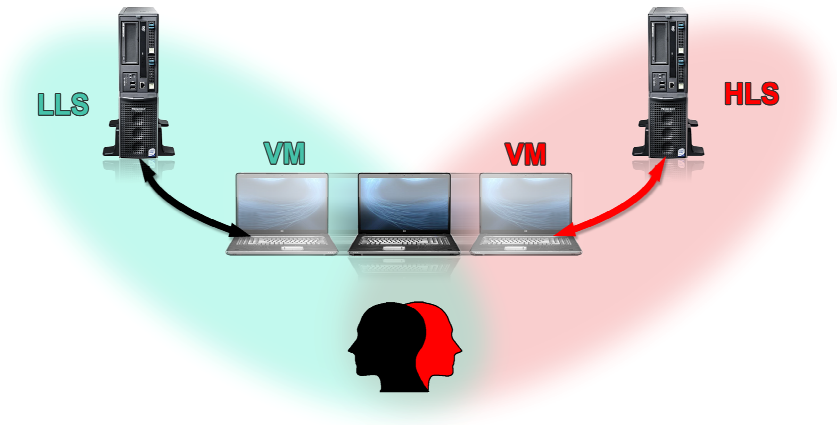
Rys. 3. Komunikacja dwukierunkowa przez układ dwóch diod

Umożliwienie transferu danych z HLS do LLS, bez względu na techniczny sposób jego uzyskania, stwarza możliwość utraty poufności danych przetwarzanych w HLS bezpośrednio, bądź za pośrednictwem kanałów ukrytych (ang. *covert channel*). Prowadzi to do konieczności rozważenia wszystkich typowych zagrożeń dla systemów teleinformatycznych i nadaje szczególne znaczenie analizie ryzyka [12]. Z analizy tej wynikają zalecenia dodatkowych środków ochrony dla połączeń realizowanych za pomocą UDD, np. zalecenie skanowania i przekształcania treści, stosowania deklasyfikatorów danych, czy wreszcie uwzględnienia informacji o etykietach bezpieczeństwa dostarczanych przez systemy klasy MLS. Dodatkowo, brak możliwości korzystania z protokołów połączeniowych (np. TCP) tak, jak to ma miejsce w klasycznych zaporach, utrudnia bezpośrednie wykorzystanie szeregu komponentów typu COTS np. agentów pocztowych (ang. *Mail Transfer Agent*), serwerów WWW czy serwerów SIP (ang. *Session Initiation Protocol*) wymuszając ich modyfikację bądź implementację stosownych usług pośredniczących.

2.5. Maszyny wirtualne

Maszyny wirtualne (VM) ze wsparciem wirtualizacji na poziomie sprzętowym np. VMware, Xen, Virtual PC, Integrity znajdują coraz to inne zastosowania, w tym zastosowania związane z bezpieczeństwem teleinformatycznym. W technologii tej na komputerze serwera VM (ang. *host*) kontrolowanego przez macierzysty system operacyjny uruchamiane są niezależne od siebie wirtualne komputery (ang. *guest*) pracujące pod kontrolną tych samych lub różnych systemów operacyjnych np. MS Windows, Linux, QNX. W trakcie pracy systemu macierzystego i systemów wirtualnych dane poszczególnych systemów z założenia nie wykorzystują wspólnych obszarów ani w pamięci operacyjnej, ani w pamięci zewnętrznej. Cecha ta jest istotna z punktu widzenia ochrony systemów.

Oprogramowanie maszyn wirtualnych może podlegać ocenie zgodnej z Common Critieria np. jądro systemu Integrity uzyskało certyfikat EAL 6+, natomiast VMWare został zbadany na poziomie EAL 4+.



Rys. 4. Łączenie sieci przez maszyny wirtualne

Technologia VM umożliwia zbudowanie konstrukcji, w której macierzysty system operacyjny jest wyposażony w specjalizowane oprogramowanie - zarządcę maszyn wirtualnych, przeznaczone do uruchamiania i obsługi VM przetwarzających dane i pracujących w sieciach o różnych poziomach ochrony. Jeśli sieci LLS i HLS oraz podłączone do nich maszyny wirtualne zapewnią brak wymiany i możliwości podsłuchu informacji (rys. 4), to konfiguracja ta będzie swoistym odpowiednikiem opisanej już pełnej separacji sieci. Zaletą takiego rozwiązania CDS jest zmniejszenie liczby komputerów (ang. *desktop reduction*)

obsługiwanych przez użytkownika wykorzystującego do działań operacyjnych systemy o różnych poziomach ochrony.

Maszyny wirtualne ułatwiają również kształtowanie bezpiecznej infrastruktury sieciowej oferując tworzenie i badanie wirtualnych sieci w obrębie tego samego serwera VM lub za pośrednictwem kompatybilnych routerów. Wirtualny komputer pozwala na wygodne badanie różnych systemów operacyjnych, aplikacji, a nawet oprogramowania złośliwego [8]. Łatwo jest wyeliminować zaśmiecanie rzeczywistych zasobów na dysku i struktur zainstalowanego systemu, a tym samym zmniejszyć ryzyko omyłkowej utraty poufności. Potencjalny intruz zwykle nie ma świadomości, czy ma do czynienia z maszyną rzeczywistą, czy wirtualną, choć istnieje szereg sposobów pozwalających na detekcję VM [8]. Działanie intruza lub oprogramowania złośliwego dotyczyć będzie tylko jednej VM – na maszynie macierzystej zwykle nie uruchamia się żadnych usług z wyjątkiem maszyn wirtualnych. Odseparowanie aplikacji na poszczególnych komputerach wirtualnych zmniejsza ryzyko w przypadku pojawienia się poważnej luki w zabezpieczeniu jednej z aplikacji, co jest szczególnie istotne w przypadku nieznanych sposobów ataku – tzw. *zero day attacks*. Wykorzystanie VM pozwala również na szybkie przywrócenie dostępu do usług zaatakowanego serwera i jednoczesne ułatwia zabezpieczenie wszelkich danych na potrzeby analizy powłamaniowej.

Przykładem rozwiązania wykorzystującego VM może być pochodzący z NSA (ang. *National Security Agency*) system NetTop prezentowany na ćwiczeniach JWID 2004. System uzyskał pozytywną ocenę JWID i SEIWG. Z wykorzystaniem tego systemu była możliwa praca w dwóch sieciach o różnych klauzulach z jednego komputera kontrolowanego przez SE Linux i VMware.

Do niedostatków VM należy zaliczyć:

- wydajność wirtualnego komputera jest niższa niż wydajność komputera-gospodarza z powodu korzystania z emulowanych, a nie rzeczywistych komponentów;
- dużym kłopotem jest poprawne z punktu widzenia bezpieczeństwa skonfigurowanie VM, uaktualnianie oprogramowania takich maszyn i dokonywanie archiwizacji danych przechowywanych w zasobach VM.
- w analizie ryzyka rozwiązań bazujących na VM należy dodatkowo uwzględnić podatności VM na nowe typu ataków [8].

3. Podsumowanie

Przedstawione środki ochrony mogą być wykorzystywane do tworzenia bardziej skomplikowanych bram międzysystemowych przeznaczonych do

transferu danych i współpracy sieciowej. Zdecydowana większość tych bram wymaga dwukierunkowej wymiany informacji, a zatem musi bazować na układzie podwójnej diody lub stosownie skonfigurowanych zaporach. Typowym przykładem mogą tu być bramy pocztowe odpowiadające za wymianę korespondencji elektronicznej pomiędzy użytkownikami i oprogramowaniem systemów zautomatyzowanych.

Konstrukcja rozwiązań zaawansowanych jest zwykle unikalną kompozycją redundantnych zabezpieczeń oraz komponentów typu COTS (ang. *commercial off-the-shelf*) lub OSS (ang. *Open Source Software*). Komponenty te najczęściej wymagają istotnych modyfikacji w celu uwzględnienia szeregu wymogów bezpieczeństwa, m.in. wprowadzenia dodatkowych, specyficznych zabezpieczeń [7], ograniczenia funkcjonalności, przystosowania do transferów jednokierunkowych, czy implementacji audytu, rejestracji i skanowania treści. Przykładowo brama komunikacyjna oferująca usługi natychmiastowej wymiany informacji (ang. *instant messaging*) pomiędzy komunikatorami internetowymi może bazować na jednym z wielu serwerów protokołów XMPP (ang. *Extensible Messaging and Presence Protocol*). Funkcje takiego serwera muszą jednak zostać ograniczone wyłącznie do wymiany wiadomości tekstowych, informacje o użytkownikach powinny zostać ukryte za pomocą readresacji, przesyłane treści powinny być skanowane i rejestrowane, a w warstwie transportowej należy wykorzystać komunikację datagramową.

Szczególnie interesujące kierunki rozwoju bram międzysystemowych związane są z tworzeniem zdolności sieciocentrycznych, a w szczególności z łączeniem systemów o architekturach zorientowanych na usługi (SOA). Idea systemów usługowo kooperujących w globalnej sieci [1] wnosi nową jakość w pojmowaniu znaczenia wymiany informacji, ale jednocześnie stwarza zupełnie nowe problemy w zapewnieniu bezpieczeństwa teleinformatycznego. Ostatnie eksperymenty i demonstracje w obrębie NATO [14], [15], [23] wskazują, że możliwe i pożądane jest wykoRzystanie szeregu standardów cywilnych proponowanych m.in. przez W3C i OASIS np. etykiet bezpieczeństwa XML (ang. XML Security Labelling), infrastruktury klucza publicznego (ang. Public Key Infrastructure), rejestrów usług UDDI, czy usług katalogowych LDAP do bezpiecznego łączenia systemów wojskowych, w tym systemów typu MLS. Zagadnieniem otwartym i niełatwym jest jednak opracowanie bram dla usług webowych WS (ang. Web Services) w postaci gotowych i certyfikowanych komponentów COTS. Obszar zastosowań takich urządzeń z uwagi na ogólność koncepcji WS jest szeroki, a przejrzyste rozdzielenie funkcji bram WS np. deklasyfikacji od filtracji treści, powinno zdynamizować integrację i akredytację systemów SZ RP.

Literatura

[1] ALBERTS D.S., GARSTKA J.J., STEIN F.P., *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd edition, Aug 1999, CCRP, http://www.dodccrp.org/files/Alberts_NCW.pdf.

[2] ANDERSON J.P., *Computer Security Technology Planning Study,* Vol. II ESD-TR-73-51, Electronic System Division, Air Force System Command, Hansom Field, Bedford, MA, 01730, 1973.

[3] ANDERSON R., *Inżynieria zabezpieczeń,* WNT, Warszawa, 2005.

[4] BAILEY M., *The Unified Cross Domain Management Office: Bridging Security Domains and Cultures*, CrossTalk, July 2008, http://www.stsc.hill.af.mil/crosstalk/2008/ 07/0807B.

[5] BELL D.E., LA PADULA L.J., *Secure Computer System: Unified Exposition and Multics Interpretation*, ESD-TR-75-306, Bedford, MA:ESD/AFSC, Hanscom AFB, http://csrc.nist.gov/publications/history/bell76.pdf.

[6] CLARK D., WILSON D.R., *A Comparison of Commercial and Military Computer Security Policies*, Proc. IEEE Symposium on Research in Security and Privacy, pp. 184-194, 1987.

[7] DEAN T., WYATT G., *Information Exchange between Resilient and High-Threat Networks: Techniques for Threat Mitigation*, RTO-MP-IST-041, NATO RTO IST Symposium on "Adaptive Defence in Unclassified Networks", Toulouse, France, 19 - 20 April 2004.

[8] FERRIE P., *Attacks on Virtual Machine Emulators*, Association of anti Virus Asia Researchers Conference, Auckland, New Zealand, Dec 2006, http://www.symantec.com/avcenter/reference/Virtual_Machine_Threats.pdf.

[9] GAWINECKI J., ZIELIŃSKI Z., LIDERMAN K., CHUDZIKIEWICZ J., SUSKI Z., PATKOWSKI A., *Bezpieczeństwo Systemów Teleinformatycznych SZ RP,* Nowoczesne technologie systemów uzbrojenia, praca zbiorowa po redakcją Z. Mierczyka, str.62-75, Wydawnictwo WAT, Warszawa, 2008.

[10] GJERTSEN T., NORDBOTTEN A.; *Military operational systems in field – multiple levels of security,* Norwegian Defence Research Establishment (FFI), 23.06.2009, http://rapporter.ffi.no/rapporter/2009/01137.pdf.

[11] KOŚLA R., *Bezpieczeństwo połączeń międzysystemowych i międzysieciowych w kontekście ochrony informacji niejawnych*, materiały X-tej konferencji Secure, Warszawa, 2006.

[12] LIDERMAN K., *Analiza ryzyka i ochrona informacji w systemach komputerowych,* PWN, Warszawa, 2008, ISBN 978-83-01-15370-0.

[13] LIDERMAN K., *Podręcznik administratora bezpieczeństwa teleinformatycznego*, MIKOM, Warszawa, 2003, ISBN 83-7279-377-8.

[14] LINCOURT D., PEUKERT H., *Enterprise SOAs for the convergence of Battle Management and Resource Management systems*, Proceedings on 12th International Command and Control Research and Technology Symposium "Adapting C2 to the 21st Century", Newport, 2007.

[15] MAŁOWIDZKI M., LIPONOGA K., SOBOŃSKI P., GONIACZ R., ŚLIWA J., PIOTROWSKI R., AMANOWICZ M., *Secure Information Sharing in a Tactical Network*, 1th Military Command Information System Conference, Gdynia, September 18-19, 2006, Ref. 2.3, s. 1-5.

[16] MCLEAN J., *The Specification and Modeling of Computer Security, Computer*, Vol. 23. No. 1 (Jan 1990), pp. 9-16.

[17] SMITH R., *Introduction to Multilevel Security*, http://www.cs.stthomas.edu/faculty/resmith/r/mls/index.html.

[18] *Coalition Warrior Interoperability Demonstrations*, http://www.cwid.js.mil.

[19] *INFORMATION ASSURANCE: National Partnership Offers Benefits, but Faces Considerable Challenges*, United States Government Accountability Office, GAO-06-392, March 2006, http://www.gao.gov/new.items/d06392.pdf.

[20] NC3A, *Speed Data Diode (HSDD)*, Materiały informacyjne z http://nato-cat.softbox.co.uk/Pages/Product.aspx?ProductID=249.

[21] *Next Generation Security Architecture for NBD Overview*, Technical Report, Swedish Defence Material Administration, 2007, http://www.fmv.se/WmTemplates/Page.aspx?id=2553.

[22] *Rozporządzenie Prezesa RM z dn. 25.08.2005 w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego* (Dz.U. nr 171 poz. 1433 z 08 września 2005 r.).

[23] *Secure Service Oriented Architectures (SOA) Supporting NEC*, Technical Report, NATO/RTO Task Group IST-061, Jan 2009, ISBN 978-92-837-0069-2.

[24] *Ustawa z dn. 22.01.1999 o ochronie informacji niejawnych* - rozdział X (Dz.U. 11/1999 poz. 95).

[25] *Ustawa z dnia 15 kwietnia 2005 r. o zmianie ustawy o ochronie informacji niejawnych oraz niektórych innych ustawach* (Dz. U. nr 85 poz. 727 z 16 maja 2005 r.).

[26] *Zestaw Nadawczo-Odbiorczy ZNO-50*, Filbico, Materiały informacyjne http://www.filbico.pl.

Beyond an air gap - cross domain networks connectivity

ABSTRACT: The paper is a brief survey of selected Cross Domain Solutions for classified network connectivity. Various needs and threats relative to CDS are discussed together with the relevant research and standardization activities. Then, the underlying information assurance components which are commonly employed in securing cross domain interfaces are described. Finally, several advanced cross domain gateways and NEC related development directions of CDS facilities are enumerated.

KEYWORDS: cross domain solutions, multilevel security, data diode

Praca wpłynęła do redakcji: 16.10.2009