Krzysztof Cabaj
Instytut Informatyki
Politechnika Warszawska

Grzegorz Kołaczek
Instytut Informatyki
Politechnika Wrocławska

Jerzy Konorski
Wydział ETI
Politechnika Gdańska

Piotr Pacyna
Katedra Telekomunikacji
Akademia Górniczo-Hutnicza

Zbigniew Kotulski, Łukasz Kucharzewski, Paweł Szałachowski
Instytut Telekomunikacji
Politechnika Warszawska

# Architektura bezpieczeństwa Systemu IIP na poziomie wirtualizacji zasobów

Artykuł przedstawia koncepcję architektury bezpieczeństwa na poziomie wirtualizacji zasobów Systemu IIP. Omawiane są trzy linie mechanizmów obronnych, w tym ochrona integralności informacji, wykrywanie anomalii i zasady pracy systemu budowania metryk zaufania węzłów wirtualnych.

## 1. Wprowadzenie

Bezpieczeństwo sieciowe znajduje się w centrum uwagi wielu projektów europejskich dotyczących Internetu Przyszłości. Zwracają przy tym uwagę zwłaszcza: 1) podnoszona konieczność uwzględnienia problematyki bezpieczeństwa już we wczesnych stadiach projektu, by przełamać paradygmat retrospektywnego przeciwdziałania pojawiającym się zagrożeniom pracy sieci oraz 2) powiązanie wybranych schematów bezpieczeństwa z mechanizmami budowy zaufania pomiędzy elementami sieci. Koncepcje architektury systemu zaufania rozwijane są m. in. w projektach X-ETP i 4WARD [1], [2], [3]. Wirtualizacja zasobów sieci, stanowiąca motyw przewodni realizowanego obecnie w Polsce projektu Inżynieria Internetu Przyszłości (IIP) [4], stwarza nowe wyzwania, do których należy zaliczyć na przykład większą podatność na nieuprawniony dostęp podmiotów spoza logicznej struktury sieci wirtualnej, związany z faktem współdzielenia fizycznej infrastruktury transmisyjnej przez wielu użytkowników, trudności w zakresie ochrony programowych maszyn wirtualnych oraz trudności zabezpieczania komunikacji pomiędzy maszynami wirtualnymi w tym samym węźle fizycznym i pomiędzy węzłami. Obecnie brakuje spójnej wizji rozwiązań w zakresie bezpieczeństwa w środowisku zwirtualizowanych zasobów sieciowych, chociaż próby sformułowania ogólnych zasad bezpieczeństwa dla takich środowisk znajdujemy w wielu źródłach.

Niniejsza praca opisuje architekturę bezpieczeństwa dla Systemu IIP, będącego prototypową instalacją integrującą różne protokoły przekazu danych i sterowania w oparciu o wirtualizację łączy, węzłów i serwerów w ramach 4-poziomowej architektury logicznej [4]. Propozycje ograniczone są do poziomu 2, odpowiedzialnego za tworzenie i funkcjonowanie zasobów wirtualnych.

## 2. Architektura bezpieczeństwa Systemu IIP na poziomie 2

Proponowana architektura bezpieczeństwa bierze pod uwagę zagrożenia, które można klasyfikować jako przypadkowe bądź celowe, a także jako wewnętrzne (pochodzące od współużytkowników fizycznej infrastruktury transmisyjnej) bądź zewnętrzne (stwarzane np. przez przejętą przez intruza maszynę wirtualną implementującą wirtualny węzeł Systemu IIP). Incydenty bezpieczeń-

Praca współfinansowana przez Unię Europejską w ramach Funduszy Europejskich 2007-2013, Nr umowy POIG.01.01.02-00-045/09-00 "Inżynieria Internetu Przyszłości".

stwa będą wspólnie określane jako *atak* dla podkreślenia ich jakościowo nieodróżnialnych konsekwencji na poziomie 2. Rozważane na tym poziomie ataki mają przynajmniej jedną z następujących cech: 1) pochodzą ze źródła zewnętrznego w stosunku do Systemu IIP i są skierowane przeciwko poprawnemu przepływowi jednostek danych (*PDU – Protocol Data Unit*) w łączach wirtualnych, lub 2) pochodzą z przejętej przez intruza maszyny implementującej wirtualny węzeł Systemu IIP. Przykłady obejmują: fałszowanie PDU przez zewnętrznych intruzów (np. przechwytywanie i modyfikacje ruchu Systemu IIP, bądź wprowadzanie obcego ruchu); wprowadzanie niebezpiecznego ruchu przez przejęte węzły wirtualne Systemu IIP dążące do dezorganizacji pracy lub degradacji wydajności węzłów odbiorczych; zakłócenia relacji czasowych lub kolejnościowych w strumieniach PDU spowodowane przyczynami obiektywnymi (niewystarczające pasmo łącza wirtualnego, niedoskonała izolacja zasobów wirtualnych), bądź działaniami celowymi (np. atakami typu *jelly-fish*, *replay* itp.); wreszcie zakłócenia izolacji względnie profili użytkowania zasobów wirtualnych spowodowane np. atakami typu *VM escape*.

2.1 Polityka bezpieczeństwa

Klasyczne podejścia oparte na znanych modelach zagrożeń i repozytoriach sygnatur ataku nie wydają się przydatne na poziomie 2. Systemu IIP. Mechanizmy znanych ataków są specyficzne względem protokołów poziomów 3. i 4. Systemu IIP – tzw. Równoległych Internetów oraz sieci wirtualnych – których znajomości ani dostępności odpowiednich informacji sterujących nie zakłada się na poziomie 2. Wskutek współdzielenia infrastruktury transmisyjnej z użyciem zróżnicowanych technik transmisyjnych ataki na poziomie 2. są trudniejsze do przewidzenia, zaś ich objawy w mniejszym stopniu charakterystyczne. Uzasadnia to stosowanie podejścia opartego na wykrywaniu anomalii. Zarazem ataki na poziomie 2. mają potencjalnie większą skalę oddziaływania: np. atak na węzeł wirtualny jednego z Równoległych Internetów może oddziaływać na pozostałe Równoległe Internety. W ramach proponowanego podejścia definiuje się typy obserwowalnych zdarzeń wskazujących na wystąpienie ataku (SRE – *security related events*). Szczególnie istotne są SRE związane z obserwacją strumieni PDU, a także z profilem wykorzystania zasobów węzłów wirtualnych. Celem polityki bezpieczeństwa jest:

- *prewencja* fałszowania PDU przez intruzów zewnętrznych w stosunku do Systemu IIP,
- *wykrywanie* wybranych ataków pochodzących z wewnątrz lub z zewnątrz Systemu IIP.

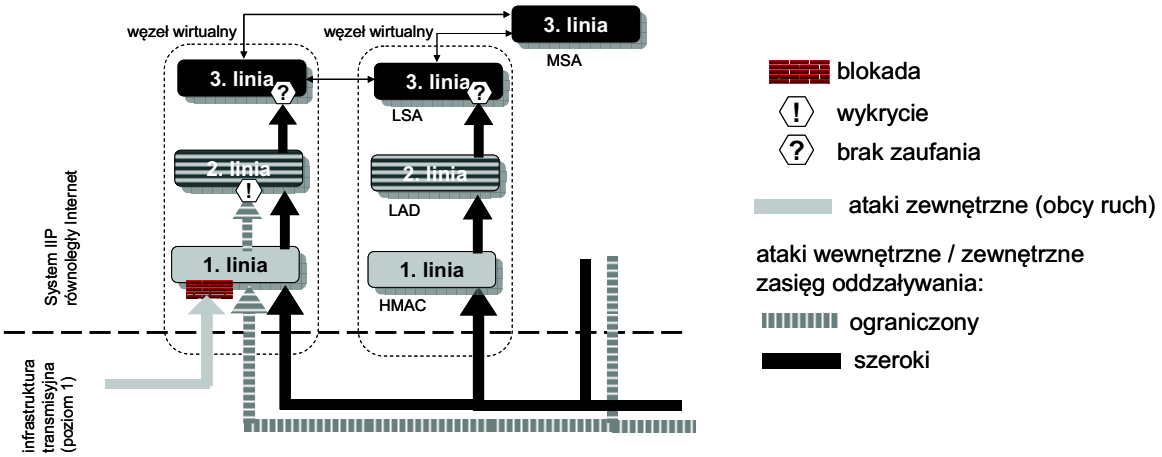
2.2 Trzy linie mechanizmów obronnych

Rys. 1 przedstawia linie obrony w węźle wirtualnym Równoległego Internetu (strzałki blokowe wskazują możliwe źródła i zasięg oddziaływania ataków).

Pierwsza linia mechanizmów obronnych zatrzymuje obcy ruch próbujący przeniknąć do Systemu IIP (neutralizując ataki przez fałszowanie PDU oraz typu *replay*). Realizuje ona ochronę integralności i uwierzytelnianie jednostek PDU wymienianych przez łącze wirtualne przy pomocy mechanizmu HMAC pracującego z nominalną przepływnością łącza, wyspecyfikowanego jako podzbiór standardu IEEE 802.1ae (MACSec). Moduły HMAC, przewidziane do implementacji w obrębie narzędzi wirtualizacyjnych realizowanych na platformie netFPGA, eliminują PDU niespełniające testu HMAC oraz raportują zdarzenia sygnalizujące podejrzenie ataku.

Drugą linię stanowią mechanizmy *soft security* lokalne dla węzła wirtualnego. Ich zadaniem jest filtracja SRE wskazujących na ataki o zasięgu lokalnym, dla których pierwsza linia obrony nie jest wystarczającą przeszkodą (np. generujące ruch zewnętrzny o charakterze jedynie "nękającym" typu DoS, bądź ruch wewnętrzny z przejętej maszyny wirtualnej Systemu IIP). Rejestrowane są SRE obserwowane przez moduły pierwszej linii (nieudane testy HMAC, źle sformatowane nagłówki PDU, niepoprawne wiadomości w płaszczyźnie zarządzania itp.), a także odchylenia od profili użytkowania zasobów wirtualnych węzła. Lokalny moduł wykrywania anomalii (LAD – *local anomaly detection*), implementowany jako fragment kodu węzła wirtualnego, interpretuje rejestr SRE przekształcając go w rejestr lokalnych anomalii, ponadto za pośrednictwem mechanizmów trzeciej linii obrony kontaktuje się z innymi węzłami celem wykrycia anomalii o szerszym zasięgu.

Trzecia linia obrony również jest typu *soft security* i przeciwdziała atakom o szerokim zasięgu oddziaływania (np. typu *slow scanning*, nieuprawniony dostęp itp.), niewykrywalnym przez LAD; niweluje też skutki niepoprawnego działania LAD w przejętym węźle wirtualnym. Lokalny moduł kooperacji między węzłami (LSA – *local security agent*) zbiera i przetwarza informacje o zaobserwowanych SRE, przekształcając je w lokalne metryki reputacyjne i przekazując wraz z rejestrem SRE do centralnego węzła (MSA – *master security agent*). MSA wylicza globalne metryki reputacyjne i wykrywa anomalie o szerszym zasięgu, po czym rozgłasza je w obrębie Równoległego Internetu jako wiadomości Secure SNMP w formie odpowiednich alarmów oraz miar zaufania. W ten sam sposób przekazywane są również uaktualnienia konfiguracji lokalnych filtrów SRE.




Rys.1. Zarys architektury bezpieczeństwa na poziomie 2 Systemu IIP

## 3. Ochrona integralności i szyfrowanie na poziomie systemu transmisyjnego IIP

Współczesne systemy transmisyjne muszą wykazywać odporność na przypadkowe oraz intencjonalne zakłócenia ich pracy. Szczególnej ochronie powinny podlegać protokoły sterujące oraz zarządzające pracą systemu, ponieważ sieć zarządzająca niekiedy korzysta z tej samej infrastruktury, w której obsługiwane są dane użytkowe. Rozwiązanie HMAC/MACSec stanowi pierwszą linię obrony Systemu IIP. HMAC/MACSec chroni ramki transmisyjne Systemu IIP na poziomie 2. W tym celu HMAC stosuje standard IEEE 802.11ae (obecnie IEEE 802.1x-2010), który wprowadza ochronę integralności ramek, gwarantuje ich autentyczność, zapobiega atakom poprzez powtórzenia oraz umożliwia uzyskanie poufności danych. Ochrona ta może być włączona osobno na każdym łączu Systemu IIP. Implementacja rozwiązania polega na wprowadzeniu do węzłów fizycznej infrastruktury transmisyjnej Systemu IIP modułu przetwarzającego MAC Security Entity (SecY), który wykonuje sprzętowe przetwarzanie ramek Systemu IIP w układzie FPGA pracującym z prędkością 1 lub 10 Gbit/s. Dzięki usytuowaniu tego elementu na poziomie 2 System IIP zyskuje jednorodny mechanizm, który może być stosowany selektywnie do ochrony Równoległego Internetu przenoszącego dowolny rodzaj ruchu, wykorzystując zarówno protokoły IP, jak również inne. Monitorując poprawność przetwarzanej ramki, HMAC/MACSec umożliwia wykrywanie ataków skierowanych przeciwko systemowi pochodzących od przejętych węzłów wirtualnych Systemu IIP (takich jak *denial of service*, *man-in-the-middle*, *masquerading*, *passive wiretapping* oraz *playback*), jak również ataków pochodzących spoza Systemu IIP. Stwierdzenie wystąpienia niepoprawnej ramki skutkuje odrzuceniem ramki oraz przekazaniem odpowiednich informacji do drugiej i trzeciej linii obrony w celu ich analizy. Zastosowane tam metody scharakteryzowano w punktach 4 i 5.

## 4. Wykrywanie anomalii

Zastosowanie metod wykrywania anomalii daje możliwość identyfikacji wcześniej nierozpoznanych metod ataku lub problemów bezpieczeństwa, dla których jeszcze nie została zdefiniowana odpowiednia sygnatura. Po zdefiniowaniu bądź wyznaczeniu charakterystyki normalnego zachowa-

nia systemu przeprowadza się identyfikację zdarzeń znacząco od niej odbiegających. Jedną z metod postępowania jest generowanie alarmów po wykryciu statystycznie rzadkich stanów systemu.

Moduł LAD wykrywa anomalie na poziomie węzła Systemu IIP. Możliwe jest też identyfikowanie anomalii osobno dla każdego z Równoległych Internetów tworzących System IIP, rozumianych jako zbiory wirtualnych węzłów. Odpowiada za to moduł PI-AD w MSA analizujący zmiany wartości wybranych atrybutów stanu danego Równoległego Internetu. Proponowane podejście do projektowania modułów LAD wykorzystuje kompleksowe informacje o stanie Systemu IIP i opiera się na metodach eksploracji danych oraz na statystycznej analizie szeregów czasowych.

### 4.1. Wykrywanie anomalii z wykorzystaniem metod eksploracji danych

Analizie podlega tutaj rejestr SRE – na przykład zapisy nieudanego logowania, odrzucenia PDU przez moduł HMAC, prób odczytania poprzez SNMP klucza z bazy MIB bez stosownych uprawnień, czy też odrzucenie niezgodnego z polityką bezpieczeństwa połączenia w płaszczyźnie zarządzania. Z każdym SRE, oprócz jego typu i czasu wystąpienia, związane są pewne atrybuty, np. nazwa konta, źródłowy i docelowy adres IP w odrzuconym PDU, czy OID klucza w bazie MIB. SRE generowane przez programy działające pod kontrolą systemu Linux w węźle Systemu IIP są logowane za pomocą standardowego podsystemu syslog, skąd moduł LAD pobiera dane do analizy. Takie rozwiązanie pozwala w przyszłości łatwo rozszerzyć zbiór zdefiniowanych SRE.

Proponowana metoda opiera się na wykrywaniu tzw. zbiorów częstych (*frequent sets*), tj. powtarzających się często wzorców zachowań. Jeśli dane do analizy traktujemy jako zbiory odpowiednich atrybutów, to zbiorem częstym nazywamy podzbiór występujący co najmniej *minSup*-krotnie w analizowanych danych. Parametr *minSup*, nazywany minimalnym wsparciem, jest parametrem wejściowym algorytmu wyszukiwania zbiorów częstych. Analizując tą metodą SRE dotyczące np. odrzuconych prób dostępu do kluczy MIB można wykryć wzorzec związany z próbą poznania przez danego użytkownika wartości pewnych elementów MIB. Jeśli wykryty zbiór częsty zawiera informację o adresie IP, oznacza to atak przeprowadzany z jednej maszyny. Brak w wykrytym zbiorze częstym identyfikatora OID świadczy o próbie dotyczy poznania różnych elementów MIB. Gdy wykryty zbiór częsty zawiera atrybut związany z OID przy braku atrybutu związanego z adresem IP, atak był przeprowadzany z wielu maszyn i dotyczył określonego elementu bazy MIB.

W wyniku analizy uzyskanych zbiorów częstych, do modułu obliczania reputacji (*reputation calculator*) zostanie przekazana ocena ryzyka (*severity*) związanego z daną anomalią oraz prawdopodobieństwo trafności oceny dokonanej przez moduł LAD. Informacje te (na rys. 2 oznaczone odpowiednio jako $c^l$ i $p_n^l$, gdzie $l$ jest symbolem anomalii a $n$ numerem okresu obserwacji) wykorzystywane są przez system zarządzania reputacją omawiany w p. 4.

### 4.2. Wykrywanie anomalii z wykorzystaniem analizy szeregów czasowych

W planowanej implementacji LAD dla środowiska wirtualizatora Xen bieżące wartości wybranych cech wirtualnych węzłów Równoległych Internetów takich jak:

- intensywność przybywających strumieni PDU danego Równoległego Internetu,
- średni rozmiar pola danych (*payload*) w PDU danego typu Równoległego Internetu,
- średni poziom obciążenia jednostki centralnej (CPU) i wykorzystania pamięci operacyjnej

będą odczytywane z lokalnej bazy MIB oraz z narzędzi systemowych vir-top oraz xentop. Rozbieżności wartości aktualnych ze stanami historycznymi analizowane będą przy pomocy wybranych i przetestowanych algorytmów analizy szeregów czasowych (np. algorytm "Plateau" wykrywania zmian przepustowości, algorytm Holta-Wintersa, czy metoda Burgessa [5]). Informacje o zaobserwowanych anomaliach umieszczane będą w lokalnej bazie MIB.

Moduł PI-AD w MSA wykrywa anomalie w zachowaniu danego Równoległego Internetu. Stan Równoległego Internetu, definiowany jako stan jego węzłów, opisany jest poprzez wektor własny macierzy korelacji wybranej cechy, obliczanej jako korelacja wartości cechy dla każdej możliwej pary węzłów. Anomalie stwierdzane są dla każdej cechy z osobna. Moduł PI-AD uzyskuje informacje o wartościach cech w węzłach poprzez zapytania Secure SNMP do centralnej bazy MIB.

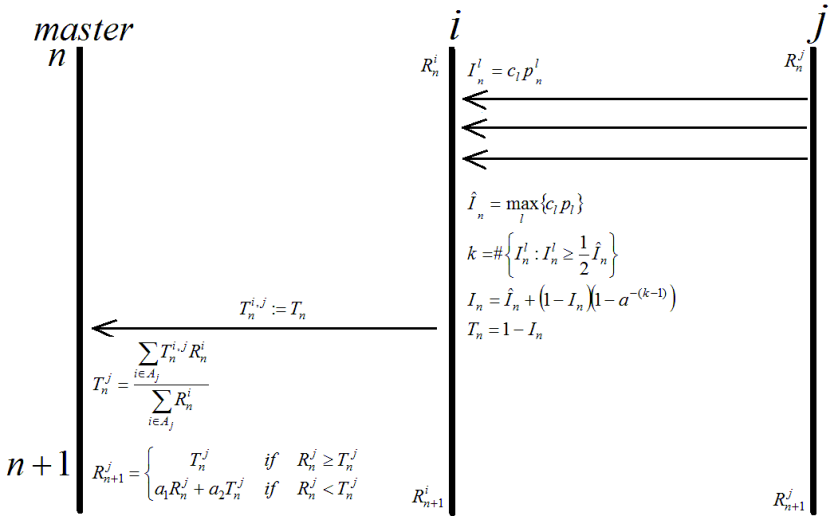
## 5. System zarządzania reputacją

Mechanizmy zarządzania, routingu i bezpieczeństwa w Systemie IIP wymagają stałej oceny poprawności pracy węzłów sieci i połączeń między węzłami. Różnorodność czynników wpływających na ich działanie oraz wiele możliwości precyzyjnego opisu wpływu każdego z tych czynników sprawia, że zdecydowano się na przyjęcie systemu reputacyjnego jako jednolitego narzędzia oceny poprawności pracy węzłów i połączeń w Systemie IIP. Rozwiązanie takie jest charakterystyczne dla systemów bez scentralizowanej administracji – sieci bezprzewodowych *mesh*, systemów obliczeń w chmurach (*cloud computing*), czy sieci społecznościowych [6], [7].

Model reputacji wykorzystany w Systemie IIP powinien zapewniać:

- elastyczność ze względu na zakres dostępnych informacji o węzłach i ruchu sieciowym, z preferencją dla danych obiektywnych z bieżącej obserwacji działania Systemu IIP,
- wrażliwość na pojawiające się zagrożenia przy zachowaniu możliwości poprawy reputacji w przypadku ustąpienia zagrożeń,
- możliwość modyfikacji obliczania reputacji (w tym zmiany modelu matematycznego) przy zachowaniu systemu przesyłania, przechowywania i udostępniania niezbędnych informacji,
- łatwość pozyskiwania danych do obliczania reputacji od wszystkich modułów analitycznych i zarządzających Systemu IIP,
- dostępność informacji o obliczonych wartościach reputacji wszystkich węzłów i łączy z innych podsystemów Systemu IIP (zarządzanie, routing, inne systemy bezpieczeństwa).

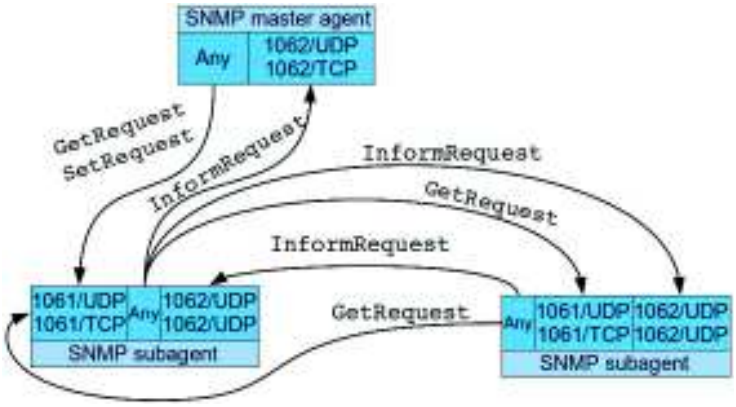
Jako model matematyczny obliczania reputacji przyjęto model heurystyczny inspirowany metodami bayesowskimi [8] – rys. 2. Jego podstawowym założeniem jest dwustopniowa ocena węzłów w ustalonych chwilach $n = 1,2,\ldots$ z użyciem pojęć zaufania (*trust*) i reputacji (*reputation*). Zaufanie $T_n^{i,j}$ jest indywidualną oceną danego węzła $j$ przez jego sąsiada $i$ w topologii poziomu 2 Systemu IIP na podstawie danych o incydentach $I_n$ dostarczonych przez inne moduły (HMAC, LAD). Reputacją $R_{n+1}^j$ węzła $j$ w chwili $n$+1 jest skumulowana informacja o zaufaniu obliczona centralnie na podstawie danych o zaufaniu $T_n^{i,j}$ dostarczonych przez jego sąsiadów, z uwzględnieniem reputacji tych sąsiadów $R_n^j$ i wartości reputacji ocenianego węzła $R_n^i$.




Rys. 2. Przykład sposobu obliczania reputacji węzłów

Jako protokół komunikacyjny dla zarządzania reputacją wybrano SNMPv3, który pracuje jako scentralizowany system agentowy w paradygmacie klient-serwer – rys. 3, ponadto ma możliwość bezpiecznej komunikacji między agentami. W podstawowej wersji systemu reputacyjnego wykorzystywana będzie jedynie komunikacja między agentami lokalnymi w węzłach Systemu IIP (agent SNMP, LSA) a centralnym agentem obliczającym reputacje węzłów (master agent SNMP, MSA).

Agent zarządzający reputacją współdzieli lokalną bazę danych z agentem SNMP, stanowiąc odrębny moduł programowy. Umożliwia to niezależną aktualizację obu systemów agentowych.




Rys. 3. Schemat komunikacji agentów protokołu SNMP dla zarządzania reputacja

Protokół SNMP wykorzystuje bazę danych MIB, w której będą zapisywane informacje o incydentach wykrytych przez lokalne moduły analityczne węzła. LSA pobiera z bazy dane o incydentach i na ich podstawie oblicza poziom zaufania do swoich sąsiadów. Następnie zapisuje wynik do bazy, a agent SNMP przesyła rezultat do MSA poprzez master agenta SNMP. W bazie tej znajdzie się również, uzyskana od MSA informacja o aktualnej reputacji węzła. Zarówno ta informacja, jak i zapisane w bazie MSA informacje o reputacji wszystkich węzłów sieci będą udostępniane mechanizmom zarządzania Systemu IIP poprzez dostęp do odpowiednich MIB master agenta SNMP i lokalnych agentów SNMP.

## 6. Podsumowanie

Architektura systemu bezpieczeństwa jest częścią specyfikacji poziomu 2 Systemu IIP, który udostępnia mechanizmy i techniki wirtualizacji dla tworzenia Równoległych Internetów. Dzięki takiemu usytuowaniu mechanizmy bezpieczeństwa będą wprowadzone do Systemu IIP w sposób jednolity i będą jednakowo dostępne dla Równoległych Internetów. Oparcie systemu bezpieczeństwa na wykrywaniu anomalii eliminuje wykorzystanie znanych modeli zagrożeń i repozytoriów sygnatur ataku. Te są bowiem nieprzydatne na poziomie 2, gdyż mechanizmy ataków są specyficzne względem wyższych poziomów Systemu IIP, zaś ich objawy mniej charakterystyczne wskutek współdzielenia infrastruktury transmisyjnej przez Równoległe Internety. Prowadzone prace projektowe zmierzają do praktycznej weryfikacji proponowanego rozwiązania w ogólnokrajowym środowisku eksperymentalnym, aktualnie budowanym w oparciu o specyfikację Systemu IIP.

## Literatura


1. A. Gavras et al., “Future Internet Research and Experimentation: The FIRE Initiative”, ACM SIGCOMM Computer Communication Review, 37, 3, July 2007.
2. “Future Internet - Strategic Research Agenda”, ver. 1.1, FI X-ETP Group, January 2010.
3. M. Soellner, “The 4WARD Approach to Future Internet”, ITG FG 5.2.3 Meeting Eschborn, 2010.
4. W. Burakowski, H. Tarasiuk, A. Beben, System IIP for supporting „Parallel Internets (Networks)”, Future Internet Assembly meeting, Ghent 2010, fi-ghent.fi-week.eu/files/2010/12/1535-4-System-IIP-FIA-Ghent-ver1.pdf.
5. M. Burgess, “Two dimensional time-series for anomaly detection and regulation in adaptive systems”, in: IFIP/IEEE 13th Int. Workshop on Distributed Systems: Operations and Management, DSOM 2002, pp. 169-185
6. A. Srinivasan, J. Teitelbaum, Jie Wu, M. Cardei, H. Liang, “Reputation-and-Trust-Based Systems for Ad Hoc Networks”, pp. 375-403, in A. Boukerche [ed.], Algorithms and Protocols for Wireless and Mobile Ad Hoc Networks, J. Wiley & Sons, Inc. 2009.
7. K. Hoffman, D. Zage, and C. Nita-Rotaru, “A survey of attack and defense techniques for reputation systems”, ACM Computing Surveys, vol. 42, no. 1, pp. 1-31, 2010.
8. T. Ciszkowski et al., “Towards Quality of Experience-based reputation models for future web service provisioning”, Telecommunication Systems, DOI: 10.1007/s11235-011-9435-2.