SYSTEM OCHRONY SIECI TELEINFORMATYCZNYCH PRZED DZIAŁANIAMI NIEUPRAWNIONYMI SOPAS

mjr mgr inż. Bartosz JASIUL
dr inż. Rafał PIOTROWSKI
WOJSKOWY INSTYTUT ŁĄCZNOŚCI
ul. Warszawska 22A
05-130 Zegrze

Streszczenie artykułu

Artykuł przedstawia prototyp opracowywanego w Wojskowym Instytucie Łączności Systemu Ochrony Przed Atakami Sieciowymi SOPAS. W artykule opisano architekturę systemu, jego główne komponenty oraz przykładowe scenariusze wykrywania ataków.

Wstęp

Doświadczenia ostatniej dekady wskazują, że charakter działań terrorystycznych zmienił się zasadniczo. Poza typowymi działaniami zbrojnymi prowadzonymi na lądzie, morzu i w powietrzu pojawił się kolejny wymiar przestrzeni walki w postaci ataków na sieci teleinformatyczne. Celem tych ataków są zarówno zasoby informacyjne, które mogą być przez atakującego przechwycone, zmodyfikowane lub zniszczone, jak również infrastruktura sieci teleinformatycznych. Zasoby tej infrastruktury są najczęściej blokowane, co w efekcie prowadzi do „paraliżu komunikacyjnego" i braku możliwości przesyłania jakichkolwiek informacji. Ogromny potencjał atakujących został zidentyfikowany na podstawie skutków zmasowanych ataków na sieci teleinformatyczne Estonii i Gruzji przeprowadzonych na tle politycznym. W mniejszym stopniu atak był odczuwalny w Polsce po niezadowoleniu z podpisania porozumienia ACTA. Niemniej działania grup hakerów wskazują, że nowy wymiar niepożądanych incydentów sieciowych jest najczęściej narzędziem wspierającym działania polityczne, gospodarcze, militarne i terrorystyczne. Z tego też powodu niektóre państwa (np. Francja, Chiny) zmieniły już swoją strategię bezpieczeństwa i zakładają prowadzenie aktywnych działań w postaci ataków na systemy teleinformatyczne swoich przeciwników.

Niniejszy artykuł poświęcony jest przeciwdziałaniu atakom cybernetycznym, a dokładniej opracowywanemu w Wojskowym Instytucie Łączności w Zegrzu Systemowi Ochrony Przed Atakami Sieciowymi SOPAS. W dalszych częściach artykułu znajdują się opis architektury prototypu systemu SOPAS, sposób wykrywania działań nieuprawnionych i elementy sensoryczne, struktura reguł decyzyjnych, informacje wymieniane o atakach z innymi systemami oraz sposoby reakcji na wybrane typy ataków. W podsumowaniu ujęte zostały planowane prace oraz informacje o przygotowaniach do weryfikacji systemu podczas ćwiczeń CWIX 2012.

Założenia na system

Opracowywany w Wojskowym Instytucie Łączności w Zegrzu, we współpracy z Naukową i Akademicką Siecią Komputerową oraz ITTI sp. z o.o., prototyp systemu SOPAS jest odpowiedzią na rosnące potrzeby ochrony wojskowych i rządowych sieci teleinformatycznych w zakresie wykrywania, przeciwdziałania i eliminowania ataków cybernetycznych. Prowadzony w WIŁ projekt zakładał wypełnienie potrzeb zidentyfikowanych w "Rządowym programie ochrony cyberprzestrzeni RP na lata 2009-2011" [1] w postaci: zapobiegania skutkom działań niepożądanych w sieciach państwowych i publicznych, kształcenia specjalistów z dziedziny bezpieczeństwa teleinformatycznego, współpracy z producentami sprzętowych i programowych zabezpieczeń, wspólnego prowadzenia badań naukowych nad bezpieczeństwem teleinformatycznym przez podmioty wywodzące się ze sfery administracji publicznej, ośrodki naukowe oraz inne instytucje dysponujące elementami krytycznej infrastruktury teleinformatycznej państwa.

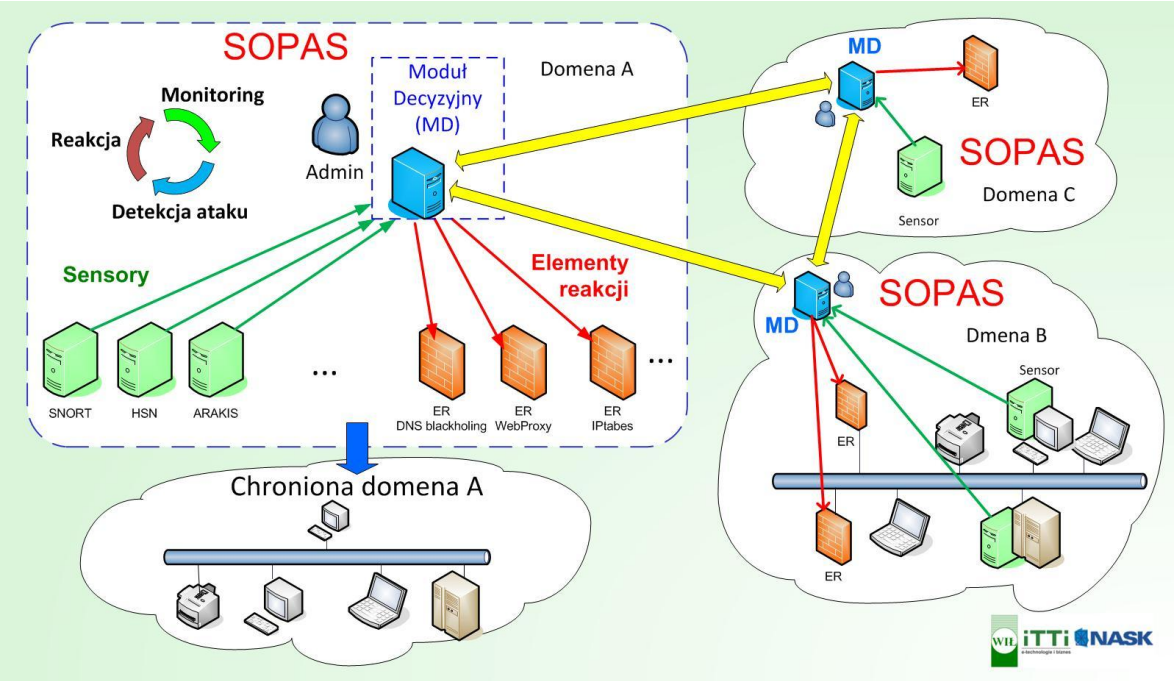
Podstawowym wymogiem do realizacji prototypu SOPAS było przyjęcie założenia, że w maksymalnym stopniu zostaną wykorzystane istniejące już mechanizmy zapewnienia bezpieczeństwa cybernetycznego oraz zostaną opracowane nowe metody wykrywania i reagowania na ataki. Zastosowanie istniejących już mechanizmów bezpieczeństwa miało na celu, oprócz wzmocnienia skuteczności ochrony sieci teleinformatycznych, wykorzystanie zakupionych już urządzeń i aplikacji w organizacjach, w których system SOPAS miałby być docelowo wdrażany. System SOPAS integrowałby zatem sensory i elementy reakcji oraz dostarczałby innowacyjnych rozwiązań zapewniających skuteczną ochronę przed zagrożeniami sieciowymi.

Dodatkowym założeniem przyjętym podczas projektowania systemu było ustalenie komunikacji pomiędzy systemami współpracującymi, mającej na celu wymianę informacji o symptomach, atakach i skutecznych metodach ochrony. Założenie to miało skutkować osiągnięciem znacznego przyrostu wykrytych ataków oraz skutecznym aplikowaniem mechanizmów reakcji. W konsekwencji współdzielenie informacji o sposobach reagowania i wykrywania ataków miało prowadzić do uzyskania efektu synergii, a zaobserwowane symptomy w innych systemach mogły być przydatne do zidentyfikowania ataków we własnej domenie. Takie współdzielenie informacji pozwala na osiągnięcie wysokiego poziomu bezpieczeństwa, który nie mógłby być osiągnięty przez system działający samodzielnie.

Architektura systemu SOPAS

System SOPAS ma budowę modularną, która pozwala na dodawanie kolejnych elementów bez konieczności ingerencji w pozostałe komponenty systemu. Głównymi elementami systemu SOPAS są Elementy Sensoryczne (ES), Elementy Reakcji (ER) oraz Moduł Decyzyjny (MD) [Rys.1].

Elementy Sensoryczne to urządzenia lub aplikacje zdolne do wykrywania w ruchu sieciowym symptomów zdarzeń, które zazwyczaj prowadzą do wykrycia działań niepożądanych. W prototypie systemu SOPAS zastosowano sensory takie jak np. Arakis, HSN oraz opracowano własny mechanizm detekcji - SOPAS sensor. ARAKIS [2] to system wczesnego ostrzegania bazujący na serwerowych pułapkach (ang. server-side honeypots). Pozwala on na wykrycie ataków poprzedzanych skanowaniem sieci w celu poszukiwania luk lub błędów zabezpieczeń. HSN [2] to system aktywnego poszukiwania zagrożeń w Internecie (HTTP/HTTPS/FTP itp.) bazujący na klienckich pułapkach (ang. client-side honeypots). Zadaniem sensora HSN jest aktywne przeszukiwanie sieci celem identyfikacji zasobów, które mogą powodować infekcję chronionego systemu teleinformatycznego. SOPAS Sensor to z kolei system wykrywania zagrożeń na bazie analizy danych z warstw 3, 4, 5 i 7 modelu OSI. Pozwala on na zidentyfikowanie anomalii, które wskazują na prowadzenie działań niepożądanych przez określonych użytkowników.

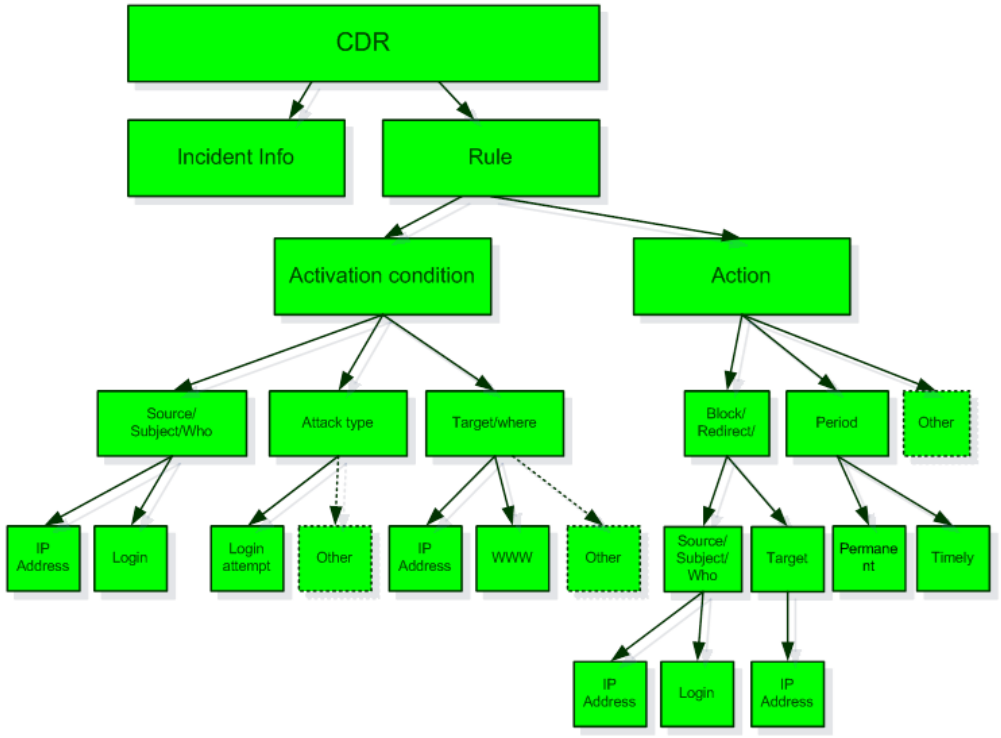


Rys. 1 Architektura systemu SOPAS

Zastosowane mechanizmy prewencji ER to szeroka gama działań reakcji na wykryte ataki. ER pozwalają na unikanie sytuacji alarmowych w przypadku wykrycia zbioru symptomów ataku lub też powodują szybką reakcję na wykryte działanie niepożądane. W obecnej wersji prototypu SOPAS głównym mechanizmem reakcji jest odcięcie od sieci źródła niebezpiecznego zachowania w miejscu jak najbliższym jego fizycznego przyłączenia do sieci. Do standardowych mechanizmów reakcji w zrealizowanym prototypie SOPAS należą między innymi IP-tables, DNS-blackholing, itp.

Zarówno ES oraz ER są sterowane i kontrolowane przez Moduł Decyzyjny. MD to centralny element systemu SOPAS, który analizuje wykryte zdarzenia przez ES oraz określa jakie reakcje mają być zastosowane wobec zaistniałego incydentu. Reguła decyzyjna wypracowana przez MD jest dostarczana do ER, które podejmują działania wobec wykrytych zagrożeń zgodnie z zapisami otrzymanego polecenia, zwanego Ogólną Regułą Decyzyjną (ORD), której schemat został przedstawiony na rysunku Rys. 2. Moduł decyzyjny posiada możliwość wykrywania ataków i zagrożeń dzięki opracowanemu i zaimplementowanemu mechanizmowi semantycznego wnioskowania bazującego na ontologii. Opracowana w prototypie SOPAS ontologia opisuje zbiór wybranych ataków i mechanizmów reakcji. Natomiast mechanizm wnioskowania przypisuje zaobserwowane zdarzenia do bazy wiedzy zgromadzonej w ontologii. Pozwala to na osiągnięcie sposobu podejmowania decyzji zbliżonego do reakcji człowieka specjalizującego się w

wykrywaniu ataków. Znaczącą różnicą na korzyść SOPAS jest szybkość reakcji i jego zautomatyzowane działanie. Istotną zaletą systemu SOPAS jest jednoczesne zastosowanie zaawansowanych metod pozyskiwania danych z sensorów, metod wnioskowania oraz korelacji symptomów na podstawie ontologii, które pozwalają na skuteczne wykrywanie anomalii, działań niepożądanych oraz ataków zarówno tych, których sygnatury są znane, jak również tych, które jeszcze nie zostały wcześniej zarejestrowane (ang. 0-day attacks).



Rys. 2 Schemat Ogólnej Reguły Decyzyjnej - ORD

Ontologia systemu SOPAS

Ontologia jest modelem danych, opisującym klasyfikacje pojęć, ich właściwości, relacje pomiędzy nimi i ich uszczegółowienia. Ontologia daje również możliwość nakładania ograniczeń, restrykcji, jak również reguł dla danej dziedziny i jej pojęć.

Jedna z formalnych definicji [3] przedstawia, iż „ontologia definiuje podstawowe terminy i relacje tworzące słownik danego obszaru tematycznego, jak również zasady dotyczące łączenia terminów i relacji do zdefiniowania poszerzania słownictwa".

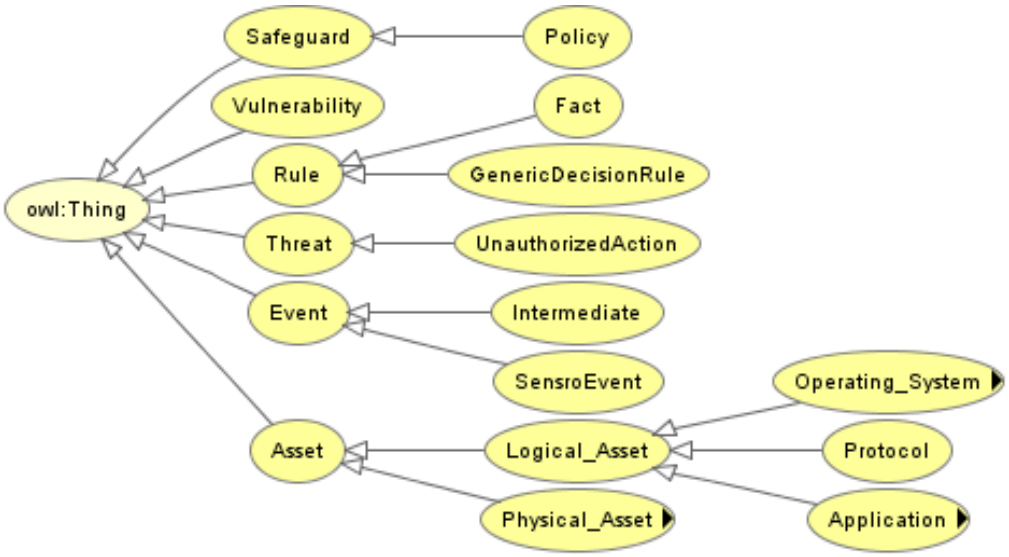
Ontologia jest rodzajem bazy wiedzy, która modeluje określoną dziedzinę. Ontologia zagrożeń projektu SOPAS opisuje dziedzinę bezpieczeństwa sieci komputerowych. Ontologia SOPAS jest oparta na standardzie ISO/IEC 13335-1:2004

(Information technology — Guidelines for the management of IT Security) [4] dotyczącym zarządzania bezpieczeństwem technologii informacyjnych.
Standard definiuje poszczególne zagadnienia:

- Zasoby – wszystko co ma wartość dla organizacji.
- Zagrożenia – potencjalne przyczyny incydentów, które mogą powodować szkodę dla systemu i/lub organizacji.
- Podatności – słabe strony zasobów lub grup zasobów, które mogą być wykorzystane przez zagrożenia.
- Środki zaradcze – praktyki, procedury lub mechanizmy które redukują podatności.

Na rysunku Rys. 3 przedstawiono główne klasy ontologii. Strzałki z pustym grotem przedstawiają relację dziedziczenia (ang. subclassOf). Żółte elipsy przedstawiają klasę. Klasa o nazwie owl:Thing jest abstrakcyjną klasą bazową, z której dziedziczą pozostałe klasy. Dla poprawienia czytelności, każda z klas posiadająca na rysunku czarny grot strzałki skierowany w prawą stronę, zawiera podklasy z niej dziedziczące.
Głównymi klasami prototypu SOPAS są:

- Asset (Zasób sieciowy),
- Event (Zdarzenie Sieciowe),
- Safeguard (Zabezpieczenia),
- Threat (Zagrożenia),
- Vulnerability (Podatność),
- Rule (Reguła).



Rys. 3 Główne klasy ontologii SOPAS.

Przykładowe ataki i metody wykrywania

W niniejszym rozdziale przedstawione zostały jedynie podstawowe typy ataków i ogólny opis ich wykrywania, ze względu na poufny charakter rozwiązań z tej dziedziny. Ujawnienie dokładnego sposobu wykrywania ataków i metod reagowania na nie może prowadzić do powstawania dedykowanych ataków, które będą miały możliwość ominięcia zabezpieczeń albo będą wykorzystywały podatności proponowanego rozwiązania. Dla wybranych ataków opisano także przykładowe mechanizmy przeciwdziałania. Głównym elementem wspierającym wykrywanie działań niepożądanych – oprócz sensorów systemu SOPAS – jest ontologia wraz z mechanizmami wnioskowania. Zaletą zastosowania ontologii jest identyfikacja odpowiednich mechanizmów reakcji dla powstałego ryzyka utraty zasobów na skutek przeprowadzonego ataku.

Wykrywanie ataku „malware infection"

„Malware infection" to działanie nieuprawnione spowodowane przez zainfekowaną maszynę znajdującą się w obszarze sieci chronionej przez system SOPAS. Infekcje wykrywane mogą być zarówno przez systemy pułapek (Honeynet) jak i przez analizę połączeń odrzuconych przez systemy Firewall. Oba z tych źródeł analizowane są przez system ARAKIS, który przy wykryciu połączeń nieuprawnionych informuje Administratora domeny, z której połączenia nastąpiły o zaistniałej sytuacji oraz blokowane są pakiety z zasobu sieciowego, na którym wykryto złośliwe oprogramowanie.

Wykrywanie ataku „reverse shell"

Shellcode to niskopoziomowy program, najczęściej w postaci kodu maszynowego, odpowiedzialny za wywołanie powłoki systemowej. Używany zwykle w ostatniej fazie przełamywania wielu błędów zabezpieczeń. Atak typu „reverse shell" polega na wstrzyknięciu do atakowanej domeny implementacji „shellcode" a następnie uruchomienie jej przez atakującego, dzięki czemu atakujący uzyskuje powłokę z uprawnieniami administratora. W przypadku wykrycia przez sensor złośliwego oprogramowania (ang. malware) administrator zostaje powiadomiony o wykryciu podejrzanego kodu. Kiedy z analizatora logów zostanie dostarczona zostanie informacja, z którego adresu wstrzyknięto podejrzane oprogramowanie, administrator jest ostrzegany o tym zdarzeniu. W przypadku kolejnego ostrzeżenia z analizatora ruchu o wykryciu, iż z określonej lokalizacji uruchomiono podejrzany kod stosowane są następujące mechanizmy reakcji –

powiadamiani są administratorzy obu domen (chronionej oraz z tej, z której wykryto działanie nieuprawnione) oraz blokowane są pakiety z zasobu sieciowego, z którego przeprowadzany jest atak.

Wykrywanie ataku „password guessing"

Atak typu „password guessing" polega na zgadywaniu hasła dostępu do udostępnianych usług lub serwerów WWW/FTP/SQL. Najczęściej przeprowadzany jest ten atak metodą słownikową poprzez dopasowanie hasła poprzez konkatenację słów lub ich fragmentów (np. „myDeskRoom10" lub „CompLenoDvd"). Często atak ten przeprowadzany jest także przy pomocy tęczowych tablic (ang. rainbow tables). Używa się do tego celu bazy skrótów popularnych funkcji jednokierunkowych (MD5, SHA-1). Umożliwia to atakującemu na zaoszczędzeniu mocy obliczeniowej koniecznej do złamania hasła metodą słownikową czy też retrospektywnego przeszukiwania (ang. brute force). Zwykłe bazy haseł słownikowych zajmują setki gigabajtów przez co są nieefektywne. W tęczowych tablicach z kolei zapisywane są skróty możliwych haseł przez co zapisywany jest jeden skrót na kilkaset, a nawet kilka tysięcy wygenerowanych haseł, a baza danych pozwala na odwrócenie skrótu w około 90% przypadków. Skraca się przez to czas łamania hasła do określonego zasobu. W przypadku wykrycia przez sensor systemu SOPAS próby wielokrotnego wywołania z odmiennym hasłem chronionego zasobu systemu, administrator tego systemu jest powiadamiany o wykryciu podejrzanego zachowania jednego z użytkowników domeny własnej lub obcej. Kiedy z analizatora logów zostanie dostarczona informacja, że intensywność (częstotliwość) wywołań usługi jest bardzo wysoka to firewall lub lub inny ER otrzymają regułę blokowania pakietów z określonego adresu IP.

Podsumowanie

System SOPAS pozwala na poprawę bezpieczeństwa typowej domeny posiadającej standardowe zabezpieczenia w postaci komercyjnych narzędzi typu firewall, IDS (Intrusion Detection System), itp. System SOPAS może być też zastosowany w całości w domenie, która w ogóle nie posiada zabezpieczeń, a sensory oraz mechanizmy reakcji dostarczone zostaną wraz z wdrażanym systemem.

Opracowany prototyp SOPAS umożliwia współdzielenie informacji pomiędzy chronionymi, równoprawnymi domenami, co poprawia ich odporność na ataki. Jest to

rozwiązanie oryginalne, które umożliwia osiągnięcie dodatkowego zabezpieczenia sieci w oparciu o informacje o wykrytych atakach pozyskiwane ze współpracujących domen/systemów. Otrzymane informacje mogą być wykorzystane przez administratorów w procesie podejmowania decyzji o przeciwdziałaniu atakom i minimalizowaniu ich skutków. Ponadto zautomatyzowanie procesu wykrywania ataków sieciowych oraz reakcji na nie pozwala na odciążenie administratorów chronionych sieci. Dodatkowo analiza zdarzeń pochodzących z różnych części sieci umożliwia również rozpoznanie ataków rozproszonych.

Prototyp systemu SOPAS będzie testowany podczas ćwiczeń NATO CWIX 2012. Będzie to pierwszy narodowy system ochrony przed cyberatakami demonstrowany w środowisku NATO CWIX. Dalszy rozwój prototypu systemu SOPAS umożliwi jego testy w środowisku operacyjnym, a w konsekwencji wdrożenie go w resortowych systemach teleinformatycznych.

Literatura

[1] Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011, marzec 2009, Warszawa

[2] http://www.cert.pl/projekty

[3] Neches R., Fikes R., Finin T., Gruber T., Patil R., Senator T., Swartout W.R., Enabling Technology for Knowledge Sharing , AI Magazine, No 12(3), 36-56, 1991.

[4] Information technology — Guidelines for the management of IT Security Part 1: Concepts and models for IT Security, ISO/IEC, TR 13335-1, 1996.