Architektura bezpieczeństwa Systemu IIP

Krzysztof Cabaj[1], Grzegorz Kołaczek[2], Jerzy Konorski[3], Zbigniew Kotulski[4], Łukasz Kucharzewski[4], Piotr Pacyna[5], Paweł Szałachowski[4]

[1] Instytut Informatyki, Politechnika Warszawska
[2] Instytut Informatyki, Politechnika Wrocławska
[3] Wydział Elektroniki, Telekomunikacji i Informatyki, Politechnika Gdańska
[4] Instytut Telekomunikacji, Politechnika Warszawska
[5] Katedra Telekomunikacji, Akademia Górniczo-Hutnicza

Streszczenie 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.

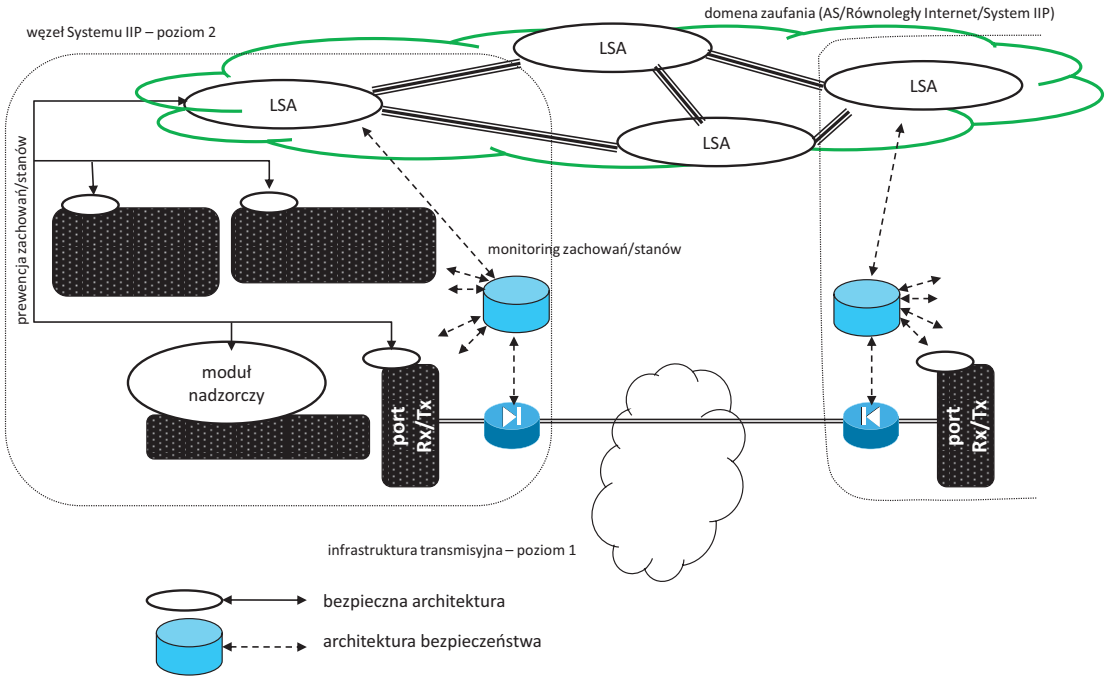
1 Wprowadzenie

Niniejszy rozdział opisuje architekturę bezpieczeństwa dla Systemu IIP - prototypowej instalacji powstającej obecnie w Polsce w ramach projektu Inżynieria Internetu Przyszłości (IIP) [1, 2], integrującej tzw. Równoległe Internety o różnych technikach transmisji. Podstawową metodą integracji jest wirtualizacja łączy, węzłów i serwerów w ramach 4-poziomowej architektury logicznej. Przedstawione tu propozycje architektury bezpieczeństwa ograniczone są do poziomu 2, odpowiedzialnego za tworzenie i funkcjonowanie zasobów wirtualnych.

Bezpieczeństwo sieciowe znajduje się w centrum uwagi wielu projektów europejskich dotyczących Internetu Przyszłości. Zauważyć w nich można zwłaszcza:

- podnoszoną konieczność uwzględnienia problematyki bezpieczeństwa sieciowego juz we wczesnych stadiach projektu, by przełamać paradygmat retrospektywnego przeciwdziałania zagrożeniom oraz
- 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 [3–8].

Wirtualizacja zasobów sieci, stanowiąca motyw przewodni Systemu IIP stwarza nowe wyzwania, do których należy zaliczyć większą podatność na nieuprawniony dostęp podmiotów spoza logicznej struktury sieci wirtualnej (związany ze współdzieleniem fizycznej infrastruktury transmisyjnej przez wielu użytkowników), trudności w zakresie ochrony programowych maszyn wirtualnych oraz trudności zabezpieczania komunikacji pomiędzy maszynami wirtualnymi w węźle fizycznym i pomiędzy węzłami.



Rysunek 1. Bezpieczna architektura i architektura bezpieczeństwa na poziomie 2

Obecnie brakuje spójnej wizji rozwiązań w zakresie bezpieczeństwa w środowisku wirtualizowanych zasobów sieciowych, chociaż próby sformułowania ogólnych zasad bezpieczeństwa dla takich środowisk znajdujemy w wielu źródłach. Na przykład w pracy [9] opisano możliwy sposób migracji współczesnej sieci w kierunku Internetu Przyszłości poprzez rozmieszczenie we wszystkich elementach sieci modułów softwarowych, zwanych *Cognitive Managers*. Każdy z nich zarządza abstrakcjami wirtualnych zasobów sieci oraz posiada wbudowany moduł pod nazwą *Supervisor and Security Module*, zapewniający ustalone atrybuty bezpieczeństwa (np. uwierzytelnianie, integralność i poufność przekazu danych, wykrywanie włamań). W ten sposób tworzona jest *bezpieczna architektura* Internetu Przyszłości; cechuje ją immanentny i proaktywny charakter mechanizmów bezpieczeństwa, co w zasadzie zapobiega wykroczeniom poza zakres normalnej pracy sieci. W odróżnieniu od tego przez *architekturę bezpieczeństwa* należy rozumieć zespół mechanizmów wzbogacających funkcjonalność już istniejącego bądź uprzednio zaprojektowanego systemu transmisyjno-komutacyjnego. Mechanizmy te są zwykle specyficzne względem przewidywanych zagrożeń i rozmieszczane jedynie w wybranych elementach systemu; w ogólności nie zapobiegają one wykroczeniom poza zakres normalnej pracy, a jedynie je sygnalizują i uruchamiają odpowiednie procedury reaktywne.

Rysunek 1 pokazuje koncepcję bezpiecznej architektury Systemu IIP na poziomie 2, gdzie każdy moduł węzła Systemu IIP (dla uproszczenia zaznaczono jedynie kilka modułów, w tym port nadawczo-odbiorczy) wyposażony jest w moduł nadzorczy bezpieczeństwa komunikujący się z lokalnym agentem bezpieczeństwa (LSA - *local security agent*). Moduły nadzorcze zapobiegają wykroczeniom odpowiednich modułów węzła poza dopuszczalne zakresy stanów lub zachowań specyfikowane przez LSA zgodnie z aktualną polityką bezpieczeństwa. Jednocześnie na podstawie danych zebranych z modułów nadzorczych LSA uzyskuje obraz stanu bezpieczeństwa własnego węzła i węzłów sąsiednich, który następnie współdzieli z LSA w innych węzłach w obrębie ustalonej domeny zaufania (np. systemu autonomicznego (AS), Równoległego Internetu, bądź Systemu IIP jako całości). Współpraca pomiędzy różnymi LSA w ramach domeny zaufania umożliwia w szczególności eliminację węzłów, w których - wskutek uszkodzenia bądź ataku intruza - LSA sam wykracza poza zakres normalnej pracy.

W proponowanym rozwiązaniu przyjęto podejście architektury bezpieczeństwa, gdyż koncepcja Systemu IIP koncentruje się na integracji technik transmisji, nie uwzględniając jawnie problematyki bezpieczeństwa. Na rysunku 1 zilustrowano fakt, że wprowadzenie kryptograficznego zabezpieczenia komunikacji na łączach wirtualnych pomiędzy sąsiednimi węzłami Systemu IIP oraz monitoring zachowań lub stanów poszczególnych modułów węzła pozwala nadal zasilać LSA obrazem stanu bezpieczeństwa węzła, jakkolwiek nie wyklucza wykraczania poza zakres normalnych zachowań lub stanów. Z tego powodu domena zaufania realizowana jest jako system reputacyjny i dostarcza jedynie rekomendacji dotyczących izolacji wybranych fragmentów Systemu IIP, co do których istnieje podejrzenie wykroczenia poza zakres normalnej pracy. Idee te zostaną bardziej szczegółowo omówione w kolejnych punktach rozdziału.

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 bezpieczeństwa 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:

- 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
- 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 *jellyfish, 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.

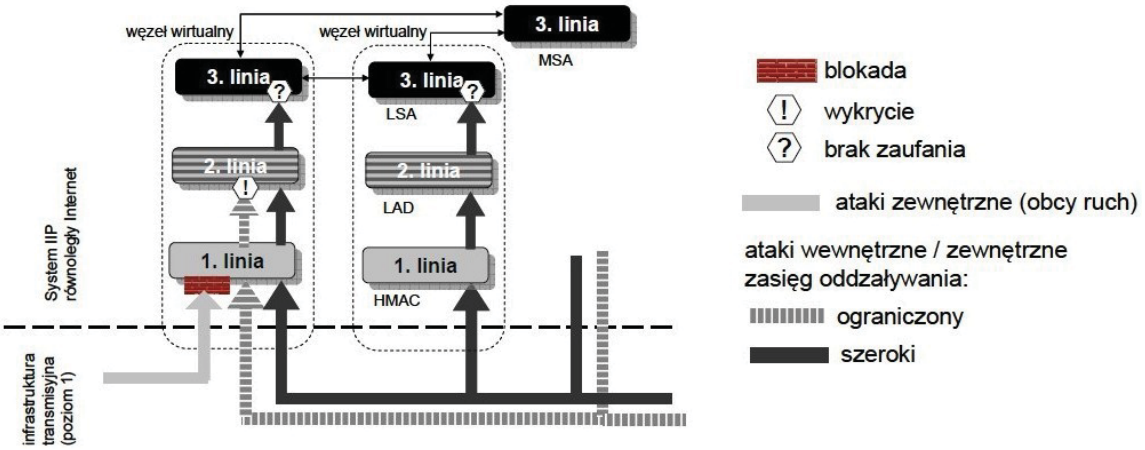
2.2 Trzy linie mechanizmów obronnych

Rysunek 2 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.



Rysunek 2. Zarys architektury bezpieczeństwa na poziomie 2 Systemu IIP

3 Ochrona integralności na poziomie systemu transmisyjnego IIP

Oczekiwania w zakresie bezpieczeństwa, kierowane pod adresem systemu transmisyjnego rozwijanego przez projekt IIP, są związane z istotną grupą zastosowań sieci wirtualnych, w których do głównych wymagań zalicza się dużą odporność na zakłócenia pracy sieci. Mowa tutaj w pierwszej kolejności o zakłóceniach będących wynikiem świadomej ingerencji niepowołanych osób trzecich w pracę sieci, głównie poprzez aktywne ingerowanie w strumienie danych użytkowych przenoszonych przez system transmisyjny, lub w dane wymieniane przez systemy sterowania i zarządzania pracą sieci, jeżeli sieć zarządzająca korzysta z infrastruktury stanowiącej sieć zarządzaną.

Moduł HMAC-SHA-1 odpowiada za identyfikację i usuwanie ruchu obcego próbującego przeniknąć do Systemu IIP, neutralizując przez to ataki polegające na ingerowaniu w zawartość jednostek PDU oraz na wprowadzaniu do systemu transmisyjnego fałszywych jednostek PDU. Rozwiązanie HMAC-SHA-1 stanowi zatem pierwszą linię obrony Systemu IIP.

Rozwiązanie HMAC-SHA-1 zostało zrealizowane w postaci sprzętowego modułu szyfrującego, wykonanego w oparciu o platformę sprzętową netFPGA 1G, wyposażoną w układ programowalny Xilinx Virtex-II Pro. Zadaniem tego modułu jest przetwarzanie strumienia napływającego w postaci ramek systemu transmisyjnego System IIP, przenoszących dane użytkowe jak również dane sygnalizacyjne, sterujące pracą sieci. Celem przetwarzania jest zapewnienie ochrony integralności przesyłanych danych. Stosowany jest tu algorytm HMAC-SHA1 [10] pracujący z nominalną przepływnością łącza. Można uznać, że Moduł HMAC-SHA1, stanowi istotne narzędzie wirtualizacyjne należące do grupy narzędzi System IIP zrealizowanych na platformie netFPGA.

Moduł HMAC-SHA-1 realizuje ochronę ramek transmisyjnych Systemu IIP na poziomie drugim, według modelu warstwowego przyjętego w projekcie IIP, w ten sposób, że przepuszcza ramki transmisyjne spełniające test integralności oraz eliminuje ramki transmisyjne niespełniające tego testu. W tym drugim przypadku raportuje zdarzenia sygnalizujące niepomyślną weryfikację, co jest odbierane jako podejrzenie wystąpienia ataku i przekazywane, wraz z dodatkowymi informacjami do dalszej analizy. Ochrona ta może być włączona osobno na każdym łączu Systemu IIP.

Dzięki usytuowaniu tego elementu w warstwie drugiej system IIP zyskuje uniwersalny mechanizm, który może być stosowany do ochrony każdej sieci wirtualnej, niezależnie od typu Równoległego Internetu w obrębie którego taka sieć została wydzielona, a więc zarówno tam, gdzie wykorzystywane są protokoły internetowe, jak również i tam, gdzie stosowane są protokoły inne niż IP. Jest to rozwiązanie niezależne od warstw wyższych systemu transmisyjnego IIP oraz transparentne dla nich.

Wdrożenie rozwiązania w prototypowym systemie polega na wprowadzeniu do węzłów systemu transmisyjnego IIP modułu przetwarzającego HMAC-SHA-1, który wykonuje sprzętowe przetwarzanie ramek IIP w układzie FPGA pracującym z nominalną prędkością 1 Gbit/s (docelowo 10 Gbit/s).

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 zachowania 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*), por. [11], 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. Zbiory częste można wykrywać za pomocą różnych algorytmów. W ramach projektu planuje się implementację algorytmu a priori. W tabeli 1 zaprezentowano kolejne kroki tego algorytmu.

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

Tabela 1. Algorytm a priori, służący do wykrywania zbiorów częstych

1. START
2. Przygotowanie C1 – listy jednoelementowych kandydatów
   Przejrzenie wszystkich zbiorów podlegających analizie w danym okresie czasu i dodanie do C1 jako jednoelementowych zbiorów wszystkich pojawiających się elementów.
3. Przygotowanie F1 – listy jednoelementowych biorów częstych
   Wyliczenie wsparcia wszystkich kandydatów z listy C1, dodanie do listy F1 tych których wsparcie jest większe lub równe minSup.
4. Przygotowanie C2 – listy dwuelementowych kandydatów
   Połączenie wszystkich zbiórów jednoelementowych z F1 w dwuelementowe zbiory w ten sposób zawsze identyfikator pierwszego elementy był mniejszy niż drugiego.
5. Przygotowanie F2 – listy dwuelementowych zbiorów częstych
   Wyliczenie wsparca wszystkich kandydatów z C2 jako liczby tych zbiorów w analizowanym okresie czasu, które zawierają oba elementy. Dodanie do F2 tylko tych zbiorów, których wsparcie jest większe niż założony parametr minSup.
6. LOOP
   (a) Przygotowanie CN – listy kandydatów o N elementach,
   (b) Łączenie tylko tych których N-1 pierwszych elementów jest identycznych,
   (c) Czyszczenie CN,
   (d) Usunięcie tych zbiorów z CN, które mają choćby jeden N-1 elementowy podzbiór nie występujący w F(N-1),
   (e) Wyliczenie wsparcia każdego zbioru z CN,
   (f) Przygotowanie FN – listy zbiorów częstych o N elementach,
   (g) Dodanie do FN tylko tych zbiorów z CN, których wsparcie jest większe lub równe parametr minSup.
7. REPEAT UNTIL lista *FN list* zawiera jakieś nowe zbiory częste.
8. KONIEC

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 rysunku 5 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 punkcie 5 tego rozdziału.

4.2 Wykrywanie anomalii z wykorzystaniem analizy szeregów czasowych

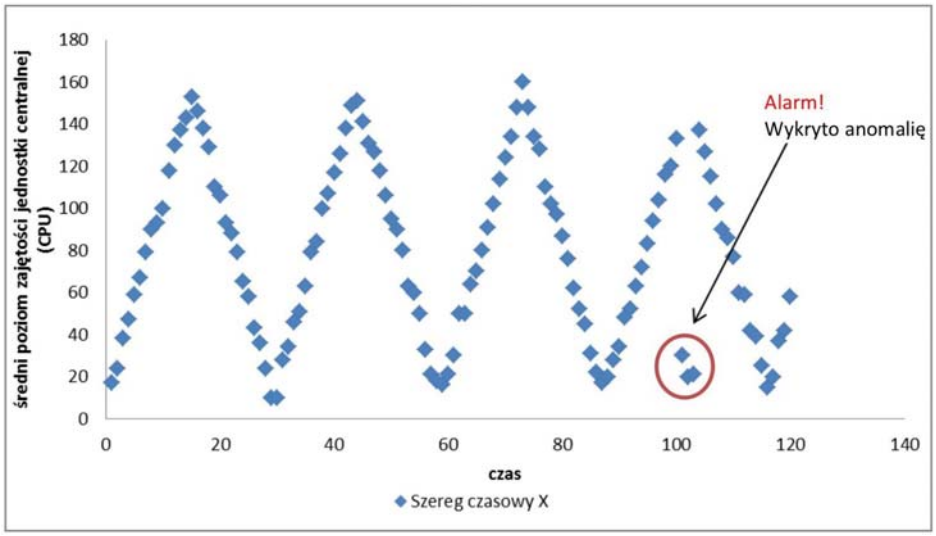
Celem modułu LAD implementującego wykrywanie anomalii z wykorzystaniem analizy szeregów czasowych jest wykrycie nietypowych zjawisk w zachowaniu pojedynczego węzła Systemu IIP. W tym celu badane są cechy charakteryzujące węzeł Systemu IIP oraz cechy charakteryzujące wirtualne węzły poszczególnych

Równoległych Internetów (PI). Agent dokonuje analizy następujących cech charakteryzujących stan węzła Systemu IIP:

1. intensywność nadchodzenia ramek dla danego typu Równoległego Internetu,
2. średni rozmiar sekcji danych w ramce dla danego typu Równoległego Internetu (PI payload),
3. średni stopień zajętości jednostki centralnej (CPU),
4. średni stopień wykorzystania pamięci operacyjnej,

oraz następujących cech charakteryzujących poszczególne wirtualne węzły Równoległych Internetów (*PI node*):

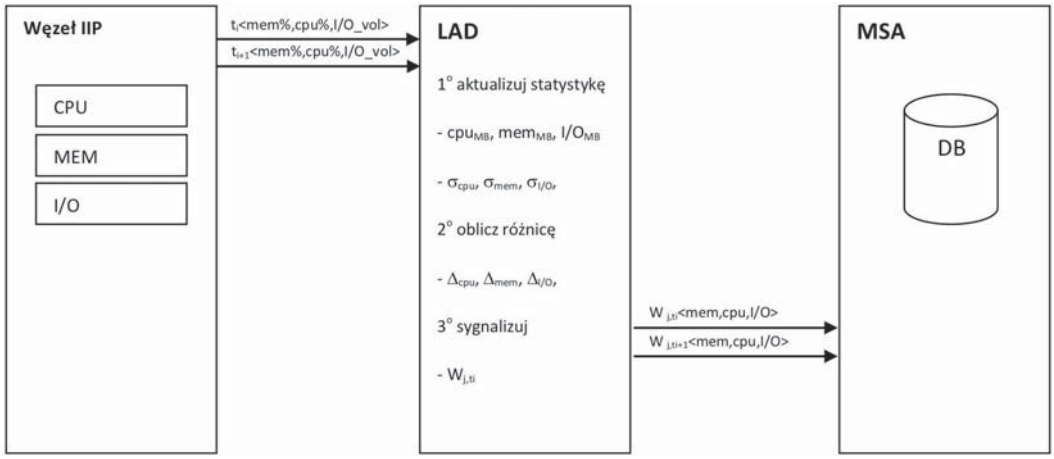
1. średnia liczba bajtów wysyłanych przez węzeł w jednostce czasu,
2. średnia liczba bajtów odbieranych przez węzeł w jednostce czasu,
3. średni stopień zajętości jednostki centralnej (CPU) w jednostce czasu,
4. średni stopień wykorzystania pamięci operacyjnej w jednostce czasu.



Rysunek 3. Anomalie w szeregach czasowych

W pierwszej kolejności planuje się implementację LAD dla węzła Systemu IIP typu Xen. W planowanej implementacji LAD dla środowiska wirtualizatora Xen bieżące wartości wybranych cech wirtualnych węzłów Równoległych Internetów są odczytywane z lokalnej bazy MIB oraz z narzędzi systemowych *vir-top* oraz *xentop*. Rozbieżności wartości aktualnych ze stanami historycznymi analizowane natomiast są przy pomocy wybranych i przetestowanych algorytmów analizy szeregów czasowych (metoda Burgessa [12]).

Komunikat $t_i < mem\%, cpu\%, I/O\_vol >$ na Rysunku 4 zawiera aktualne wartości obserwowanych zmiennych charakteryzujących stan węzła Systemu



Rysunek 4. Przetwarzanie informacji o stanie węzła IIP

IIP, które są zbierane i przetwarzane przez LAD w chwilach $t_i, t_{i+1}, ...$, o stałym i ustalonym odstępie. LAD aktualizuje na podstawie odczytanych wartości stanu węzła Systemu IIP swoje wewnętrzne struktury danych, a następnie oblicza zgodnie z metodą Burgessa wartości statystyk – wartości średnie $(cpu_{MB}, mem_{MB}, I/O_{MB})$ oraz odchylenia standardowe $(\sigma_{cpu}, \sigma_{mem}, \sigma_{I/O})$. Na tej podstawie obliczana jest wartość $\Delta_{cpu}, \Delta_{mem}, \Delta_{I/O}$ określającą poziom zgodności aktualnej obserwacji $t_i < mem\%, cpu\%, I/O\_vol >$ z historycznym zachowaniem się węzła Systemu IIP. W rezultacie LAD przesyła wartość $W_{j,t_i} < mem, cpu, I/O >$ (por. rysunek 4) z przedziału $< 0, 1 >$ będącą informacją poziomie zaobserwowanej anomalii w zachowaniu węzła j Sytemu IIP w chwili t_i do agenta MSA, gdzie 0 oznacza zachowanie zgodne z historycznymi obserwacjami węzła (brak anomalii), a 1 maksymalną różnicę (maksymalny poziom anomalii). LAD przesyła również analogiczny komunikat z wykorzystaniem protokołu SNMP do systemu zarządzania reputacją, co umożliwia aktualizację wartości reputacji węzła Systemu IIP również z uwzględnieniem informacji statystycznych.

Obserwacja stanów węzła Systemu IIP i wykrywanie anomalii z wykorzystaniem analizy szeregów czasowych ma na celu wykrywanie ataków na mechanizmy umożliwiające wirtualizację zasobów w Systemie IIP. Potencjalnymi atakami tej kategorii, które mogą być wykryte przez LAD są ataki typu przejęcie systemu gościa, atak na dostępność usług realizowane poprzez systemy goszczące lub bezpośrednio przeciw systemowi umożliwiającemu wirtualizację.

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 poprawno-

ści 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 [13, 14].

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 [15], por. rysunek 5. Jego podstawowym założeniem jest dwustopniowa ocena węzłów w ustalonych chwilach $n = 1, 2, ...$ 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 (n oznacza numer okresu obserwacji) dostarczonych przez inne moduły (HMAC, LAD).

Ocena ryzyka I_n^l incydentu o identyfikatorze l obliczana jest jako $I_n^l = c_l \times p_n^l$, gdzie $c_l \in [0, 1]$ oznacza koszt incydentu (severity) a p_n^l prawdopodobieństwo (probability), że ten incydent rzeczywiście wystąpił. Przyjęto, że węzeł gromadzi informację o każdym z sąsiadów z okresie n i oblicza zaufanie do każdego z nich według nastepujących wzorów:

$$\begin{aligned} \check{I}_n &= \max_l \big(c_l \times p_n^l\big), \\ k &= \#\big(I_n^l : I^l{}_n > \frac{1}{2}\check{I}_n\big), \\ I_n &= \check{I}_n + \big(1 - \check{I}_n\big) \times \big(1 - a^{-(k-1)}\big), \\ T_n &= 1 - I_n, \end{aligned} \tag{1}$$

gdzie a jest stałą wyznaczaną emiprycznie. Przyjęto taki model zaufania, aby rownoczesnie uwzględnic decydujący wpływ na zaufanie incydentu o największym ryzyku oraz, jeżeli występują, licznych incydentów o ryzyku znaczącym. W kolejnym kroku węzeł o numerze i przesyła informację o zaufaniu do węzla j odpowiednio ją oznaczając, $T_n^{i,j} = T_n$. Na podstawie informacji zebranych od wszystkich sąsiadów agent centralny oblicza skumulowane zaufanie do węzła j w ocenianym okresie obserwacji n według wzoru:

$$T_n^j = \frac{\sum_{i \in A_j} T_n^{i,j} R_n^i}{\sum_{i \in A_j} R_n^i}, \tag{2}$$

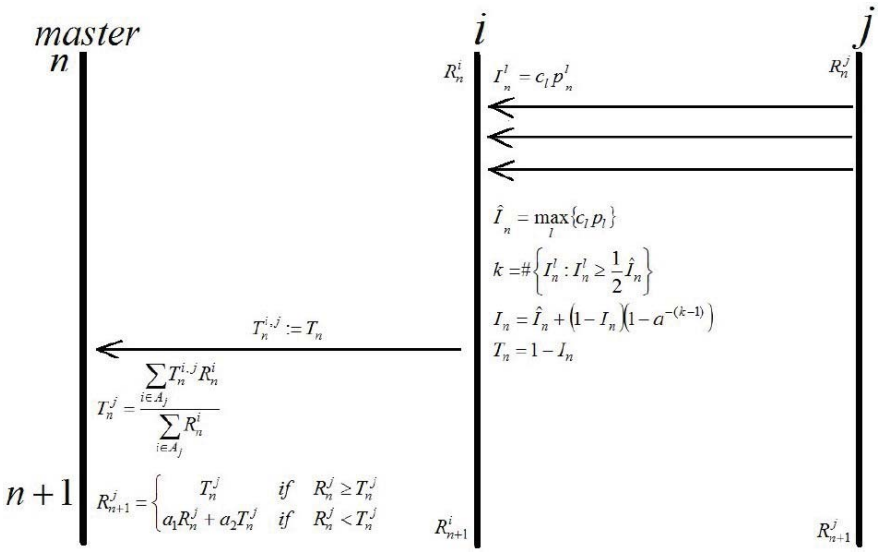
gdzie

- A_j jest zbiorem węzłów sąsiadujących z węzłem j i oceniających go,
- R_n^j jest reputacją węzła j w analizowanym okresie[6] n.

Reputacja R_{n+1}^j węzła j w kolejnej chwili $n+1$ jest obliczana na podstawie skumulowanej informacji o zaufaniu T_n^j do tego węzła, obliczonej centralnie na podstawie danych o zaufaniu $T_n^{i,j}$ dostarczonych przez jego sąsiadów, z uwzględnieniem reputacji tych sąsiadów R_n^i i wartości reputacji ocenianego węzła R_n^j. Przyjęto, że reputacja w kolejnej chwili ma wartość:

$$R_{n+1}^j = \begin{cases} T_n^j, & \text{jeżeli } R_n^j \geqslant T_n^j, \\ a_1 R_n^j + a_2 T_n^j, & \text{jeżeli } R_n^j < T_n^j, \end{cases} \tag{3}$$

gdzie stałe $0 < a_1, a_2 < 1$, $a_1 + a_2 = 1$ są dobrane eksperymantalnie. Taka postac wyrazenia dla reputacji sprawia, że reputacja zaatakowanego węzła zmniejsza się szybko, a w czasie jego poprawnej pracy odbudowywana jest powoli.



Rysunek 5. Przykład sposobu obliczania reputacji węzłów

Przedstawione powyżej podejście do oceny sieci komunikujących się wezłów za pomocą systemu reputacyjnego zakłada ocenę danego węzła przez jego sąsiadów na podstawie obserwacji ruchu nadchodzącego do nich od ocenianego węzła. Ocena taka nie jest wystarczająca, jeżeli chcemy uwzględniać w ocenie również

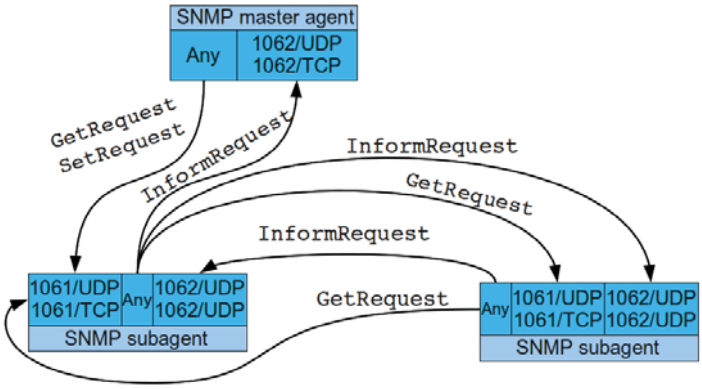
[6] W chwili rozpoczynania obliczeń przyjmujemy reputację węzłów jako 1.

wewnętrzne parametry węzła, takie jak obciążenie procesora, zajętość pamięci operacyjnej czy wykorzystanie pamięci masowej. W takiej sytuacji lokalny agent bezpieczeństwa powinien oceniać działanie swojego węzła obliczając w każdym cyklu obserwacji własną ocenę zaufania do węzła T_n^{*j} w sposób analogiczny do oceny węzła sąsiedniego, por. (1). Skumulowane zaufanie do węzła j ma w takim rozbudowanym modelu zaufania następującą postać:

$$T_n^j = \frac{\sum_{i \in A_j} T_n^{i,j} \times R_n^i + T_n^{*j} \times R_n^j}{\sum_{i \in A_j} R_n^i + R_n^j}. \tag{4}$$

Przesyłanie komunikatów o zaufaniu i sposób obliczenia reputacji są takie jak w poprzednim przypadku, podanym we wzorze (3).

Jako protokół komunikacyjny dla zarządzania reputacją wybrano SNMPv3, który pracuje jako scentralizowany system agentowy w paradygmacie klient-serwer, por. rysunek 6, ponadto ma możliwość bezpiecznej komunikacji między agentami. Protokół zapewnie poufność, integralność oraz świeżość danych [16] jak również zaawansowaną kontrolę dostępu dla użytkowników [17]. 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,



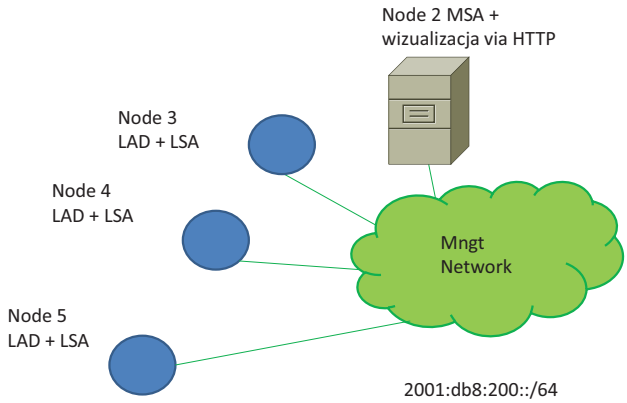
Rysunek 6. Schemat komunikacji agentów protokołu SNMP dla zarządzania reputacja

stanowiąc odrębny moduł programowy. Umożliwia to niezależną aktualizację obu systemów agentowych. Protokół SNMP wykorzystuje bazę danych MIB [18], 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 zarządza-

nia Systemu IIP poprzez dostęp do odpowiednich MIB master agenta SNMP i lokalnych agentów SNMP.

6 Eksperymenty

W ramach pierwszego etapu implementacji powstały prototypy modułu LAD, LSA i MSA. Główny nacisk został położony na implementację interfejsów pomiędzy modułami, z uproszczonymi algorytmami wykrywania anomalii (moduł LAD) czy możliwościami dynamicznej konfiguracji liczby i adresów węzłów (moduły LSA, MSA). Uproszczone na tym etapie implementacji elementy będą rozwijane w ramach dalszych prac nad projektem. Powstałe oprogramowanie zostało zintegrowane w sieci testowej grupy bezpieczeństwa na Politechnice Warszawskiej. Na potrzeby eksperymentów zostały uruchomione w środowisku Xen cztery maszyny wirtualne, reprezentujące cztery węzły systemy IIP. Wszystkie elementy komunikowały się jedynie za pomocą protokołu IPv6, wykorzystując adresy z prefixem 2001:db8:200::/64. Na rysunku 7 znajduje się logiczna topologia sieci testowej. Na węźle o nazwie Node 2 uruchomiony został moduł MSA oraz moduł wizualizacji poziomu zaufania. Na pozostałych trzech węzłach o nazwach Node 3, Node 4 i Node 5 uruchomione zostały moduły LAD i LSA.



Rysunek 7. Schemat topologii sieci testowej w której były przeprowadzano eksperymenty

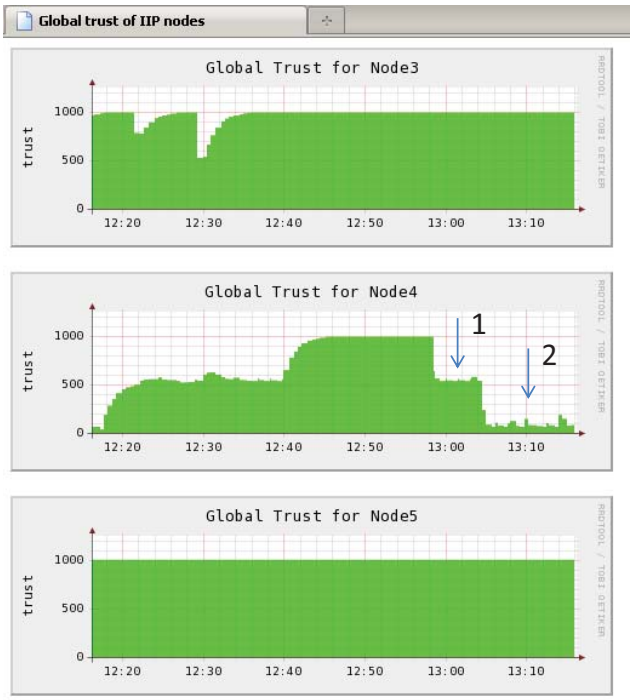
Na potrzeby testów komunikacji między modułami i wyliczania poziomu zaufania analizowane były jedynie zdarzenia SRE związane z naruszeniem polityki bezpieczeństwa w sieci zarządzania. Zdarzenia te były generowane i wysyłane

do podsystemy syslog bezpośrednio przez zaporę ogniową systemu Linux skonfigurowaną za pomocą programu *ip6tables*. Eksperymenty bazowały na danych uzyskiwanych w czasie rzeczywistym. Do symulacji ataków były wykorzystane standardowe narzędzia administracyjne ping6 oraz nmap, które mogą posłużyć do przeprowadzenia wstępnej fazy rozpoznania rzeczywistych ataków. Wynikiem eksperymentów był obliczony przez MSA globalny poziom zaufania do poszczególnych węzłów – liczba z zakresu $0 \ldots 1000$ (jest to przeskalowana reputacja, oryginalnie przyjmująca wartości z zakresu $0 \ldots 1$). Podczas eksperymentów wartość kluczowych parametrów wzorów (1) i (3) przyjmowały wartości $a = 4$, $a_1 = 0,7$ oraz $a_2 = 0,3$. Przeprowadzane w czasie rzeczywistym ataki powodowały zgłaszanie do systemu reputacji anomalii o parametrach *severity* $c_l = 0,15$, *probability* $p_n^l = 0,7$ dla *ping6* oraz *severity* $c_l = 1$ i *probability* $p_n^l = 1$ dla *nmap*.

Wyliczony przez MSA poziom zaufania do poszczególnych węzłów był wizualizowany w czasie rzeczywistym. Poniżej znajdują się przykładowe wykresy poziomu globalnego zaufania dla węzłów uzyskane podczas eksperymentów wraz z komentarzem opisującym przebieg eksperymentu. Na rysunku 6 przedstawiony jest wpływ liczby węzłów raportujących anomalie dotyczącą wybranego węzła, na uzyskany globalny poziom reputacji. Podczas tego eksperymentu węzeł Node 4 rozpoczął skanowanie węzła Node 3. Wywołało to spadek jego globalnego zaufania do poziomu bliskiego 500. Sytuacja ta jest widoczna na drugim wykresie i oznaczona strzałką z numerem 1. W momencie kiedy z węzła Node 4 rozpoczęto skanowanie kolejne węzła (Node 5) jego reputacja spadła do poziomu bliskiego 0, co zaznaczone jest strzałką z numerem 2. Eksperyment ten potwierdza wpływ liczby raportujących węzłów na globalny poziom zaufania. W realnym systemie odzwierciedla to sytuację kiedy jeden z węzłów rozpoczyna ataki na wiele innych węzłów. Wykrycie tego faktu, poprzez raporty od wielu maszyn, znacznie obniża reputację atakującego. Drugi eksperyment miał na celu potwierdzenie wpływu globalnego zaufania węzła raportującego anomalię do zmiany poziomu zaufania podejrzanej maszyny. Podczas tego eksperymentu z węzła Node 3 wykonywano dwa skanowania z wykorzystaniem programu nmap: systemu który ma zaufanie 1000 oraz systemu o zaufaniu bliskim 0. Na rysunku 6 strzałka z numerem 1 pokazuje sytuację kiedy anomalie dotyczące węzła atakującego są zgłaszane przez węzeł o minimalnym zaufaniu (Node 4). W takim przypadku globalne zaufanie do atakującego zostaje zmniejszone minimalnie. Zupełnie inne efekt obserwujemy, gdy raport na temat anomalii został wygenerowany przez zaufaną stację (Node 5). W takim przypadku spadek zaufania potencjalnego atakującego jest bardzo istotny. Taką sytuację wskazuje strzałka z numerem 2.

7 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 wy-

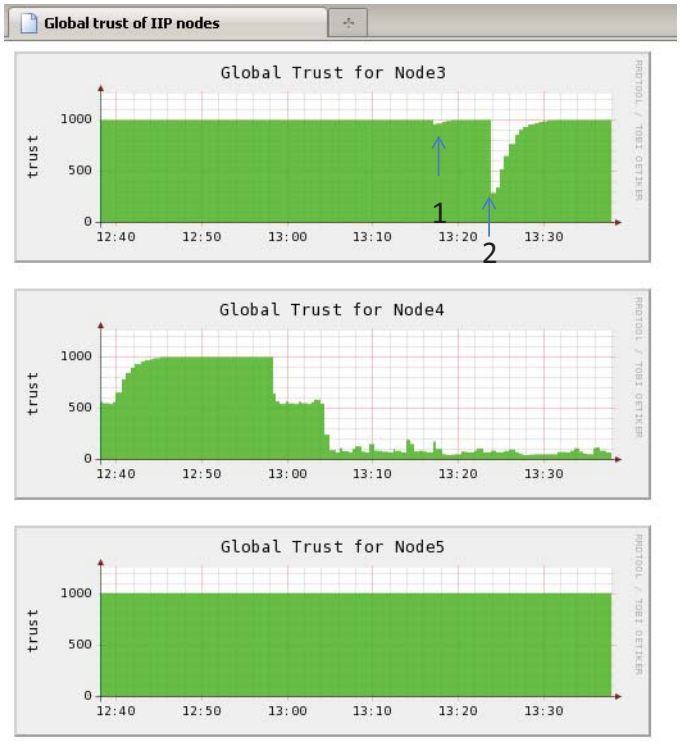


Rysunek 8. Wpływ liczby węzłów raportujących anomalie na poziom globalnego zaufania atakującego

krywaniu 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. 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.
2. `https://www.iip.net.pl/`
3. A. Gavras et al., "Future Internet Research and Experimentation: The FIRE Initiative", ACM SIGCOMM Computer Communication Review, 37, 3, July 2007.



Rysunek 9. Wpływ reputacji węzła raportującego anomalie na poziom globalnego zaufania atakującego

4. "Future Internet - Strategic Research Agenda", ver. 1.1, FI X-ETP Group, January 2010.
5. M. Soellner, "The 4WARD Approach to Future Internet", ITG FG 5.2.3 Meeting Eschborn, 2010.
6. `http://www.syssec-project.eu/`
7. `http://www.nessos-project.eu/`
8. `http://www.effectsplus.eu/`
9. M. Castrucci, F. Delli Priscoli, A. Pietrabissa, and V. Suraci, "A Cognitive Future Internet Architecture", J. Domingue et al. (Eds.): Future Internet Assembly, LNCS 6656, pp. 91-102, 2011.
10. RFC 2104, "HMAC: Keyed-Hashing for Message Authentication", IETF 02.1997.
11. R. Agrawal, R. Srikant, "Fast algorithm for mining association rules", In: J.B. Bocca, M. Jarke, and C.Zaniolo, editors. Proceedings of 20th International Conference on Very Large Databases, pp. 487-499, (1994).
12. 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

13. 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.
14. 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.
15. T. Ciszkowski, W. Mazurczyk, Z. Kotulski, T. Hossfeld, M. Fiedler, D. Collange, "Towards Quality of Experience-based reputation models for future web service provisioning", Telecommunication Systems, DOI: 10.1007/s11235-011-9435-2.
16. RFC 5591, "Transport Security Model for the Simple Network Management Protocol (SNMP)", IETF 06.2009.
17. RFC 3415, "View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)", IETF 12.2002.
18. RFC 3418, "Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)", IETF 12.2002.