Autoreferat

Bogdan Księżopolski

25 sierpnia 2015

Spis treści

1 Imię i nazwisko

Bogdan Księżopolski

2 Posiadane dyplomy, stopnie

Magistra: Wydział Matematyki, Fizyki i Informatyki, Uniwersytet Marii Curie-Skłodowskiej, Lublin, czerwiec 2002

Doktora: Wydział Informatyki, Polsko-Japońska Wyższa Szkoła Technik Komputerowych, Warszawa, grudzień 2006

3 Informacje o dotychczasowym zatrudnieniu

2012 - obecnie - adiunkt, Katedra Sieci Komputerowych, Wydział Informatyki, Polsko-Japońska Akademia Technik Komputerowych w Warszawie

2007- obecnie - adiunkt, Zakład Układów Złożonych i Neurodynamiki, Instytut Informatyki, Uniwersytet Marii Curie-Skłodowskiej w Lublinie

2005-2007 - asystent, Zakład Układów Złożonych, Instytut Informatyki, Uniwersytet Marii Curie-Skłodowskiej w Lublinie

2001-2005 - administrator systemów i sieci komputerowej, Katedra Fizyki Teoretycznej, Uniwersytet Marii Curie-Skłodowskiej w Lublinie

4 Wskazanie osiągnięcia wynikającego z art. 16 ust. 2 ustawy z dnia 14 marca 2003 r. o stopniach naukowych i tytule naukowym oraz o stopniach i tytule w zakresie sztuki

4.1 Tytuł osiągnięcia naukowego (jednotematyczny cykl publikacji)

Wieloaspektowe modelowanie systemów bezpieczeństwa za pomocą języka QoP-ML.

4.2 Wykaz monotematycznych publikacji wchodzących w skład osiągnięcia naukowego z wykazaniem procentowego udziału współautorów

[A] **B. Księżopolski** [100%], *QoP-ML: Quality of Protection modeling language for cryptographic protocols*, Elsevier: Computers & Security 31(4), 2012, s.569-596 (IF=1,158).

[B] **B. Księżopolski** [65%], D. Rusinek [20%], A. Wierzbicki [15%], *On the efficiency modeling of cryptographic protocols by means of the Quality of Protection Modelling Language (QoP-ML)*, AsiaARES 2013, Yogyakarta, Indonesia, LNCS, v. 7804, s.261-270, 2013.

[C] **B. Księżopolski** [45%], T. Żurek [45%], M. Mokkas [10%], *Quality of Protection evaluation of security mechanisms*, The Scientific World Journal, s.1-18, 2014 (IF=1,219).

[D] K. Mazur [45%], **B. Księżopolski** [40%], Z. Kotulski [15%], *The robust measurement method for security metrics generation*, The Computer Journal, Oxford University Press, 2014, w druku (IF=0,888).

[E] D. Rusinek [45%], **B. Księżopolski** [40%], A. Wierzbicki [15%],*Security trade-off and energy efficiency analysis in Wireless Sensor Networks*, International Journal of Distributed Sensor Networks, s.1-17, 2015 (IF=0,665).

[F] **B. Księżopolski** [65%], D. Rusinek [20%], A. Wierzbicki [15%], *On the modelling of the computer security impact on the reputation systems*, AsiaARES 2014, Bali, Indonesia, LNCS v.8407, s.526-531, 2014.

[G] **B. Księżopolski** [100%], *Multilevel Modeling of secure systems in QoP-ML*, CRC Press, s.1-262, 2015.

4.3 Charakterystyka prac związanych z przedstawionym osiągnięciem

4.3.1 Wprowadzenie

Obecnie zagadnienia związane z bezpieczeństwem systemów w cyberprzestrzeni stają się coraz ważniejsze w projektowaniu systemów informatycznych. Budowanie bezpiecznych systemów jest związane z analizą wielu złożonych elementów, co czyni ten proces zagadnieniem trudnym. Rosnąca złożoność tworzonych systemów informatycznych jest wyzwaniem dla metod pozwalających wykonać taką analizę bezpieczeństwa. Jedną z metod umożliwiającą wykonanie takiej analizy jest wykorzystanie mechanizmów abstrakcji, które pozwalają utworzyć model będący abstrakcyjną reprezentacją rzeczywistości. Formalny model systemu umożliwia przygotowywanie analizy na temat modelowanego systemu, który następnie pozwoli odpowiedzieć na postawione pytania i finalnie rozwiązać złożony problem.

Języki modelowania systemów bezpieczeństwa, pozwalające tworzyć abstrakcyjne modele systemów informatycznych, są aktualnie przedmiotem badań i eksperymentów wielu naukowców. W literaturze można wyodrębnić dwa kierunki badań w tym zakresie [29], pierwszy dotyczy formalnej weryfikacji systemów, a w szczególności protokołów kryptograficznych [2], oraz drugi, który wykorzystuje modelowanie systemów bezpieczeństwa sterowane modelem [6] (ang. model-driven security, MDS). Formalna analiza protokołów dotyczy weryfikacji własności protokołów (np. poufności, integralności, uwierzytelnienia) oraz ich poprawności. Metody formalnej weryfikacji protokołów można podzielić na trzy podstawowe grupy [29]: indukcyjne, dedukcyjne oraz modelowe. Podstawą analizy bezpieczeństwa, wykorzystującą podejście sterowane modelem (MDS), jest utworzenie modelu systemu wraz z elementami odnoszącymi się do jego bezpieczeństwa a następnie jego analizę ze względu na zdefiniowane własności bezpieczeństwa. Taka analiza wykonywana jest często przed jego implementacją, dzięki czemu można wyeliminować luki systemu już w fazie projektowej. Wśród wiodących podejść można wymienić te, które stanowią rozszerzenie standardu UML, czyli SecureUML [23] oraz UMLsec [11].

Wspomniane podejścia posiadają pewne znaczące ograniczenie. Dotyczy ono braku możliwości analizy wpływu zastosowanych środków ochrony informacji na inne parametry określające funkcjonowanie systemu. Tradycyjne podejście zakłada, że w celu realizacji zdefiniowanych własności

dotyczących jego bezpieczeństwa należy stosować środki ochrony informacji na najwyższym możliwym poziomie. Badania naukowe wskazują [46, 45, 17, 18], że takie podejście może prowadzić do zastosowania zawyżonych środków ochrony informacji, co w konsekwencji powoduje nadmierne obciążenie systemu. Problem ten jest szczególnie istotny dla systemów o ograniczonych zasobach, takich jak np. bezprzewodowe sieci sensoryczne, których wydajność i żywotność są czynnikami krytycznymi. Innym przykładem są chmury obliczeniowe, w których można zaobserwować efekt skali. W takich systemach zwiększając nieznacznie wydajność realizowanych tam pojedynczych procesów, uzyskuje się znaczny wzrost wydajności oraz redukcję kosztów.

Kolejnym aspektem związanym ze stosowaniem zawyżonych środków ochrony informacji jest zwiększenie kosztów wdrożenia jak i utrzymania takiego systemu. Jest to spowodowane między innymi tym, że wykonanie każdej operacji kryptograficznej wprowadzającej dodatkowe zabezpieczenie w systemie wiąże się z dodatkowym obciążeniem jednostki obliczeniowej, co bezpośrednio wpływa na zużycie energii elektrycznej i w konsekwencji zwiększa koszty. Dodatkowo warto zauważyć, że każdy zastosowany element ochrony informacji zwiększa złożoność systemu, co zwiększa koszty wdrożenia. Warto wspomnieć o jeszcze jednym efekcie związanym z potencjalnym zawyżonym zużyciem energii elektrycznej przez elementy architektury IT - jest to wpływ na środowisko naturalne (ang. green computing). Oddziaływanie na środowisko, określane wielkością emisji CO_2, jest uzależnione od rodzaju źródeł energii. W przypadku Polski jest to znaczący wpływ, ponieważ udział energetyki opartej na spalaniu węgla jest na wysokim poziomie.

Możliwym rozwiązaniem problemu, związanym ze stosowaniem zawyżonych środków ochrony informacji, jest wprowadzenie rozwiązań wykorzystujących środki ochrony informacji dostosowane do potencjalnych zagrożeń. W literaturze zagadnienie to określane jest terminem jakości zabezpieczeń (ang. Quality of Protection, QoP) [43, 32, 47, 25]. Jest to podzbiór zagadnień związanych z jakością usługi (ang. Quality of Service, QoS), które są wykorzystywane do określenia wydajności systemu lub sieci. Jakość zabezpieczeń reprezentowana jest jako poziom realizacji poszczególnych własności ochrony informacji (np. poufności, integralności, uwierzytelnienia, dostępności).

4.3.2 Omówienie osiągnięcia naukowego

Na przedkładane osiągnięcie składa się zbiór monotematycznych prac dotyczących wieloaspektowego modelowania systemów bezpieczeństwa za pomocą języka QoP-ML (Quality of Protection Modeling Language). Przedstawiony cykl publikacji zawiera cztery artykuły opublikowane w czasopismach z listy Journal Citation Reports (JCR) **[A,C,D,E]**, dwa artykuły wydane w serii wydawniczej LNCS przez wydawnictwo Springer **[B,F]** oraz jedną monografię **[G]**.

Omówienie przedłożonego osiągnięcia składa się z następujących tematów badawczych poruszanych w prezentowanym cyklu prac.

- Język modelowania QoP-ML.
- Model oceniający jakość zastosowanych zabezpieczeń.
- Metodyka wykonywania pomiarów czynników związanych z bezpieczeństwem systemu.

- Metodyka pozwalająca szacować żywotność architektur sieci sensorowych ze względu na zastosowane środki ochrony informacji.
- Analiza bezpieczeństwa systemów reputacyjnych.
- Wieloaspektowa analiza systemów bezpieczeństwa.

Język modelowania QoP-ML

W literaturze [3, 15, 34, 25, 22] zaprezentowano wiele podejść, które dotyczą modelowania systemów bezpieczeństwa z uwzględnieniem jakości zastosowanych zabezpieczeń. Wszystkie te podejścia posiadają dwa podstawowe ograniczenia. Pierwsze z nich dotyczy faktu, że ocena QoP wykonywana jest dla systemów, które reprezentowane są przez nieformalne modele, bez możliwości kontroli spójności oraz poprawności modelowanych procesów komunikacyjnych. Analiza takich modeli nie daje gwarancji, że wszystkie możliwe stany systemu zostały zbadane, co może prowadzić do błędnych wyników. Drugim ograniczeniem jest brak możliwości przeprowadzenia analizy wieloaspektowej. Analiza wieloaspektowa charakteryzuje się dwoma cechami. Pierwsza dotyczy możliwości opisu systemu w taki sposób, że będzie on uwzględniał wiele elementów wpływających na bezpieczeństwo, np. algorytmy kryptograficzne, parametry algorytmów kryptograficznych, protokoły kryptograficzne, zarządzanie kluczami. Druga dotyczy możliwości wykonania wieloaspektowej analizy systemu z punktu widzenia wpływu zastosowanych środków ochrony informacji (QoP) na inne parametry systemu, takie jak jego wydajność, analizy finansowej rozwiązania, czy analizy wpływu na środowisko. Wymienione ograniczenia stały się motywacją do stworzenia nowego języka modelowania uwzględniającego czynnik QoP, który jednocześnie nie posiadałby wspomnianych braków. W pracy **[A]** przedłożonego cyklu publikacji przedstawiono nowy język modelowania QoP-ML, który jest językiem domenowym (ang. Domain-Specific Language) będącym częścią inżynierii sterowanej modelem (ang. Model-Driven Engineering, MDE).

Główne cechy języka modelowania QoP-ML.

1. Pozwala tworzyć modele systemów, a w szczególności protokołów kryptograficznych, zachowując spójność oraz kompletność wykonywanych tam operacji oraz kroków komunikacyjnych.
2. Pozwala określić pełny zbiór operacji wpływających na bezpieczeństwo analizowanego systemu – wieloaspektowa analiza.
3. Pozwala odwzorować operacje, które odwołują się do wszystkich własności/usług bezpieczeństwa.
4. Pozwala wykonać ocenę jakościową (QoP) dla analizowanych systemów.
5. Pozwala wykonać analizę czasową, która jest elementem kluczowym dla oceny wydajności systemów oraz usługi dostępności.

Język QoP-ML wykorzystuje do opisu systemów wysoki poziom abstrakcji, co pozwala skoncentrować się na opisie jakościowym stosowanych środków ochrony oraz ich wpływie na inne

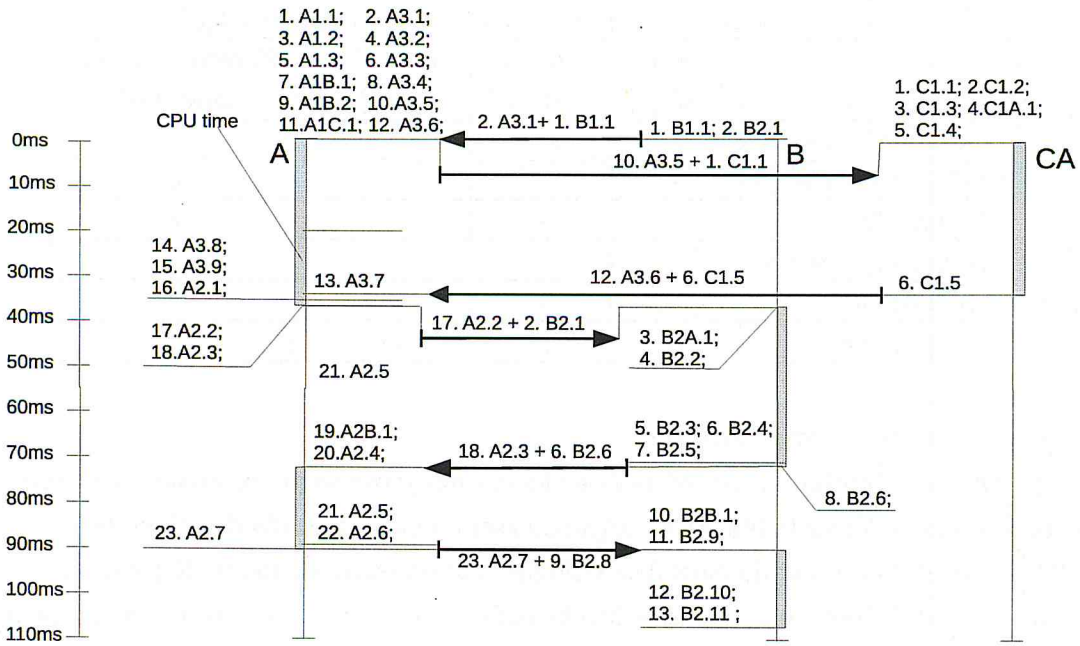
parametry sytemu. Modele utworzone w QoP-ML składają się z: procesów, funkcji, kanałów komunikacyjnych, zmiennych oraz metryk bezpieczeństwa. Procesy są obiektami globalnymi, które są zgrupowane w głównych procesach reprezentujących węzły obliczeniowe (np. komputer, czujnik obliczeniowy, router). Procesy określają zachowanie węzła, które reprezentowane są przez funkcje realizujące zaplanowane operacje. Kanały oraz zmienne opisują warunki, w jakich procesy są realizowane. Składnia podstawowej wersji języka QoP-ML została opisana w standardzie BNF [5] w pracy **[A]**. Podstawowa wersja języka QoP-ML stanowi podstawę dla innych modułów określających dodatkowe parametry analizy. Moduły te dodają nowe elementy do składni języka. Pełna składnia języka została opisana w monografii **[G]**. Semantyka podstawowej wersji języka QoP-ML została opisana w pracy **[A]**, która razem z 11 algorytmami określa działanie poszczególnych elementów.

Istotnym zagadnieniem, zbadanym w pracy **[A]**, była weryfikacja poprawności uzyskiwanych wyników dla modeli wykonanych w języku QoP-ML. W tym celu został utworzony model protokołu kryptograficznego Needhama-Schroedera oraz wykonana została jego analiza. Analiza dotyczyła wpływu zastosowanych algorytmów kryptograficznych oraz jego parametrów na wydajność protokołu. Elementem kluczowym w tym procesie jest określenie czasu wykonania protokołu, co zostało obliczone na podstawie modelu protokołu utworzonego w języku QoP-ML. Na podstawie uzyskanych wyników, wykonano Rysunek 1 na którym został przedstawiony przepływ danych w protokole Needhama-Schroedera realizowanego z protokołem OCSP, wraz z czasem CPU wymaganym do wykonania poszczególnych operacji. W pracy **[A]** została wykonana weryfikacja poprawności uzyskanych wyników. W tym celu protokół Needhama-Schroedera został zaimplementowany a czas wykonania tego protokołu w środowisku laboratoryjnym został porównany z wynikami uzyskanymi podczas analizy za pomocą języka QoP-ML. Uzyskane wyniki potwierdziły poprawność wyliczanych czasów wykonania protokołu uzyskanych w języku QoP-ML.

Określenie czasu wykonania modułów kryptograficznych, wchodzących w skład protokołów kryptograficznych, jest elementem kluczowym do określenia ich wpływu na wydajność systemu. W celu ponownej weryfikacji czasów wykonywania protokołów, których modele zostały wykonane w języku QoP-ML, w pracy **[B]** została przeprowadzona analiza powszechnie używanego protokołu kryptograficznego używanego w Internecie, czyli protokołu TLS. W tym celu utworzono model dwóch wersji protokołu TLS i przedstawiono ich analizę wydajnościową ze względu na gwarantowany poziom QoP. W pierwszym kroku wyliczono czas wykonania protokołu TLS na podstawie modelu wykonanego w QoP-ML, a następnie wykonano testy w środowisku laboratoryjnym, gdzie zaimplementowano analizowane wersje protokołu TLS. Wyniki uzyskane podczas modelowania QoP-ML oraz podczas testów laboratoryjnych, uwzględniając odchylenie standardowe wykonywanych testów, pokrywają się z czasami uzyskanymi z modelu QoP-ML. Przeprowadzone badania potwierdzają poprawność otrzymywanych wyników w procesie modelowania za pomocą języka QoP-ML.

Model oceniający jakość zastosowanych zabezpieczeń

Ocena jakości zastosowanych zabezpieczeń, zaproponowana w podstawowej wersji języka QoP-ML, ma charakter jakościowy. Ocena ta polega na wykonaniu analizy eksperckiej, zastosowanych środków ochrony informacji oraz oszacowaniu poziomu QoP dla poszczególnych wersji systemu.



Rysunek 1: Schemat przepływu danych w protokole Needhama-Schroedera realizowanego wraz z protokołem OCSP [A].

Ze względu na brak formalnej reprezentacji wiedzy, wymaganej do wykonania takiej analizy oraz nieformalny charakter oceny, taka analiza ma ograniczone zastosowanie, szczególnie w przypadku gdy badany system jest bardzo złożony. W celu wyeliminowania wspomnianych ograniczeń utworzono model pozwalający na zaawansowaną ocenę poziomu ochrony informacji (QoP) analizowanego systemu **[C]**. Ocena systemu dotyczy zestawu własności bezpieczeństwa danego systemu. Na początku procesu oceny system opisywany jest za pomocą zbioru zdarzeń, określanych jako fakty. Fakty te reprezentują wszystkie elementy danego systemu. Na podstawie zbioru faktów, bazy wiedzy, mechanizmów reprezentacji wiedzy oraz systemu eksperckiego, wykorzystując wnioskowanie w przód (ang. forward chaining mechanism), utworzyć można szczegółowy opis systemu i w konsekwencji przeprowadzić dokładniejszą ocenę jakości zabezpieczeń.

W literaturze można znaleźć różne podejścia [3, 25, 34] zajmujące się oceną jakości ochrony mechanizmów bezpieczeństwa. W Tabeli 1 przedstawiono porównanie zaproponowanego modelu z powszechnie stosowanymi rozwiązaniami. W tym celu zdefiniowano sześć kluczowych własności, które charakteryzują modele oceniające jakość środków ochrony informacji.

Ilościowa ocena - odnosi się do oceny ilościowej oszacowanej jakości ochrony. Wszystkie z prezentowanych metod, z wyjątkiem jednej [34], umożliwiają ocenę ilościową QoP mechanizmów bezpieczeństwa. Petriu et al. wykonuje analizę wydajnościową pod względem używanego poziomu bezpieczeństwa, ale analiza ta ma charakter jakościowy.

Formalna reprezentacja - odnosi się do reprezentacji jakości oceny ochrony mechanizmów bezpieczeństwa przez formalną reprezentację systemu. Wśród wyliczonych podejść tylko zaproponowany model **[C]** ma utworzoną formalną reprezentację obiektów potrzebnych do oceny, pozostałe reprezentowane są za pomocą modeli analitycznych bez formalnej definicji obiektów i

Tabela 1: Cechy modeli pozwalających wykonać ocenę QoP.

	Agarwal et al. [3]	Luo A. et al. [25]	Petriu D. C. et al. [34]	**Zaproponowany model [C]**
Ilościowa ocena	✓	✓	-	✓
Formalna reprezentacja	-	-	-	✓
Wykonywalność	-	-	✓	✓
Pośrednie rozumowanie	-	-	-	✓
Całościowość	✓	✓	-	✓
Kompletność	✓	✓	✓	✓

zasad niezbędnych do oceny formalnej.

Wykonywalność - określa możliwość realizacji zautomatyzowanego narzędzia mogącego wykonać ocenę mechanizmów QoP. Narzędzie wsparcia zostało utworzone dla dwóch podejść. W pracy Petriu et al. [34] zaprezentowano narzędzie UMLsec. Zaproponowany model **[C]** jest obsługiwany przez narzędzie SMETool (ang. Security Mechanisms Evaluation Tool), które można pobrać ze strony projektu [1]. Przepływ danych w narzędziu SMETool wraz z opisem kroków wymaganych do utworzenia modelu oceny został przedstawiony w monografii **[G]**.

Pośrednie rozumowanie - wszystkie z prezentowanych metod, z wyjątkiem zaproponowanego modelu **[C]**, mają jedno znaczące ograniczenie. Modele te mogą ocenić tylko te wersje, które wcześniej były bezpośrednio zdefiniowane i opisane w szczegółach. Prezentowany model zapewnia możliwość wykonania jakościowej oceny zastosowanych środków zabezpieczeń dla niebezpośrednio zdefiniowanych scenariuszy. Jest to wykonywane dzięki metodom rozumowania pośredniego.

Całościowość – cecha ta określa możliwość wykonania oceny wszystkich własności/usług bezpieczeństwa. Wszystkie prezentowane modele, z wyjątkiem jednego [34], mogą być stosowane do oceny wszystkich właściwości bezpieczeństwa.

Kompletność – cecha ta odnosi się do możliwości reprezentacji wszystkich mechanizmów bezpieczeństwa. Wszystkie modele realizują tę funkcjonalność.

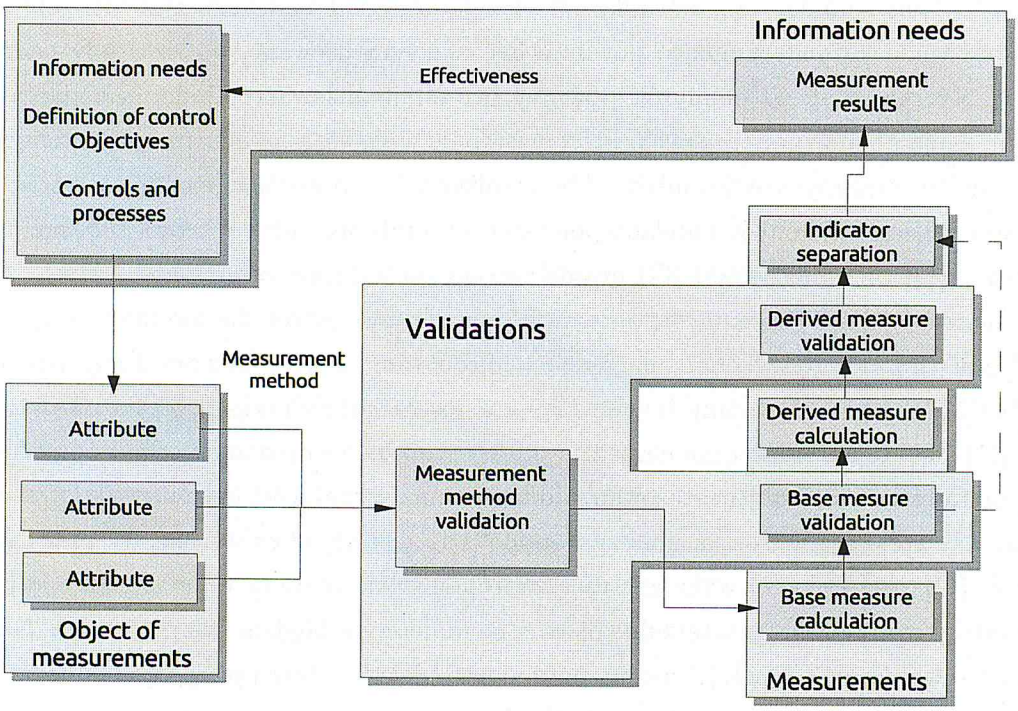
Zaproponowany model oceny jakości zastosowanych środków ochrony **[C]** jest wykorzystywany w języku QoP-ML do wykonywania ilościowej oraz jakościowej oceny czynnika QoP. Przykład wykorzystania modelu oceny dla protokołu TLS został zaprezentowany w pracy **[C]**. Istotnym elementem wykonywanym podczas takiej analizy jest połączenie konkretnych elementów modelu QoP utworzonego w języku QoP-ML na operacje atomowe określone w modelu oceny jakości zabezpieczeń. Proces ten dla protokołu TLS został przedstawiony w monografii **[G]**.

Metodyka wykonywania pomiarów czynników związanych z bezpieczeństwem systemu

Podczas analizy jakości zastosowanych środków ochrony informacji istotnym elementem jest powiązanie konkretnych zabezpieczeń (np. algorytmów kryptograficznych) z wydajnością systemu. W języku QoP-ML jest to realizowane przy pomocy tzw. metryk bezpieczeństwa określających szczegółowe informacje dotyczące wykonywanych operacji. Dla przykładu, w przypadku algorytmów kryptograficznych, będzie to czas wykonywania algorytmu w zależności od długości klu-

cza oraz danych wejściowych. Konieczność określenia takich czynników prowadzi do kolejnego kluczowego zagadnienia, które dotyczy poprawności wykonywania pomiarów. W celu uzyskania poprawnego pomiaru, należy pamiętać, że istnieje wiele czynników, które zdarzają się wewnątrz systemu wpływających na opóźnienia prowadzące do uzyskiwania niewiarygodnych wyników. Do tych czynników można zaliczyć np.: przerwania systemowe, obsługa pamięci podręcznej, dostęp do dysku twardego i nieoczekiwane działanie innych aplikacji.

W celu wykonania wspomnianych pomiarów można użyć jednego z międzynarodowych standardów np. ISO/IEC 27004. Niestety we wspomnianym standardzie model wykonywania takich pomiarów nie uwzględnia metod pozwalających zweryfikować poprawność uzyskiwanych wyników. Ograniczenie to, które ma znaczący wpływ na uzyskiwanie wiarygodnych miar dotyczących wskaźników bezpieczeństwa, było powodem utworzenia nowej metodyki wykonywania pomiarów. W pracy **[D]** zaproponowano nowy model wykonywania pomiarów rozszerzający ten opisany w standardzie ISO/IEC 27004 o metody sprawdzania ich jakości. Efektem zastosowania nowego modelu jest utworzenie pomiarów, które są powtarzalne, miarodajne, które sprawiają, że określone na ich podstawie wskaźniki wydajnościowe są bardziej wiarygodne oraz niezawodne.



Rysunek 2: Schemat nowego modelu wykonywania pomiarów z dodatkową ich walidacją [D].

Nowy model, względem standardu ISO/IEC 27004, wprowadza trzy nowe kroki: walidacje metod pomiaru, walidacje bazowych wartości pomiarowych oraz walidacje pomiarów pochodnych względem podstawowych. Zmodyfikowany model jest zaprezentowany na Rysunku 2.

Zaproponowany krok odpowiedzialny za walidację metod pomiarowych odnosi się do walidacji środowiska, w którym będzie wykonywany proces pomiaru. Wśród elementów, które wpływają na ten proces, można wymienić: weryfikację źródła danych, stanu komputera i jakości urządze-

nia pomiarowego, eliminację źródeł zewnętrznych zakłóceń, weryfikację poprawności metodyki pomiarowej i ochronę przed atakami na źródła danych.

Drugim dodanym krokiem jest walidacja podstawowych wyników pomiarów, ponieważ wyniki powinny zostać sklasyfikowane oraz zatwierdzone przed ich dalszym zastosowaniem. Po pierwsze, trzeba zdecydować, czy pomiary stanowią szereg czasowy czy są próbkami statystycznie niezależnymi. Taka decyzja może być podjęta po analizie serii pomiarów przy zastosowaniu metod np.: średnich ruchomych oraz oceny krzyżowej [4], czy modeli Markowa lub ukrytych modeli Markowa [35]. Jeśli uzyskane pomiary są szeregami czasowymi, wówczas należy je doprowadzić do postaci użytecznej w dalszych obliczeniach (np. jako sumę danych niestacjonarnych (trendu) i deterministycznych danych stacjonarnych (wahania przypadkowe)). W kolejnym kroku, dla danych stanowiących próbę statystyczną, weryfikowana jest ich jednorodność oraz niezależność. W tym celu można wykonać testy różnego rodzaju [24], wśród nich można wymienić np. testy Q Dixona. Tak przygotowane pomiary mogą następnie zostać wykorzystane do wyliczenia miar pochodnych.

Ostatnim zaproponowanym krokiem jest walidacja miar pochodnych. Miary pochodne to te, które są wykorzystywane podczas określania ostatecznych wskaźników opisujących badany obiekt. Muszą one spełniać dwa warunki: informacje na temat badanego zjawiska zebrane podczas wykonywania każdego pomiaru powinny być maksymalizowane, podczas gdy nadmiarowe informacje zbierane podczas pomiarów powinny być minimalizowane. Takie wymagania chronią przed kumulacją błędów pomiarowych, które następnie wpływają na informacje wykorzystywane do obliczania wymaganych wskaźników. Aby zrealizować te postulaty, można stosować metody oparte na analizie wzajemnych korelacji pomiarów [44] lub przy użyciu teorii informacji [12].

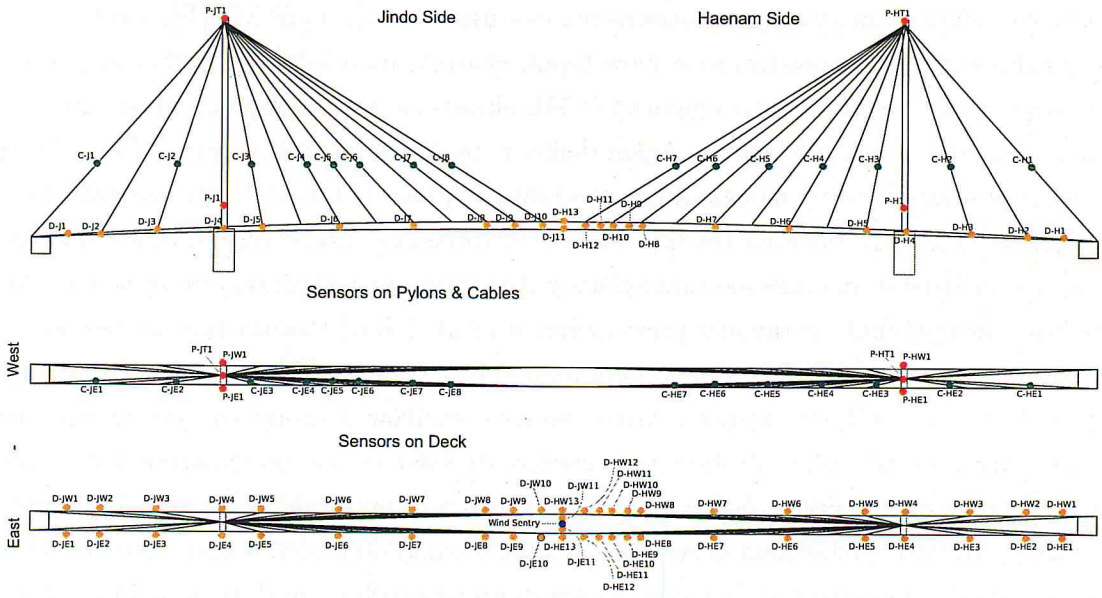
W pracy **[D]** oraz monografii **[G]** przedstawiono sprawdzenie poprawności użycia zaproponowanej metodyki dla wyliczenia współczynników wydajnościowych dla modułów kryptograficznych. W tym celu zostało wykonane narzędzie CMTool (ang. Crypto Metrics Tool). Architektura narzędzia CMTool, przepływ danych wraz z opisem poszczególnych części została również opisana w pracy **[D]**. Jest to automatyczne narzędzie zaprojektowane i wdrożone zgodnie z przedstawioną w pracy metodyką. CMTool jest stosowany do testowania wydajności prymitywów kryptograficznych oraz ich walidacji wykorzystując zaproponowane metody statystyczne. W pracy **[D]** oraz monografii **[G]** pokazano, że wykorzystując zaproponowane metody walidacji, uzyskujemy pomiary bardziej wiarygodne, powtarzalne opatrzone mniejszym błędem statystycznym. Na stronie internetowej projektu QoP-ML [1] można pobrać narzędzie CMTool i przy jego zastosowaniu wykonać testy algorytmów kryptograficznych dla danego sprzętu oraz oprogramowania. Na stronie projektu [1] przedstawiony jest również zestaw wspomnianych testów dla wybranych konfiguracji serwerów obliczeniowych. Wyniki tych testów mogą zostać wykorzystane jako dane wejściowe dla tzw. metryk bezpieczeństwa, które są wymagane podczas tworzenia modeli systemów bezpieczeństwa za pomocą języka QoP-ML.

Metodyka pozwalająca szacować żywotność architektur sieci sensorowych ze względu na zastosowane środki ochrony informacji

Zagadnienie odpowiedniego doboru środków ochrony informacji jest szczególnie istotne dla bezprzewodowych sieci sensorowych (ang. Wireless Sensor Networks, WSN). Jest to spowodowa-

ne faktem, że bezprzewodowe sieci sensorowe są systemami rozproszonymi składającymi się z urządzeń o ograniczonych zasobach (mała pamięć, małe moce obliczeniowe i silne ograniczenia energetyczne). Ograniczone zasoby węzłów sieci powodują to, że nie mogą one wykonywać zaawansowanych obliczeń kryptograficznych, przechowywać dużej ilości danych oraz z powodów energetycznych muszą ograniczać kroki komunikacyjne. Ze względu na duże ograniczenia węzłów sieci zagadnienie efektywnego doboru mechanizmów ochrony informacji staje się elementem kluczowym. W ramach wykonanych badań **[E]** zaproponowano metodę pozwalającą analizować żywotność architektur sieci sensorowych w zależności od zastosowanego poziomu ochrony informacji oraz wymagań związanych z dokładnością wykonywanych pomiarów.

Wykonanie wspomnianej analizy bezprzewodowych sieci sensorowych wymagało rozszerzenia podstawowego modelu komunikacyjnego dla języka QoP-ML. W pracy **[E]** wprowadzono dodatkowe struktury, które pozwalają określić między innymi zaawansowaną topologię sieci, filtracje pakietów oraz trasowanie pakietów. Dzięki wprowadzonym strukturom można analizować bardziej zaawansowane architektury informatyczne, a w szczególności te które wykorzystują komunikację bezprzewodową. W pracy **[E]** został opisany również moduł analizy energetycznej, gdzie wprowadzono składnię modułu wraz wymaganymi algorytmami. W dalszej części badań została wykonana przykładowa analiza sieci sensorowych umiejscowionych na moście Jindo w Korei Południowej (Rysunek 3). Wykonano symulację funkcjonowania sieci sensorowej na moście i przedstawiono żywotność architektury (Tabela 2) w zależności od różnych scenariuszy związanych z zastosowanym poziomem ochrony i dokładności uzyskiwanych pomiarów. W ramach badań wykazano znaczny wpływ analizowanych czynników na żywotność architektury WSN.



Rysunek 3: Architektura sieci sensorowych na moście Jindo w Korei Południowej [E].

Szczegółowe modele protokołów kryptograficznych dla bezprzewodowych sieci sensorowych, utworzone w języku QoP-ML, zostały przedstawione w monografii **[G]**. Wykonano tam analizę pięciu protokołów uwierzytelnienia dla węzłów w bezprzewodowych sieciach sensorowych. Analiza dotyczyła zużycia energii dla różnych wersji analizowanych tam protokołów. Za pomocą

Tabela 2: Zużycie energii oraz prognoza dotycząca żywotności architektury bezprzewodowych sieci sensorowych [E].

Scenario [40]	Energy consumption (J)	Lifetime prediction (days)
S.1	43.34	299
S.2	68.99	187
S.3	75.20	172
S.4	260.06	49
S.5	413.92	31
S.6	451.21	28
S.7	378.90	34
S.8	262.01	49
S.9	261.90	49
S.10	294.16	44

uzyskanych tam rezultatów projektant może określić różne scenariusze uwierzytelnienia węzłów sieci dostosowane do wymagań żywotności projektowanych architektur.

Analiza bezpieczeństwa systemów reputacyjnych

Innym zagadnieniem, związanym z jakością stosowanych zabezpieczeń, jest bezpieczeństwo systemów reputacyjnych. Okazuje się [10], że systemy reputacyjne, wykorzystywane przez różne portale i serwisy internetowe, mogą zostać zmodyfikowane w wyniku różnych ataków technicznych. Zagrożenie to stało się motywacją do utworzenia modułu do języka QoP-ML **[F]**, który będzie pozwalał analizować bezpieczeństwo systemów reputacyjnych, uwzględniając techniczną realizację tych systemów. W module reputacyjnym QoP-ML określa się algorytmy, za pomocą których obliczane są wartości reputacji agentów. Agent definiowany jest jako część całej struktury IT, gdzie realizowana jest analizowana usługa. Zaproponowany w pracy **[F]** moduł reputacyjny, który jest częścią języka QoP-ML, pozwala tworzyć modele abstrakcyjne zawierające mechanizmy obrony a następnie analizować realizowane tam systemy reputacyjne z technicznej perspektywy. Moduł ten pozwala uwzględniać, w ramach prowadzonej analizy, jakość stosowanych systemów zabezpieczeń oraz analizować ich wpływ na system reputacyjny. W pracy **[F]** zaprezentowano przykład takiej analizy, która dotyczy wpływu zastosowanych środków ochrony na system reputacyjny stosowany przez portal eBay. Została tam zaprezentowana prosta modyfikacja tego systemu, która wpływa na otrzymywane oceny transakcji. Zmiana oceny uzależniona została od sposobu komunikacji, którym wystawiona ocena zostanie przekazana do systemu zliczającego. Taka modyfikacja pozwala zmniejszyć wpływ potencjalnych ataków technicznych na system reputacyjny. Można wyobrazić sobie scenariusz, w którym oceny transakcji wysłane przez kupujących zostaną zmodyfikowane przez atakującego w efekcie ataku określanego jako „z osobą pośrodku" (ang. Man in the middle, MITM). Ten rodzaj ataku można łatwo wykonać, gdy ocena będzie przekazane za pośrednictwem nieszyfrowanego kanału. Natomiast jeżeli ocena zostanie przesłana do serwera reputacyjnego z wykorzystaniem protokołu TLS, wówczas taki atak będzie praktycznie niemożliwy do wykonania. Rozszerzona analiza problemu, zawierająca przykłady innych ataków

oraz inny systemy reputacyjny, została przedstawiona w monografii **[G]**. Przedstawiono tam model systemu realizującego transakcje w ramach aukcji internetowych, który stosuje równocześnie system reputacyjny dla uczestników tych aukcji. Utworzono cztery poziomy bezpieczeństwa za pomocą których mogą być realizowane transakcje, a następnie przeanalizowano wrażliwość systemu reputacyjnego na trzy scenariusze ataków.

Wieloaspektowa analiza systemów bezpieczeństwa

Jak wspomniano wcześniej, zagadnienie bezpieczeństwa w systemach IT jest pojęciem złożonym. Idea wieloaspektowej analizy bezpieczeństwa za pomocą języka QoP-ML została przedstawiona w monografii **[G]**. Monografia ta opisuje w sposób syntetyczny główne osiągnięcia habilitanta dotyczące modelowania za pomocą języka QoP-ML.

Schemat wieloaspektowej analizy bezpieczeństwa za pomocą języka QoP-ML został przedstawiony na Rysunku 4. Analiza ta składa się z pięciu kroków: utworzenie modelu, określenie metryk bezpieczeństwa, zdefiniowanie scenariuszy, zarządzanie przepływem danych oraz wykonanie analiz.

Pierwszym etapem wieloaspektowej analizy bezpieczeństwa jest utworzenie modelu wybranego środowiska IT wraz z wykorzystywanymi środkami ochrony informacji. Język QoP-ML **[A]**, który został opisany wcześniej, jest wyspecjalizowanym językiem modelowania pozwalającym opisać analizowany system IT wraz z uwzględnieniem czynników wpływających na jakość systemu zabezpieczeń (QoP).

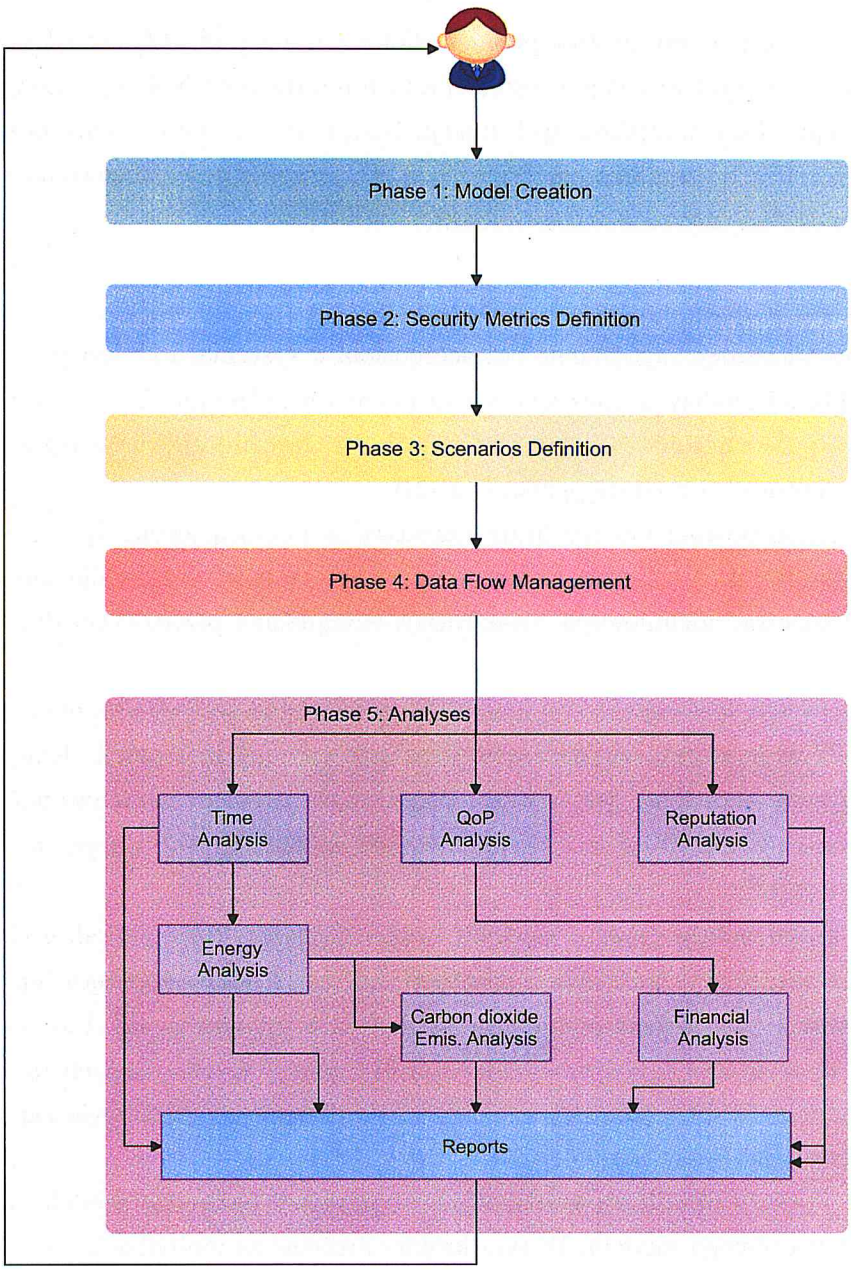
W drugim kroku należy określić metryki bezpieczeństwa, które charakteryzują zawarte w modelu operacje, łącząc je jednocześnie z parametrami zastosowanego sprzętu (np. CPU, pamięć) czy oprogramowania (np. system operacyjny, biblioteki kryptograficzne). Uzyskanie stabilnych, powtarzalnych metryk bezpieczeństwa, dotyczących operacji wykonywanych przez analizowany system (np. operacje kryptograficzne) może zostać wykonane na podstawie zaproponowanej w pracy **[D]** metodyki ich generowania.

Trzeci krok dotyczy określania konkretnych scenariuszy badanego modelu, które są różnymi wersjami analizowanego modelu. W tym kroku określane są modyfikacje systemu IT. Wśród nich można wymienić np. zastosowanie różnych protokołów kryptograficznych czy mechanizmów bezpieczeństwa. Dodatkowo można zmieniać parametry sprzętowe oraz oprogramowanie analizowanych urządzeń.

Czwarty krok polega na przypisaniu wcześniej określonych scenariuszy do konkretnych wymogów danej organizacji. W tym celu należy scharakteryzować typy danych oraz rodzaj informacji przetwarzanych przez organizację, a następnie przydzielić im środki ochrony informacji na odpowiednim poziomie bezpieczeństwa. Przykładową strukturą w organizacjach, pozwalającą wdrożyć różne poziomy ochrony, jest wprowadzenie różnych poziomów dostępowych, które mogą zostać zrealizowane poprzez model RBAC (ang. Role Based Access Control Model).

W piątym kroku wykonywana jest wieloaspektowa analiza bezpieczeństwa, w ramach której można wymienić sześć rodzajów analizy:

- analiza czasowa,
- analiza energetyczna,



Rysunek 4: Schemat wieloaspektowej analizy bezpieczeństwa za pomocą języka QoP-ML [G].

- analizy jakości zabezpieczeń (QoP),
- analiza ekonomiczna,
- analiza emisji dwutlenku węgla,
- analiza systemów reputacyjnych.

Analiza czasowa

Celem analizy czasowej jest oszacowanie czasu wykonania wszystkich zdefiniowanych operacji podczas pracy systemu, a w szczególności tych wpływających na bezpieczeństwo systemu. Na podstawie uzyskanych czasów można określić obciążenie systemu, a w szczególności obciążenie

jednostek obliczeniowych. Analiza czasowa pomaga określić mechanizmy, które są najbardziej wydajne między badanymi środkami ochrony informacji.

Analiza energetyczna

Poza analizą czasu może zostać wykonany proces analizy zużycia energii systemu IT. Aby uzyskać całkowitą ilość zużywanej energii przez operacje przewidziane w modelu, należy określić czas wykonania poszczególnych kroków. Zużycie energii jest obliczane jako suma energii zużywanej przez wszystkie operacje, które wymagają użycia jednostki centralnej CPU, takie jak: mechanizmy bezpieczeństwa, inne operacje arytmetyczne czy operacje związane z komunikacją (nasłuchiwanie, odbierania i wysyłanie).

Analizy jakości zabezpieczeń

Innym istotnym aspektem analizy wieloaspektowej jest ocena jakości zabezpieczeń. Analiza ta jest oparta na ocenie wpływu zastosowanych mechanizmów bezpieczeństwa na określone w systemie właściwości bezpieczeństwa (np. poufność, integralność, dostępność). Zaproponowane podejście pozwala ocenić jakość bezpieczeństwa zdefiniowanych w modelu mechanizmów ochrony informacji, jak również pozwala określić czynnik QoP dla niebezpośrednio zdefiniowanych konfiguracji zabezpieczeń.

Analiza ekonomiczna

Powodem wprowadzenia czynnika ekonomicznego do wieloaspektowej analizy jest jego kluczowy wpływ podczas projektowania systemów IT. Oszacowanie całkowitego kosztu utrzymania infrastruktury IT, a w szczególności centrów danych, jest często czynnikiem determinującym wybór. Jednym z elementów wpływających na koszty utrzymania systemów IT jest pobór mocy konieczny do utrzymania infrastruktury IT. W rozległych architekturach IT, składających się z tysiąca pracujących maszyn, zużycie energii elektrycznej jest czynnikiem, który tworzy jeden ze znaczących wydatków. Szczegóły analizy ekonomicznej zostały zawarte w monografii **[G]**. Został tam przedstawiony przykład takiej analizy dla centrum obliczeniowego.

Analiza emisji dwutlenku węgla

Przy pomocy modułu do analizy energetycznej można oszacować wpływ zastosowanych mechanizmów bezpieczeństwa na zużycie energii. Zużycie energii wpływa nie tylko na element finansowy, ale również na emisję dwutlenku węgla do atmosfery. Kolejnym elementem analizy jest oszacowanie emisji dwutlenku węgla do atmosfery jaka powstała w wyniku wytworzenia energii koniecznej do utrzymania projektowanej architektury IT. Analiza czynnika związanego z wpływem funkcjonowania architektury IT na środowisko jest zależna od różnych czynników. Wśród nich można wymienić: wielkość centrum danych (liczba urządzeń wchodzących w skład centrum danych), obciążenia serwerów (co przekłada się na wykorzystywane kilowatogodziny) oraz rodzaj źródła wykorzystywanego do generowania energii elektrycznej. Szczegóły analizy dotyczącej emisji dwutlenku węgla do atmosfery zostały opisane w monografii **[G]**.

Analiza systemów reputacyjnych

Głównym celem analizy systemów reputacyjnych jest możliwość ich analizowania z technicznego punktu widzenia, a w szczególności zastosowanych środków ochrony informacji. Reputacja agentów jest obliczana według określonych algorytmów, które są określane przez proces w systemie operacyjnym, wykonywanym przez danego hosta. Ten host jest częścią całej architektury IT, w której mogą zostać wykonywane różne ataki techniczne. Analiza w ramach modułu pozwala analizować wpływ ataków technicznych na algorytmy reputacyjne oraz wpływ zastosowanych mechanizmów ochrony na te systemy.

Istotnym elementem dotyczącym przedstawionej koncepcji jest możliwość wykonania wieloaspektowej analizy bezpieczeństwa dla złożonych systemów IT. Taka analiza będzie możliwa tylko wtedy, gdy ten proces zostanie wsparty przez aplikacje pozwalające wykonać automatyczne symulacje utworzonych modeli QoP-ML. W tym celu został utworzony symulator AQoPA (ang. Automated Quality of Protection Analysis Tool)[41], który wykonuje automatyczną symulację utworzonych modeli w języku QoP-ML. Głównym zadaniem symulatora AQoPA jest generowanie wszystkich możliwych stanów urządzeń wchodzących w skład systemu IT określonego w modelu QoP-ML. Symulator ten również wykrywa błędy, które nie zostały znalezione podczas parsowania modelu. Do takich błędów można zaliczyć: wykorzystanie zmiennej przed jej zdefiniowaniem, zakleszczenia czy niejednoznaczność równań. W ramach symulatora AQoPA zostały zaimplementowane wszystkie wspomniane rodzaje analizy wieloaspektowej. Innym narzędziem wspomagającym proces analizy wieloaspektowej jest aplikacja SMETool (ang. Security Mechanisms Evaluation Tool), która pozwala wykonać analizę jakości zastosowanych zabezpieczeń. Przy pomocy tego narzędzia można utworzyć bazę wiedzy oraz model oceny QoP i następnie wykonać automatyczną ocenę bezpieczeństwa zarówno jakościową jak i ilościową. Trzecim wykorzystywanym narzędziem jest wcześniej wspomniana aplikacja CMTool służąca do generowania metryk bezpieczeństwa dotyczących wydajności poszczególnych prymitywów kryptograficznych. Źródła wszystkich utworzonych aplikacji wraz z instrukcjami ich użycia oraz utworzonymi modelami są dostępne do pobrania ze strony projektu dotyczącego języka QoP-ML [1]. W monografii **[G]** przedstawiono architekturę trzech wspomnianych aplikacji.

4.4 Podsumowanie

Główne rezultaty zaprezentowane w jednotematycznym cyklu publikacji.

- Utworzenie nowego języka modelowania QoP-ML, który pozwala utworzyć model systemu IT a następnie przeprowadzenie analizy jakości zastosowanych środków ochrony informacji oraz oszacowanie czasu wykonania operacji przewidzianych w modelu.
- Utworzenie logiki do reprezentacji relacji między mechanizmami bezpieczeństwa, która pozwala dokonać zaawansowanej oceny ilościowej zastosowanych środków ochrony informacji.
- Zaproponowanie rozszerzenia modelu komunikacyjnego języka QoP-ML o możliwość określenia zaawansowanej topologii sieci, filtrację pakietów czy trasowanie pakietów.

- Zaproponowanie modelu oraz rozszerzenia języka QoP-ML pozwalającego wykonać analizę energetyczną modelowanego systemu ze względu na zastosowane środki ochrony informacji.
- Wprowadzenie modelu oraz rozszerzenia języka QoP-ML szacującego wpływ zastosowanych mechanizmów bezpieczeństwa na emisję dwutlenku węgla do atmosfery (ang. green computing).
- Opracowanie modelu oraz rozszerzenia języka QoP-ML umożliwiającego wykonanie analizy ekonomicznej modelowanych architektur IT.
- Utworzenie modelu oraz rozszerzenia języka QoP-ML, które pozwalają wykonać analizę systemów reputacyjnych uwzględniając techniczną ich realizację a w szczególności zastosowane środki ochrony informacji.
- Zaproponowanie rozszerzenia metodyki wykonywania metryk bezpieczeństwa wg ISO/IEC 27004 o nowe elementy związane z walidacją metod pomiarowych oraz walidacją uzyskiwanych wyników.
- Zaproponowanie metodyki wieloaspektowej oceny systemów IT, w szczególności protokołów kryptograficznych.
- Utworzenie modeli QoP-ML protokołów kryptograficznych (TLS, Needhama-Schroedra, protokołów uwierzytelnienia dla sieci sensorowych) oraz wykonanie ich analizy ze względu na jakość oraz wydajność zastosowanych zabezpieczeń.
- Wykonanie wieloaspektowej analizy bezpieczeństwa dotyczącej centrum dystrybucji danych wykorzystującej architekturę chmury obliczeniowej.
- Utworzenie symulatora do automatycznej analizy systemów IT (AQoPA) oraz pozostałych narzędzi wymaganych do przeprowadzenia wieloaspektowej analizy bezpieczeństwa (CMTool, SMETool).

Rezultaty przedstawione w cyklu publikacji mają wkład w rozwój informatyki w obszarze modelowania bezpiecznych systemów informatycznych, w szczególności protokołów kryptograficznych przeznaczonych dla urządzeń o silnie ograniczonych zasobach oraz bardzo złożonych systemów takich jak chmury obliczeniowe.

5 Omówienie pozostałych osiągnięć naukowo-badawczych

W ramach badań naukowych prowadzonych po uzyskaniu stopnia doktora (2007-2015) niewyszczególnionych w ramach osiągnięcia w punkcie 4, habilitant uzyskał wyniki prowadzone w ramach 5 zagadnień związanych z ochroną informacji. Zagadnienia te dotyczą:

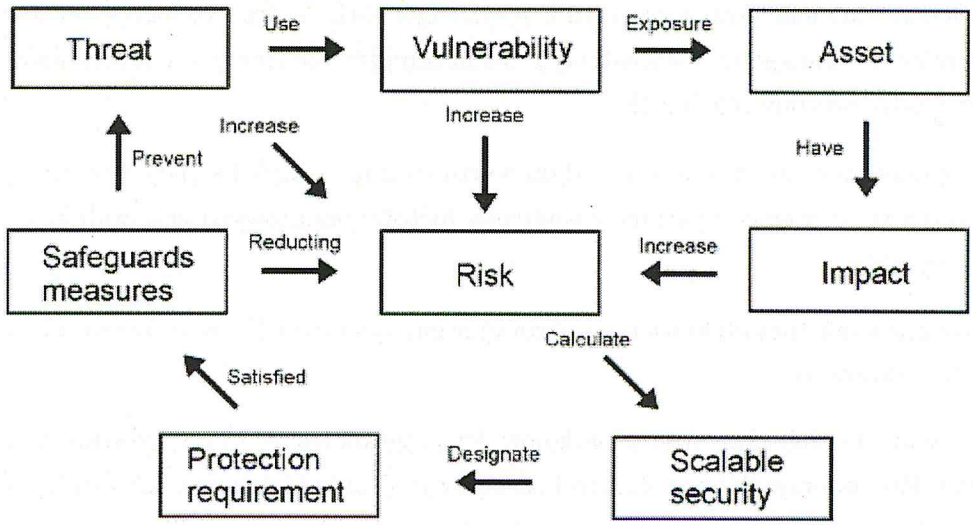
1. **adaptacyjnych mechanizmów doboru zabezpieczeń,**
2. **bezpieczeństwa bezprzewodowych sieci sensorowych,**
3. **zarządzania bezpieczeństwem informacji w systemach IT,**

4. **bezpieczeństwa oraz wydajności hurtowni danych,**

5. **projektowania oraz analizy protokołów kryptograficznych.**

Adaptacyjne mechanizmy doboru zabezpieczeń

Tematyka adaptacyjnych mechanizmów doboru zabezpieczeń była przedmiotem badań habilitanta przed doktoratem i została dalej rozwijana po doktoracie. Rozszerzeniem wyników przedstawionych w doktoracie były te przedstawione w pracy [15], gdzie zaproponowano nowy schemat analizy ryzyka, który uwzględnia proces określenia czynników związanych ze skalowalnym bezpieczeństwem (Rysunek 5).



Rysunek 5: Nowy schemat analizy ryzyka uwzględniający skalowalne bezpieczeństwo [15].

W dalszych badaniach [17] wykorzystano zaproponowany wcześniej mechanizm adaptacyjnego doboru zabezpieczeń [15] dla protokołu TLS a następnie oszacowano parametry związane z gwarantowanym poziomem bezpieczeństwa oraz przeprowadzono testy wydajnościowe zaproponowanych rozwiązań. W kolejnym kroku [21] utworzono mechanizmy optymalizacyjne oraz automatyczne narzędzie wspomagające proces optymalizacji (SPOT - ang. Secure Protocol Optimization Tool), które pozwalały na wyszukiwanie scenariuszy charakteryzujących się najmniejszym ryzykiem. Przykładowa optymalizacja, wykorzystująca zaproponowane mechanizmy oraz narzędzie SPOT, została przedstawiona dla protokołu TLS i została opisana w pracy [33].

Tabela 3: Wybór algorytmów kryptograficznych - różne poziomy bezpieczeństwa [18].

security level	*ciphers*
Version 1 - low level	**RC2-CBC + MD5**
Version 2 - mid level	**DES-CBC + SHA1**
Version 3 - high level	**3DES-CBC + SHA1**

Technologia VPN jest obecnie powszechnie używana do zagwarantowania bezpieczeństwa przesyłanych danych w sieci Internet. W dalszych badaniach [18] przeanalizowano 3 poziomy bezpieczeństwa (Tabela 3) dla tuneli VPN i zbadano maksymalną możliwą osiągalną przepustowość dla transmisji video realizowanej w ramach tunelowania VPN (Tabela 4). Pokazano, że w

przypadku realizacji tunelowania na najwyższym poziomie bezpieczeństwa osiągana przepustowość spada na tyle, że może prowadzić do braku możliwości realizacji video transmisji z wysoką jakością obrazu.

Tabela 4: Przepustowość transmisji tunelowanej przez VPN [18].

Version 1 - low level	
Bit rate	501KB/s
Version 2 - mid level	
Bit rate	480KB/s
Version 3 - high level	
Bit rate	453KB/s

Bezpieczeństwo bezprzewodowych sieci sensorowych

Wykonanie analizy bezpieczeństwa bezprzewodowych sieci sensorowych wiąże się z określeniem szeregu parametrów związanych z operacjami wykonywanymi przez węzły bezprzewodowych sieci sensorowych. W tym celu zostały utworzone oraz przeanalizowane metryki bezpieczeństwa zaawansowanych a zarazem niewymagających dużej mocy obliczeniowej trybów kryptograficznych. W pracy [48] po raz pierwszy w literaturze przedstawiono analizę wydajnościową trybów CMAC, CCM oraz GCM/GMAC dla węzłów bezprzewodowych sieci sensorowych. Kolejnymi zbadanymi trybami kryptograficznymi były tryby CCM, CBC-MAC oraz CTR [37], których analiza została wykonane dla wysokowydajnych węzłów opartych na platformie Imote2. W architekturach WSN takie węzły często pełnią rolę koordynatora mniejszych podsieci, co wiąże się z wykonywaniem wielu dodatkowych operacji.

Kolejne badania [39, 38] dotyczyły analizy parametrów komunikacyjnych bezprzewodowych sieci sensorowych, dostępnych w ramach systemu operacyjnego TinyOS oraz standardu IEEE.15.4, oraz ich wpływu na wydajność oraz żywotność sieci sensorowych. Zaprezentowane tam wyniki wskazują te operacje, które w sposób znaczący zwiększają niezawodność przekazywania danych, jednocześnie wpływając w sposób nieznaczny na wydajność węzłów sieci. W dalszej części badań [48] wykonano analizę wpływu zastosowania dodatkowych metod uwierzytelnienia dla bezprzewodowych sieci sensorowych oraz ich wpływu na opóźnienia w próbkowaniu. Okazuje się, że stosując dodatkowe środki ochrony informacji, znacznie ograniczamy maksymalną częstość próbkowania danych przez sensory, co jest szczególnie istotne dla systemów czasu rzeczywistego.

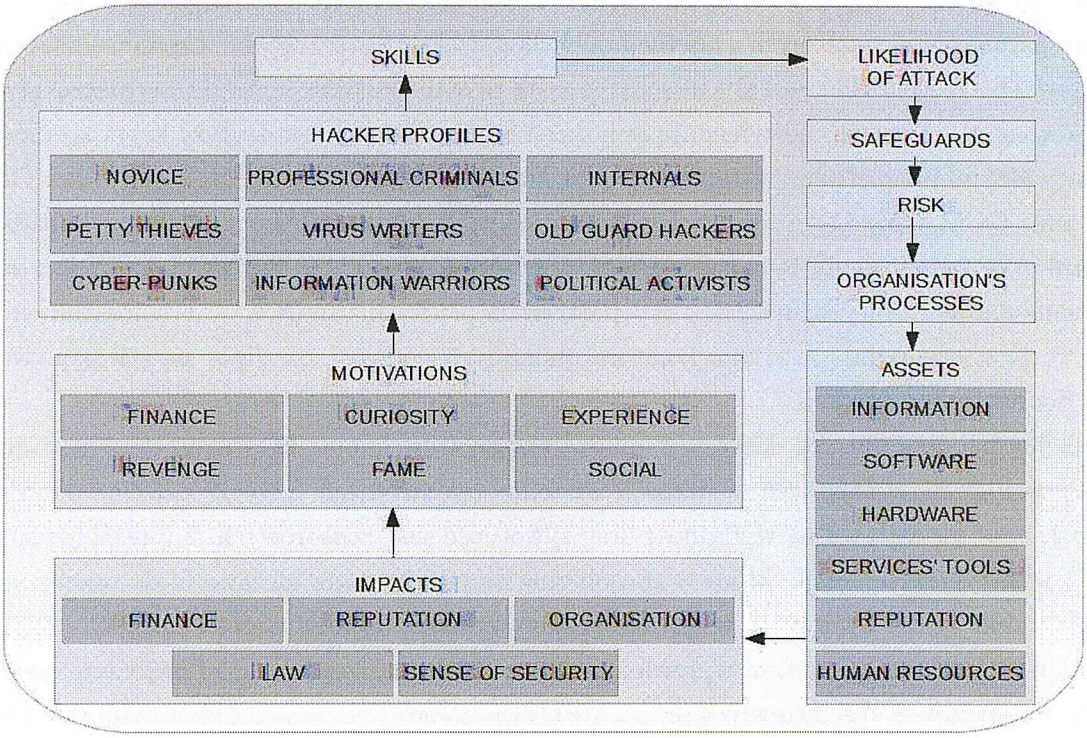
Przesyłając dane między węzłami w sieciach sensorowych, warto zastanowić się, czy trasowanie pakietów ma wpływ na żywotność całej sieci. W pracy [49] wykonano analizę różnych schematów doboru węzłów sieci sensorowych, które uczestniczyły w przesyłaniu danych przez sieć. Utworzono algorytmy, które pozwalają modyfikować trasy przesyłania danych ze względu na aktualny stan zużycia baterii oraz ze względu na wymagane obliczenia arytmetyczne. Wykazano, że stosując wspomniane algorytmy trasowania pakietów, można zwiększyć żywotność całej bezprzewodowej sieci sensorowej.

Najnowsze badania habilitanta w dziedzinie bezprzewodowych sieci sensorowych dotyczą zastosowanie ich w szybach naftowych w celu monitorowania oraz kontroli parametrów związanych z wydobyciem. W pracy [7] przedstawiono koncepcje takiej architektury oraz podstawową analizę

bezpieczeństwa związaną z realizacją takiego systemu.

Zarządzanie bezpieczeństwem informacji w systemach IT

Kolejną tematyką naukową poruszaną przez habilitanta jest tematyka zarządzania bezpieczeństwem informacji w systemach IT. W ramach tych badań zaproponowano nową metodykę analizy ryzyka [31], która w odróżnieniu od klasycznych podejść, bazuje na czynnikach związanych z motywacją atakującego (Rysunek 6). Metodyka ta nie wymaga określania podatności zasobów organizacji a następnie zagrożeń, które mogą wykorzystywać te podatności, a jedynie na określeniu motywacji atakującego dla poszczególnych zasobów systemu oraz ogólnego profilu atakującego. W porównaniu z metodami tradycyjnymi, zaproponowane podejście znacznie ogranicza złożoność procesu szacowania ryzyka, co w konsekwencji wpływa na czas wymagany do przeprowadzenia analizy.



Rysunek 6: Schemat nowej metodyki analizy ryzyka [31].

W procesie zarządzania bezpieczeństwem informacji innym kluczowym zagadnieniem jest dostosowanie systemu zabezpieczeń do wymagań określonych w standardzie ISO/IEC 27002. Standard ten zawiera pełną listę środków ochrony informacji wraz z najlepszymi praktykami dotyczącymi ich wdrożenia. Zawarte tam zagadnienia dotyczą wszystkich wymiarów wpływających na bezpieczeństwo informacji w organizacji, co w wielu zastosowaniach znacznie przekracza obszary działalności, z którymi związana jest dana organizacja. W pracy [8] zaproponowano metodę audytu zastosowanych środków ochrony informacji dla aplikacji internetowych. Metoda ta polega

na wybraniu zagadnień z normy ISO/IEC 27002, które dotyczą aplikacji webowych a następnie wprowadzeniu algorytmu ich szeregowania ze względu na poziom ich wpływu na funkcjonowanie systemu.

Dalsze badania dotyczyły analizy zagadnień ochrony informacji w metodyce COBIT (ang. Control Objectives for Information and related Technology) oraz powiązania ich z najlepszymi praktykami określonymi w normie ISO/IEC 27002 [13]. Utworzenie takiego zestawienia jest istotne, ponieważ standard COBIT definiuje jedynie ogólne cele bezpieczeństwa, jakie powinna spełnić organizacja a nie zawiera szczegółów dotyczących najlepszych praktyk w tej dziedzinie.

W innej pracy [30] został zaproponowany prosty mechanizm ochrony prywatności dla aplikacji webowych oraz przedstawiona została analiza skutków zastosowania tego mechanizmu dla powszechnie stosowanych systemów reklamowych. Analiza ta szacuje straty firmy Google związane z dostarczaniem reklam w przypadku gdyby wspomniany mechanizm został zastosowany powszechnie w sieci Internet. Wysokość potencjalnych strat świadczy o wysokim ryzyku opisywanego procesu, co wskazuje na potrzebę dodatkowych czynności związanych z zarządzaniem bezpieczeństwem informacji, które będą wdrażały dodatkowe mechanizmy kontroli procesów informatycznych w organizacjach.

Bezpieczeństwo oraz wydajność hurtowni danych

Badania naukowe habilitanta dotyczące hurtowni danych koncentrują się głównie wokół zagadnień związanych z ich wydajnością ze względu na zastosowane środki ochrony informacji. W pracy [28] przeanalizowano wydajność chmur obliczeniowych realizujących procesy biznesowe na różnym poziomie bezpieczeństwa. W tym celu utworzono różne poziomy dostępowe do danych (Tabela 5) a następnie wykonano analizę czasu wykonania poszczególnych sesji (Tabela 6). Uzyskane wyniki wskazują na znaczny wpływ zastosowania środków ochrony informacji na wydajność chmur obliczeniowych. W dalszej części badań [27] wykonano analizę wpływu zastosowanych środków informacji dla średniej wielkości centrum obliczeniowego. W tym celu wskazano cele bezpieczeństwa określone w standardzie ISO/IEC 27002 odnoszące się do zaprojektowanego centrum a następnie przydzielono do ich realizacji różne poziomy ochrony. W założeniach określono również maksymalne obciążenie serwerów na poziomie 90% oraz wymaganą liczbę serwerów potrzebnych do realizacji wymaganej liczby sesji. Następnie wyliczono koszty utrzymania takiego centrum, które związane są z opłatą za energię elektryczną wymaganą do utrzymania serwerów oraz urządzeń chłodzących. Otrzymane wyniki (Tabela 7) wskazują, że zmieniając poziom ochrony można zmniejszyć liczbę serwerów z 520 do 156, co w konsekwencji znacznie wpływa na wymagane koszty utrzymania serwerów.

Kolejnymi badaniami [42], dotyczącymi wydajności hurtowni danych, są analizy 5 scenariuszy realizacji procesów w systemach bazodanowych, które charakteryzują się różnymi poziomami bezpieczeństwa. W pracy przedstawiono analizę wydajnościową takich systemów ze względu na zastosowane poziomy ochrony informacji. Badania te potwierdziły znaczący wpływ zastosowanych środków informacji na wydajność systemów bazodanowych.

Inne badania habilitanta dotyczyły utworzenia architektury repozytorium danych [16]. Zaprezentowana koncepcja pozwala zagwarantować usługę niezaprzeczalności dla zapytań użytkowników oraz wszelkich akcji wykonywanych przez hurtownie danych. W pracy zaproponowano nowy

Tabela 5: Różne poziomy dostępowe do chmury obliczeniowej [8].

Scenario			
RBAC role / RBAC privileges	*customer*	*system operator*	*system administrator*
Application access (single session)	FTP, Web (WWW), Data Center Servers	FTP, Web (WWW), Data Center Servers	FTP, Web (WWW), Data Center Servers
Data size (for each action separately)	10MB	10MB	10MB
Security mechanisms	TLSv1 (security level - low)	TLSv2 (security level - medium)	TLSv3 (security level - high)

Tabela 6: Wydajność serwerów realizowanych przez chmury obliczeniowe [8].

Scenario			
RBAC role / Action performed (access)	*customer*	*system operator*	*system administrator*
FTP, Web (WWW), Data Center	2.98s (each)	6.24s (each)	12.22s (each)
Total time (full session)	8.94s	18.72s	36.66s

Tabela 7: Szacowana liczba wymaganych serwerów oraz roczne koszty za energię elektryczną oraz chłodzenie przy założeniu obciążenia serwerów na poziomie 90% i równej liczbie realizowanych sesji [27].

	Scenario 0.95 *(users to handle* ≈ 15 824 764 800*)*	
	server(s)	$\zeta_{power+cooling}$
role1	156	57 051 $
role2	352	128 728 $
role3	520	190 168 $

protokół kryptograficzny oraz utworzone zostały nowe struktury danych dla zaproponowanej architektury realizującej usługę niezaprzeczalności.

Projektowanie oraz analiza protokołów kryptograficznych

W ramach współpracy z grupą badawczą LIMOS we Francji, habilitant brał udział w projektowaniu protokołów kryptograficznych dla bezprzewodowych sieci sensorowych, które miały za zadanie uwierzytelnienie węzłów sieci. Efektem tej współpracy było zaprojektowanie oraz analiza 4 protokołów kryptograficznych [26], które gwarantowały różne właściwości ochrony informacji (Tabela 8) oraz charakteryzowały się różną wydajnością.

Innym zaprojektowanym protokołem [36] jest protokół elektronicznego głosowania, który jest rozszerzeniem protokołu zaproponowanego przez Cetinkaya [9]. Rozszerzenie dotyczy wprowadzenia możliwości weryfikacji niezaprzeczalności oddania głosu. Dodatkowo wprowadzono modyfikacje do oryginalnego protokołu w ten sposób, że jego implementacja jest znacznie uproszczona.

W ramach wspólnych badań z grupą badawczą z ETH Zurich przeprowadzona została analiza poprawności protokołu kryptograficznego dotyczącego elektronicznego głosowania [14]. Efektem badań było znalezienie ataku na ten protokół, który wraz z poprawkami eliminującymi możliwość

Tabela 8: Operacje wykonywane przez węzły pośrednio łączące się z siecią (IJS) [26].

	Operations on intermediate nodes					
Protocol name	Authentication	Key type	from R to S		from S to R	
			Encrypt	Decryption	Encrypt	Decryption
IJS_{orig}	no	DH with S	no	no	no	no
$IJS_{NK,dec/enc}$	yes	network key	yes	yes	yes	yes
$IJS_{K,dec/enc}$	yes	session key	yes	yes	yes	nie
$IJS_{NK,onion}$	yes	session key	yes	no	no	tak

jego wykonania został opisany w pracy [19].

Innym protokołem, którego analiza wydajnościowa została wykonana, jest protokół Kerberos [20]. W ramach badań wykonano model dwóch wersji protokołu w języku QoP-ML, które różniły się od siebie liczbą generowanych kluczy. Wykonana analiza wykazała, że czas wykonania wersji protokołu, gdzie tylko jeden klucz symetryczny będzie generowany, jest dwukrotnie krótszy od czasu wykonania wersji protokołu, gdzie dodatkowo klucze sesyjne będę generowane. Uzyskane wyniki mogą posłużyć projektantów systemów IT w doborze odpowiednich parametrów dla protokołu Kerberos.

5.1 Autorstwo i współautorstwo publikacji naukowych

Habilitant jest autorem lub współautorem 40 prac opublikowanych w latach 2007-2015 (okres po doktoracie - Tabela 9). Wśród nich 7 jest indeksowanych w bazie **Journal Citation Reports (JCR)**, 12 zostało wydanych w seriach wydawniczych **Springer**, 7 zostało opublikowanych w czasopismach z **listy B** (wg ministerialnego wykazu czasopism) oraz 1 monografia naukowa wydana w wydawnictwie **CRC Press, Taylor & Francis Group.**

Prace z listy **JCR** zostały opublikowane w następujących czasopismach (IF liczony wg daty publikacji):

- **Computers & Security** - IF=0,737 (2007) * 1, IF=1,158 (2012) * 1, 5YIF=1,386,
- **Information Processing Letters** - IF=0,612 (2010) * 1, 5YIF=0,642,
- **The Scientific World Journal** - IF=1,219 (2014) * 1, 5YIF=1,60,
- **Computer Journal** - IF=0,888 (2014) * 1, 5YIF=0,962,
- **Mathematical Problems in Engineering** - IF=0,762 (2015) * 1, 5YIF=0,798,
- **International Journal of Distributed Sensor Networks** - IF=0,665 (2015) * 1, 5YIF=0,601.

Sumaryczny **IF = 6,041**
Sumaryczny **5 letni IF = 7,375**

Wśród opublikowanych prac w latach 2007-2015 (Tabela 9):

- 14 publikacji jest indeksowanych w bazie **Web of Science** ,

Tabela 9: Publikacje w latach 2007-2015 (po doktoracie).

Rodzaj publikacji	**liczba publikacji**	**Punkty MNiSW**
indeksowane w JCR	7	175
wydawnictwo Springer (indeksowane w bazie WoS)	8	80
wydawnictwo Springer (oczekujące na indeksację w bazie WoS)	4	0
czasopisma z lista B MNiSW	7	41
inne czasopisma zagraniczne	1	0
monografie, podręczniki	3	25
rozdziały w monografiach, podręcznikach	4	15
materiały konferencyjne w j.angielskim, raporty techniczne	5	10
materiały konferencyjne (oczekujące na indeksację w bazie WoS)	1	0
SUMA	**40**	**346**

- 2 publikacje w czasopismach indeksowanych w **JCR** oczekują na indeksację w bazie **Web of Science**,
- 5 publikacji konferencyjnych oczekuje na indeksację w bazie **Web of Science**, zgodnie z oświadczeniem wydawcy lub organizatorów konferencji,
- 28 publikacji jest indeksowanych w bazie **DBLP** Computer Science Bibliography,
- 18 publikacji jest indeksowanych w bazie **Scopus**.

5.2 Liczba cytowań, indeks Hirscha

Liczba cytowań publikacji oraz indeks Hirsha według bazy Web of Science (WoS), bazy Scopus oraz Google Scholar zostały przedstawione w Tabeli 10.

Tabela 10: Liczba cytowań publikacji oraz indeks Hirscha.

Baza	**liczba cytowań**	**liczba cytowań bez autocytowań**	**indeks Hirscha**
Web of Science	46	12	4
Scopus	48	8	5
Google Scholar	178	-	8

5.3 Kierowanie międzynarodowymi lub krajowymi projektami badawczymi lub udział w takich projektach

1. W latach **2007-2009** wykonawca w projekcie **Budowa modelu funkcjonalnego Krajowego Magazynu Danych - (R02 055 03, projekt celowym MNiSW)**. System

ten służy do przechowywania danych o zasięgu krajowym, dostępny jest za pośrednictwem sieci naukowej PIONIER oraz sieci miejskich MAN. System ten zapewnia wiarygodność i bezpieczeństwo przechowywania danych oraz wysoką wydajność. Usługi systemu charakteryzują się wysoką dostępnością, m.in. dzięki geograficznej replikacji danych, redundancji infrastruktury oraz wewnętrznym mechanizmom obsługi awarii.

2. **Od 2012 roku do chwili obecnej** wykonawca w projekcie **RECONCILE – Robust Online Credibility Evaluation Of Web Content, Polish-Swiss Research Project.** Projekt kierowany przez prof Adama Wierzbickiego z PJATK i profesora Karla Aberera z EPFL w Lozannie. Celem projektu Reconcile jest stworzenie nowych mechanizmów wsparcia użytkowników w ocenie wiarygodności treści internetowych.

3. **Od 2013 do chwili obecnej** wykonawca w projekcie **Mechanizmy rekomendacji wirtualnych zespołów dla realizacji złożonych zadań wymagających otwartej współpracy - NCN (2012/05/B/ST6/03364).** Projekt weryfikuje hipotezę, że możliwa jest poprawa jakości współpracy w wirtualnych zespołach poprzez wprowadzenie systemów rekomendacji dla całych zespołów lub poszczególnych ich członków. Weryfikacja tej hipotezy wymaga rozwiązania dwóch problemów badawczych: utworzenia efektywnych algorytmów dla zespołu i rekomendacji członka zespołu i analizy wpływu tych algorytmów w procesie wyłaniania drużyny.

4. W latach **2011-2012** wykonawca w projekcie dla młodych naukowców, przyznany przez Wydział Matematyki, Fizyki i Informatyki, Uniwersytetu Marii Curie-Skłodowskiej w Lublinie, który dotyczył **utworzenia języka modelowania systemów teleinformatycznych opierających swoją funkcjonalność o protokoły kryptograficzne.** Język ten umożliwia opisanie protokołu kryptograficznego z uwzględnieniem jakości stosowanych zabezpieczeń (ang. Quality of Protection).

5. W latach **2013-2014** wykonawca w projekcie dla młodych naukowców, przyznany przez Wydział Informatyki, Polsko-Japońskiej Akademii Technik Komputerowych w Warszawie, który dotyczył **modelowania oraz symulacji adwersarzy dla usług reputacji i wiarygodności w systemach Web 2.0.** Celem realizacji projektu było utworzenie różnych modeli adwersarzy, które różnią się od siebie możliwościami interakcji z uczestnikami protokołów. W ramach projektu zostały wykonane symulacje interakcji utworzonych wcześniej modeli adwersarzy dla wybranych modeli aplikacji Web 2.0, dla których istotnym elementem jest ich system reputacyjny.

5.4 Wygłaszanie referatów na międzynarodowych i krajowych konferencjach

W latach 2007-2015 habilitant przedstawił 12 referatów na konferencjach międzynarodowych.

1. The 17th International Conference on Enterprise Information Systems (ICEIS) - 27-30.04.2015, Barcelona, Hiszpania.

2. The 2014 Asian Conference on Availability, Reliability and Security - (AsiaARES) - 14-17.04.2014, Bali, Indonesia.
3. The 2013 Asian Conference on Availability, Reliability and Security - (AsiaARES) - 25-29.03.2013, Yogyakarta, Indonesia.
4. The 3rd Workshop on Web Content Credibility - 4.01.2013, Warszawa, Polska.
5. The 2nd International Conference on Cryptography and Security Systems - 24-26.09.2012, Kazimierz Dolny, Polska.
6. The 18th Conference on Computer Networks (CN) - 14-18.06.2011, Ustroń, Polska.
7. The 1st European Teletraffic Seminar - 14-16.02.2011, Poznań, Polska.
8. The 17th Conference on Computer Networks (CN) - 15-19.06.2010, Ustroń, Polska.
9. The 9th International Conference on Applied Computer Science, 11-13.02.2009, Kazimierz Dolny, Polska.
10. The 16th Conference on Computer Networks (CN) - 16-20.06.2009, Wisła, Polska.
11. The 7th International Scientific SHP Congress - 21-24.06.2007, Warszawa, Polska.
12. The 7th International Conference on Applied Computer Science, 8-10.02.2007, Kazimierz Dolny, Polska.

5.5 Nagrody za działalność naukową

1. Nagroda III stopnia Rektora Uniwersytetu Marii Curie-Skłodowskiej w Lublinie za pracę naukową - 2012.
2. Nagroda III stopnia Rektora Uniwersytetu Marii Curie-Skłodowskiej w Lublinie za pracę naukową - 2013.

6 Dorobek dydaktyczny i popularyzatorski oraz inne osiągnięcia

6.1 Uczestnictwo w programach europejskich i innych programach międzynarodowych lub krajowych

1. Od 2012 do chwili obecnej, udział w projekcie **MEDET Nr 530574 – TEMPUS-1-2012-1-ES-TEMPUS-JPCR(2012-3008/001-001) - UE Project**.
2. W latach 2005-2008 udział w projekcie **Sophia-Warsaw Group of the Philosophy and fundamentals of science - Sophia Europa Project**, w ramach sieci naukowej finansowanej przez Sir John Templeton Foundation.

6.2 Udział w międzynarodowych lub krajowych komitetach organizacyjnych oraz programowych konferencji naukowych

Udział w komitetach organizacyjnych konferencji naukowych.

1. CSS'2014 – 3rd International Conference of Cryptography and Security Systems, Lublin, Polska - **przewodniczący komitetu organizacyjnego.**
2. CSS'2012 – 2nd International Conference of Cryptography and Security Systems, Kazimierz Dolny, Polska - **przewodniczący komitetu organizacyjnego.**
3. CSS'2011 – 1st International Workshop of Cryptography and Security Systems, Naleczow, Poland - **przewodniczący komitetu organizacyjnego.**
4. SIS'2010 – 4th International Workshop on Secure Information Systems, Wisla, Poland - **jeden z przewodniczących komitetu organizacyjnego.**
5. IBIZA'2009 - 9th International Conference on Applied Computer Science, Kazimierz Dolny, Polska - **członek komitetu organizacyjnego.**
6. IBIZA'2008 - 8th International Conference on Applied Computer Science, Kazimierz Dolny, Polska - **członek komitetu organizacyjnego.**
7. IBIZA'2007 - 7th International Conference on Applied Computer Science, Kazimierz Dolny, Polska - **członek komitetu organizacyjnego.**
8. IBIZA'2006 - 6th International Conference on Applied Computer Science, Kazimierz Dolny, Polska - **członek komitetu organizacyjnego.**
9. IBIZA'2005 - 5th International Conference on Applied Computer Science, Kazimierz Dolny, Polska - **członek komitetu organizacyjnego.**

Udział w komitetach programowych konferencji naukowych.

1. NTMS'2015 – 7th International Conference on New Technologies, Mobility and Security, Paris, Francja.
2. KBI'2014 – Kryptografia i bezpieczeństwo informacji, Warszawa, Polska.
3. CSS'2014 – 3rd International Conference of Cryptography and Security Systems, Lublin, Polska
4. NTMS'2014 – 6th International Conference on New Technologies, Mobility and Security, Dubai, Zjednoczone Emiraty Arabskie.
5. NTMS'2012 – 5th International Conference on New Technologies, Mobility and Security, Istanbul, Turcja.
6. CSS'2012 – 2nd International Conference of Cryptography and Security Systems, Kazimierz Dolny, Polska.

7. CSS'2011 – 1st International Workshop of Cryptography and Security Systems, Naleczow, Polska.

8. SIS'2010 – 4th International Workshop on Secure Information Systems, Wisla, Polska.

6.3 Otrzymane nagrody i wyróżnienia

1. Otrzymanie tytułu **Homo Didacticus Wydziału Matematyki Fizyki i Informatyki UMCS 2009** w kategorii osób prowadzących ćwiczenia, przyznawanego przez społeczność studencką Wydziału MFI UMCS prowadzącym ćwiczenia szczególnie cenionym za pasję, obiektywizm oraz umiejętność przekazywania wiedzy.

6.4 Kierowanie projektami realizowanymi we współpracy z naukowcami z innych ośrodków polskich i zagranicznych, a w przypadku badań stosowanych we współpracy z przedsiębiorcami

1. Projekt nr 790/P/DUN/2012 MNiSW, dotyczący **organizacji międzynarodowej konferencji Cryptography and Security Systems 2012**, Kazimierz Dolny, 24-27 września 2012 r.

2. Projekt nr 739/P/DUN/2011 MNiSW, dotyczący **organizacji konferencji Cryptography and Security Systems 2011**, Nałęczów, 26-28 września 2011 r.

6.5 Udział w komitetach redakcyjnych i radach naukowych czasopism

Członkostwo w komitetach redakcyjnych czasopism

1. Journal of Network and Communication Technologies, Canadian Center of Science and Education (od 2013 r.).

2. Open Journal of Information Security and Applications, Scientific Online Publishing, USA (od 2013 r.).

3. Annales UMCS Sectio AI Informatica, Polska (od 2015 r.).

Gościna edycja (ang. guest editor) numerów czasopism

1. Zbigniew Kotulski/Bogdan Księżopolski/Pascal Lafourcade: A special issue of Journal of Sensor and Actuator Networks (ISSN 2224-2708), MDPI Switzerland, Special Issue „Security Issues in Sensor Networks, 2015.

2. Zbigniew Kotulski/Bogdan Księżopolski: Cryptography and Security Systems, Springer, Communications in Computer and Information Science Volume 448, 2014.

3. Zbigniew Kotulski/Bogdan Księżopolski: Special Issue of Journal Annales UMCS ser. Informatica: Cryptography and data protection, AI, XIV, 1, 2014.

4. Zbigniew Kotulski/Bogdan Księżopolski: Special Issue of Journal Annales UMCS ser. Informatica: Security Systems, Cryptographic protocols Network security, AI, XIV, 2, 2014.

5. Zbigniew Kotulski/Bogdan Księżopolski: Special Issue of Journal Annales UMCS ser. Informatica: Cryptography and data protection, AI, XII, 3, 2012.

6. Zbigniew Kotulski/Bogdan Księżopolski: Special Issue of Journal Annales UMCS ser. Informatica: Security Systems, Cryptographic protocols Network security, AI, XII, 4, 2012.

7. Zbigniew Kotulski/Bogdan Księżopolski: Special Issue of Journal Annales UMCS ser. Informatica: Security Systems, AI, XI, 3, 2011.

8. Zbigniew Kotulski/Bogdan Ksiezopolski: Special Issue of Journal Annales UMCS ser. Informatica: Cryptography and data protection, AI, XI, 2, 2011.

6.6 Członkostwo w międzynarodowych lub krajowych organizacjach i towarzystwach naukowych

1. Członek Komisji Podstaw i Zastosowań Fizyki i Chemii w Technice, Rolnictwie i Medycynie, **Oddział Lubelski Polskiej Akademii Nauk** (od 2015r.).

2. Członek organizacji **ACM** (ang. Association for Computing Machinery) - Professional Member (od 2012 r.).

3. Członek organizacji **IEEE** - Professional Member (od 2012 r.).

4. Członek organizacji **IACR** (ang. International Association for Cryptologic Research) (od 2013 r.).

5. Członek organizacji **INSTICC** (ang. Institute for Systems and Technologies of Information, Control and Communication) (od 2015 r.).

6.7 Osiągnięcia dydaktyczne i w zakresie popularyzacji nauki

W ramach pracy dydaktycznej habilitant prowadzi lub prowadził zajęcia z 10 przedmiotów (wykłady i zajęcia laboratoryjne). Zajęcia prowadzone były na Uniwersytecie Marii Curie Skłodowskiej w Lublinie oraz w Polsko-Japońskiej Wyższej Akademii Technik Komputerowych w Warszawie. Wykaz prowadzonych przedmiotów obejmuje:

- bezpieczeństwo systemów komputerowych (wykład + laboratorium),
- bezpieczeństwo sieci komputerowych (wykład + laboratorium),
- zaawansowane metody ochrony informacji (wykład + laboratorium),
- systemy operacyjne i sieci komputerowe (wykład + laboratorium),
- audyt bezpieczeństwa systemów IT (wykład + laboratorium),
- system Unix (laboratorium),
- środowisko programisty (laboratorium),

- technologie sieciowe (laboratorium),
- zaawansowane technologie sieciowe CISCO (wykład + laboratorium),
- systemy operacyjne (laboratorium).

Habilitant jest autorem lub współautorem 4 skryptów akademickich z informatyki.

1. Bogdan Księżopolski: **Audyt Bezpieczeństwa Systemów IT** – Ćwiczenia, wydawnictwo UMCS, 2012.
2. Bogdan Księżopolski, Damian Rusinek: **Administracja Systemu Linux/Unix**, wydawnictwo UMCS, 2012.
3. Bogdan Księżopolski: **Bezpieczeństwo i optymalizacja procesów realizowanych drogą elektroniczną**, wydawnictwo UMCS, 2011.
4. Bogdan Księżopolski, Pawel Szałachowski: **Audyt Bezpieczeństwa Systemów IT**, wydawnictwo UMCS, 2011.

6.8 Opieka naukowa nad studentami

W latach 2007-2015 habilitant był promotorem 17 prac magisterskich oraz 9 prac licencjackich.

6.9 Opieka naukowa nad doktorantami w charakterze opiekuna naukowego lub promotora pomocniczego

Obecnie habilitant pełni funkcję promotora pomocniczego w jednym otwartym przewodzie doktorskim oraz pełni rolę pomocniczego opiekuna naukowego dla dwóch doktorantów.

1. Habilitant jest **promotorem pomocniczym w przewodzie doktorskim pana mgr. Damiana Rusinka**; przewód doktorski został otwarty w 2012 roku na Wydziale Elektroniki i Technik Informacyjnych Politechniki Warszawskiej.
2. Od 2013 roku habilitant **jest pomocniczym opiekunem naukowym pana mgr. Michaila Mokkasa**, doktoranta na Wydziale Informatyki, Polsko-Japońskiej Akademii Technik Komputerowych w Warszawie. Aktualne prowadzone są badania naukowe dotyczące modeli jakościowej oceny usług internetowych (ang. Quality of Experience), w szczególności w odniesieniu do zastosowanego poziomu ochrony informacji (QoP).
3. Od 2012 roku habilitant **jest pomocniczym opiekunem naukowym pani mgr Agaty Nieścieruk**, doktorantki na Wydziale Informatyki, Polsko-Japońskiej Akademii Technik Komputerowych w Warszawie. Aktualne prowadzone są badania naukowe dotyczące wielokryterialnych metod optymalizacji systemów informatycznych ze względu na zastosowany poziom ochrony informacji.

6.10 Staże w zagranicznych lub krajowych ośrodkach naukowych lub akademickich

- 16.09-29.09.2013 - Wizyta naukowa w ośrodku LIMOS, Clermont-Ferrand, Francja.
- 21.03-23.03.2011 - Wizyta studyjna na Politechnice Warszawskiej.
- 6.09-11.09.2010 - Udział w międzynarodowych warsztatach FOSAD 2010 - Foundations of Security Analysis and Design - organizowanych przez Uniwersytet w Bolonii, Włochy.
- 30.10-2.11.2009 - Wizyta studyjna w Instytucie Podstawowych Problemów Techniki PAN w Warszawie.
- 1.09.2008-31.08.2009 - Roczna współpraca naukowa w Instytucie Podstawowych Problemów Techniki PAN w Warszawie (regularne dwutygodniowe spotkania naukowe z zespołem prof. dr hab. inż. Zbigniewa Kotulskiego oraz zgoda Dyrektora Instytutu na korzystanie z zasobów IPPT PAN).
- 09-13.09.2006r. - Udział w międzynarodowych warsztatach - International Summer School Marktoberdorf 2006 – Software System Reliability and Security organizowanych przez Advanced Study Institute of the NATO Security Through Science Committee and Institut fur Informatik, Technische Universitat Munchen, Niemcy.

6.11 Wykonanie ekspertyz i innych opracowań

1. W roku 2006 habilitant wykonał ekspertyzę dotyczącą **warunków organizacji usług informatycznych na terenach ZSROW**, projektu realizowanego w ramach Pilotażowego Programu LEADER+ współfinansowanego ze środków Unii Europejskiej.

6.12 Udział w zespołach eksperckich i konkursowych

1. Członek jury w drużynowym konkursie informatycznym - NetMatesrsCUP 2013.

6.13 Recenzowanie międzynarodowych referatów konferencyjnych i artykułów do czasopism, recenzowanie projektów międzynarodowych i krajowych

Wykonanie łącznie 25 recenzji artykułów na następujące konferencje.

1. INDIN 2015 - 13th IEEE International Conference on Industrial Informatics, Cambridge, UK.
2. NTMS'2015 – 7th International Conference on New Technologies, Mobility and Security, Paris, France.
3. CSS'2014 – 3rd International Conference of Cryptography and Security Systems, Lublin, Poland.

4. NTMS'2014 – 6th International Conference on New Technologies, Mobility and Security, Dubai, United Arab Emirates.
5. NTMS'2012 – 5th International Conference on New Technologies, Mobility and Security, Istanbul, Turkey.
6. CSS'2012 – 2nd International Conference of Cryptography and Security Systems, Kazimierz Dolny, Poland.
7. CSS'2011 – 1st International Workshop of Cryptography and Security Systems, Naleczow, Poland.
8. SIS'2010 – 4th International Workshop on Secure Information Systems, Wisla, Poland.

Wykonanie 48 recenzji artykułów dla czasopism naukowych w tym 25 dla czasopism z listy Journal Citation Reports (JCR).

1. Computers & Security, Elsevier, (IF=1,172) - 13 recenzji.
2. Sensors, MDPI, (IF=2,05) - 1 recenzja.
3. Multimedia Tools and Applications, Springer, (IF=1,06) - 3 recenzje.
4. EURASIP Journal on Wireless Communications and Networking, Springer, (IF=0,81) - 1 recenzja.
5. Wireless Networks, Springer, (IF=1,06) - 1 recenzja.
6. Science China Information Sciences, Springer, (IF=0,702) - 1 recenzja.
7. Security and Communication Networks, John Wiley Sons, (IF=0,43) - 4 recenzje.
8. Fundamenta Informaticae, Polish Mathematical Society, (IF=0,48) - 1 recenzja.
9. Future Internet, MDPI - 1 recenzja.
10. Network and Communication Technologies, Canada - 1 recenzja.
11. International Journal of Computers and Applications, Acta Press, Canada - 5 recenzji.
12. Open Journal of Information Security and Applications, Scientific Online Publishing, USA - 1 recenzja.
13. Annales UMCS ser. Informatica, Poland - 15 recenzji.

W latach 2008-2009 habilitant wykonał recenzje 4 informatycznych projektów naukowo-przemysłowych dla Programu Innowacyjnej Gospodarki (POIG).

Bogdan Księżopolski

Literatura

[1] The web page of the qop-ml project. http://qopml.org/, 2014.

[2] Martin Abadi and Andrew D. Gordon. A calculus for cryptographic protocols: The spi calculus. *Information and Computation*, 148:36–47, 1999.

[3] Avesh K. Agarwal and Wenye Wang. On the impact of quality of protection in wireless local area networks with ip mobility. *Mobile Networks and Applications*, 12(1):93–110, 2007.

[4] Sylvain Arlot and Alain Celisse. A survey of cross-validation procedures for model selection. *Statist. Surv.*, 4:40–79, 2010.

[5] John. W. Backus. The syntax and semantics of the proposed international algebraic language of the zurch acm-gamm conference. In *Information Processing: Proceedings of the InternationalConference on Information Processing, Paris*, pages 125–132. UNESCO, 1959.

[6] David Basin, Jürgen Doser, and Torsten Lodderstedt. Model driven security: From uml models to access control infrastructures. *ACM Trans. Softw. Eng. Methodol.*, 15(1):39–91, January 2006.

[7] Bartłomiej Bielecki, Bogdan Księżopolski, Andrzej Krajka, and Adam Wierzbicki. The concept and security analysis of wireless sensor network for gas lift in oilwells. *Annales UMCS, Informatica*, 14(2):117–127, 2014.

[8] Wojciech Bylica and Bogdan Księżopolski. On scalable security audit for web application according to iso 27002. In Andrzej Kwiecien, Piotr Gaj, and Piotr Stera, editors, *CN*, volume 160 of *Communications in Computer and Information Science*, pages 386–397. Springer, 2011.

[9] Orhan Cetinkaya and Ali Doganaksoy. A practical verifiable e-voting protocol for large scale elections over a network. In *The Second International Conference on Availability, Reliability and Security*, pages 432–442, 2007.

[10] Kevin Hoffman, David Zage, and Cristina Nita-Rotaru. A survey of attack and defense techniques for reputation systems. *Journal ACM Computing Surveys*, 42(1), 2009.

[11] Jan Jürjens. *Secure System Development with UML*. Springer, 2007.

[12] Zbigniew Kotulski. Optimization of sensors' location in a stochastic extrapolation problem. *Journal of Sound and Vibration*, 138(3):351 – 363, 1990.

[13] Bogdan Księżopolski. Information security governance according to the cobit methodology. In *Information System in Management*, pages 50–58, 2011.

[14] Bogdan Księżopolski and Zbigniew Kotulski. Cryptographic protocol for electronic auctions with extended requirements. *Annales UMCS, Informatica*, 2(1):391–400, 2004.

[15] Bogdan Księżopolski and Zbigniew Kotulski. Adaptable security mechanism for dynamic environments. *Computers & Security*, 26(3):246 – 255, 2007.

[16] Bogdan Księżopolski and Zbigniew Kotulski. Middleware non-repudiation service for the data warehouse. *Annales UMCS, Informatica*, 11(2):145–158, 2010.

[17] Bogdan Księżopolski, Zbigniew Kotulski, and Paweł Szałachowski. Adaptive approach to network security. In Andrzej Kwiecien, Piotr Gaj, and Piotr Stera, editors, *CN*, volume 39 of *Communications in Computer and Information Science*, pages 233–241. Springer, 2009.

[18] Bogdan Księżopolski, Zbigniew Kotulski, and Paweł Szałachowski. On qop method for ensuring availability of the goal of cryptographic protocols in the real-time systems. In *European Teletraffic Seminar*, pages 195–202. Jasart Studio, 2011.

[19] Bogdan Księżopolski and Pascal Lafourcade. Attack and revision of electronic auction protocol using ofmc. *Annales UMCS, Informatica*, 6(1):171–183, 2007.

[20] Bogdan Księżopolski, Damian Rusinek, and Adam Wierzbicki. On the modelling of kerberos protocol in the quality of protection modelling language (qop-ml). *Annales UMCS, Informatica*, 12(4):69–81, 2012.

[21] Bogdan Księżopolski, Pawel Szalachowski, and Zbigniew Kotulski. Spot: Optimization tool for network adaptable security. In Andrzej Kwiecien, Piotr Gaj, and Piotr Stera, editors, *CN*, volume 79 of *Communications in Computer and Information Science*, pages 269–279. Springer, 2011.

[22] Bogdan Księżopolski, Tomasz Żurek, and Michail Mokkas. Quality of protection evaluation of security mechanisms. In *The Scientific World Journal*, volume 2014, pages 1–18, 2014.

[23] Torsten Lodderstedt, David A. Basin, and Jürgen Doser. Secureuml: A uml-based modeling language for model-driven security. In Jean-Marc Jézéquel, Heinrich Hußmann, and Stephen Cook, editors, *UML*, volume 2460 of *Lecture Notes in Computer Science*, pages 426–441. Springer, 2002.

[24] Sachs Lothar. *Applied Statistics. A Handbook of Techniques.* Springer, 1984.

[25] An'an Luo, Chuang Lin, Kai Wang, Lei Lei, and Chanfang Liu. Quality of protection analysis and performance modeling in ip multimedia subsystem. *Computer Communications*, 32(11):1336–1345, 2009.

[26] Ismail Mansour, Gerard Chalhoub, and Micel Misson. *Security architecture for multi-hop wireless sensor networks.* CRC Press Book, 2014.

[27] Katarzyna Mazur, Bogdan Księżopolski, and Zbigniew Kotulski. On security management: Improving energy efficiency, decreasing negative environmental impact and reducing financial costs for data centers. *Mathematical Problems in Engineering*, (in press), 2015.

[28] Katarzyna Mazur, Bogdan Księżopolski, and Adam Wierzbicki. On the modelling of the influence of access control management to the system security and performance. In *17th International Conference on Enterprise Information Systems*, volume 2, pages 346–354, Barcelona, Hiszpania, 2015. SCITEPRESS.

[29] Kurkowski Mirosław. *Formalne metody weryfikacji własności protokołów zabezpieczających w sieciach komputerowych.* Akademicka Oficyna Wydawnicza EXIT, Warszawa, 2013.

[30] Radosław Nielek, Bogdan Księżopolski, Adam Wierzbicki, and Łukasz Anwajler. Surprising consequences of simple privacy protection method. In *3rd International Conference on IT Convergence and Security*, pages 1–5. IEEE, 2013.

[31] Agata Niescieruk and Bogdan Księżopolski. Motivation-based risk analysis process for it systems. In *AsiaARES*, volume 8407 of *Lecture Notes in Computer Science*, pages 446–455. Springer, 2014.

[32] Chui Sian Ong, Klara Nahrstedt, and Wanghong Yuan. Quality of protection for mobile multimedia applications. In *ICME*, pages 137–140. IEEE, 2003.

[33] Szałachowski Paweł, Księżopolski Bogdan, and Kotulski Zbigniew. Optimization of the tls security protocol. *Annales UMCS Informatica*, 2:59–75, 2009.

[34] Dorina C. Petriu, C. Murray Woodside, Dorin Bogdan Petriu, Jing Xu, Toqeer Israr, Geri Georg, Robert B. France, James M. Bieman, Siv Hilde Houmb, and Jan Jürjens. Performance analysis of security aspects in uml models. In Vittorio Cortellessa, Sebastián Uchitel, and Daniel Yankelevich, editors, *WOSP*, pages 91–102. ACM, 2007.

[35] Lawrence R. Rabiner. A tutorial on hidden markov models and selected applications in speech recognition. In *Proceedings of IEEE*, volume 77, pages 257–286. IEEE, 1989.

[36] Damian Rusinek and Bogdan Księżopolski. Voter non-repudiation oriented scheme for the medium scale e-voting protocol. In *9th International Multidiscipinary Conference on e-Commerce and e-Government*, pages 325–330. IEEE, 2009.

[37] Damian Rusinek and Bogdan Księżopolski. Influence of ccm, cbc-mac, ctr and stand-alone encryption on the quality of transmitted data in the high-performance wsn based on imote2. *Annales UMCS, Informatica*, 11(3):117–127, 2011.

[38] Damian Rusinek and Bogdan Księżopolski. On effect of security and communication factors on the reliability in wireless sensor networks. *Journal of Sensor and Actuator Networks*, 3(1):81–94, 2014.

[39] Damian Rusinek, Bogdan Księżopolski, and Zbigniew Kotulski. On effect of the communication factors on the protocols goal availability service in high performance real-time wireless sensor networks. *Studia Informatica*, 3(32):187–197.

[40] Damian Rusinek, Bogdan Księżopolski, and Adam Wierzbicki. *International Journal of Distributed Sensor Networks.*

[41] Damian Rusinek, Bogdan Księżopolski, and Adam Wierzbicki. Aqopa: Automated quality of protection analysis framework for complex systems. In *14th International Conference on Computer Information Systems and Industrial Management Applications*, Communications in Computer and Information Science. Springer, 2015.

[42] Damian Rusinek, Bogdan Księżopolski, and Adam Wierzbicki. On the balancing security against performance in database systems. In Andrzej Kwiecien, Piotr Gaj, and Piotr Stera, editors, *22nd International Science Conference on Computer Networks*, Communications in Computer and Information Science, pages 102–116. Springer, 2015.

[43] Phyllis A. Schneck and Karsten Schwan. Authenticast: An adaptive protocol for high-performance, secure network applications. Technical report, 1997.

[44] Robert H. Shumway and David S. Stoffer. *Time Series Analysis and Its Applications*. Springer, 2011.

[45] Nicolas Sklavos, Paris Kitsos, K. Papadopoulos, and Odysseas G. Koufopavlou. Design, architecture and performance evaluation of the wireless transport layer security. *The Journal of Supercomputing*, 36(1):33–50, 2006.

[46] Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach. Managing the performance impact of web security. *Electronic Commerce Research*, 5(1):99–116, 2005.

[47] Yan Sun and Anup Kumar. Quality-of-protection (qop): A quantitative methodology to grade security services. In *ICDCS Workshops*, pages 394–399. IEEE Computer Society, 2008.

[48] Paweł Szalachowski, Bogdan Księżopolski, and Zbigniew Kotulski. Cmac, ccm and gcm/gmac: Advanced modes of operation of symmetric block ciphers in wireless sensor networks. *Inf. Process. Lett.*, 110(7):247–251, March 2010.

[49] Paweł Szałachowski, Zbigniew Kotulski, and Bogdan Księżopolski. Secure position-based selecting scheme for wsn communication- springer: Ccis. In Andrzej Kwiecien, Piotr Gaj, and Piotr Stera, editors, *CN*, volume 160 of *Communications in Computer and Information Science*, pages 289–297. Springer, 2011.