Autoreferat
informujący o zainteresowaniach i osiągnięciach w działalności naukowo-badawczej wraz z wykazem prac naukowych

1. Imię i Nazwisko

Piotr L. Cofta

2.Posiadane dyplomy, stopnie naukowe/ artystyczne – z podaniem nazwy, miejsca i roku ich uzyskania oraz tytułu rozprawy doktorskiej.

Magister inżynier informatyk (z wyróżnieniem)
Politechnika Gdańska, 1980
Generator translatorów języków adresów symbolicznych dla mikroprocesorów

Doktor nauk technicznych w zakresie informatyki
Politechnika Gdańska, 1989
Proces translacji w ujęciu przetwarzania tekstu

3. Informacje o dotychczasowym zatrudnieniu w jednostkach naukowych / artystycznych.

1980-1995 Politechnika Gdańska
1980-1981 Programista
1981-1982 Asystent, Wydział Elektroniki, Telekomunikacji i Informatyki (ETI)
1982-1991 Starszy asystent, Wydział ETI
1991-1995 Adiunkt, Wydział ETI

1990-1991 University of Oulu (Finlandia)
Wyzytujący Profesor

1993-1995 École Franco-Polonaise (Polska)
Starszy Wykładowca

2000-2004 Nokia Research Centre, USA i Finlandia
Kierowniki Zespołu Badawczego

2004-2005 MIT Media Lab Europe, Irlandia
Kierowniki Zespołu Naukowego

2005-2012 British Telecom, Wielka Brytania
Kierowniki Zespołu Badawczego

2014 University of Hertfordshire (Wielka Brytania)
Wizytujący Wykładowca

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 (Dz. U. nr 65, poz. 595 ze zm.):

Tytuł osiągnięcia naukowego

Teoria i projektowanie systemów informatycznych godnych zaufania

Publikacje

Poniższe trzy monografie całkowicie opracowane przez habilitanta stanowią osiągnięcie naukowe wskazane na potrzeby habilitacji. Szczegółowy opis treści tych publikacji jest podany w dalszej części wniosku.

Cofta, P. (2007) Trust, Complexity and Control: Confidence in a Convergent World. John Wiley & Sons.

Monografia wprowadzająca formalny model podejmowania decyzji oparty na dualiźmie zaufania i kontroli, wraz z prezentacją zastosowań modelu związanych ze współczesną technologią informatyczną.

Cofta, P. (2011) The Trustworthy and Trusted Web. Now Publishers.

Monografia wprowadzająca analityczną metodologię badań nad zaufaniem wiodącą do systematycznej analizy porównawczej zaufania i do pojęcia zaufania systemowego.

Cofta, P. (2013) The Foundations of a Trustworthy Web. Now Publishers.

Monografia opisująca szczegółowy model systemów informatycznych godnych zaufania oraz metod projektowania takich systemów na potrzeby internetu.

Wprowadzenie

Począwszy od roku 1999, badania prowadzone przez habilitanta koncentrowały się na rozwoju teorii systemów informatycznych godnych zaufania. Celem tej teorii jest usprawnienie metodologii projektowania systemów tego typu. Habilitant traktuje systemy informatyczne jako systemy socjo-techniczne. Podchodzi do problemu poprzez modelowania interakcji pomiędzy elementami socjalnymi i technicznymi systemu informatycznego w celu ujednolicenia podejścia do zaufania znanego z nauk technicznych i z socjologii. W swoich badaniach habilitant wykorzystuje swoją wiedzę akademicką i przemysłowe doświadczenie w informatyce, łącząc je ze swoimi studiami socjologicznymi.

Wybrany kierunek badań habilitanta jest motywowany obserwacją iż szereg niefunkcyjnych własności systemów informatycznych (takich jak bezpieczeństwo czy niezawodność) zależy w dużej mierze od tego czy projektanci i operatorzy tych systemów potrafią rozumować w kategoriach zaufania, zarówno zaufania społecznego jak i technicznego. Ta sama obserwacja dotyczy również akceptacji systemów informatycznych. Bieżący wzrost zainteresowania zarządzanymi usługami informatycznymi (i zarządzanymi systemami) takimi jak chmury, inteligentne miasta czy też wszechobecny Internet zwiększa tylko potrzebę na zaufanie do systemów informatycznych.

Umiejętność projektowania systemów informatycznych godnych zaufania jest zatem

jednym z większych wyzwań przed którym stoją projektanci systemów informatycznych. Jest to tym trudniejsze iż to wyzwanie jest często nie rozpoznane lub marginalizowane. Podstawowym problemem jest brak jednolitej metodologii która pozwoliłaby na analizę zaufania pomiędzy technicznymi i socjologicznymi elementami systemu. Dodatkowo, brakuje modelu który pozwoliłby na analizę odpowiadającą skali i złożoności systemów które powinny jej podlegać, t.j. na automatyzację, przyspieszenie i globalizację takiej analizy.

Definicja pojęcia systemów informatycznych godnych zaufania (ang. trustworthy information systems) przedstawiona poniżej jest zgodna z rozumieniem tego terminu przez habilitanta. Jest ona celowo przeciwstawiona systemom bazującym na zaufaniu (ang. trusted information systems).

Klasa systemów bazujących na zaufaniu jest dobrze zdefiniowana w literaturze. Obejmuje ona systemy (oraz ich elementy) którym **trzeba** zaufać (niezależnie od ich własności) aby uzyskać pożądane własności systemowe, szczególnie bezpieczeństwo. Habilitant wykonał szereg badań w tej dziedzinie, jednakże celowo się od niej tutaj dystansuje, gdyż zaufanie żądane przez takie systemy może być nieuzasadnione bądź nieodwzajemnione.

Kontrastując, systemy informatyczne godne zaufania są to systemy którym **można** (i potencjalnie należy) ufać ze względu na ich cechy i własności. Ta definicja jest zbliżona do definicji spotykanej w literaturze, z tą różnicą że celowo nie specyfikuje ona jakie cechy czynią system godnym zaufania a nie tylko n.p bezpiecznym lub niezawodnym.

W opinii habilitanta uniwersalną cechą która wyróżnia systemy godne zaufania jest ich adaptacyjna odporność (ang. adaptive resilience). Cecha ta oznacza że system pozostaje odporny na niepożądane zakłócenia w swoim środowisku podczas gdy zmienia się on na własne życzenie tak, aby ci którzy ufają systemowi mogli nadal mu ufać. Adaptacyjna odporność jest technicznym odpowiednikiem takich terminów socjologicznych jak prawość, lojalność czy też przestrzeganie systemu wartości.

Tezy osiągnięcia naukowego

Badania dotyczące systemów informatycznych godnych zaufania należą do dziedziny informatyki, lecz są również interdyscyplinarne, silnie łącząc się z socjologią. Od strony informatyki, habilitant bazuje na pracach Checklanda, na teorii bezpieczeństwa systemów informatycznych (wraz z teorią ryzyka) oraz na badaniach nad zarzadzaniem ryzykiem. Strona socjologiczna bazuje na pracach Luhmanna, Giddena i Sarlea.

W skrócie, teoria systemów informatycznych godnych zaufania może być opisana poprzez następujący zestaw tez:

(a) Zarządzane systemy informatyczne (które stanowią większość współczesnych systemów informatycznych) dzielą społeczeństwo na użytkowników i operatorów (którzy w tym modelu pełnią również rolę projektantów)
(b) Systemy informatyczne są odwzorowaniem rzeczywistości społecznej operatorów. Systemy te wpływają na fizyczną rzeczywistość użytkowników i zakłócają tworzenie ich rzeczywistości społecznej.
(c) Zaufanie jest konieczne dla udanego operowania systemem informatycznym. Zaufanie może być uzupełnione kontrolą (zarządzaniem) i analizą ryzyka. Istnienie zaufania jest pod wieloma względami bardziej opłacalne dla operatorów i użytkowników.

(d) Systemy informatyczne godne zaufania mogą być interpretowane jako techniczne połączenie pomiędzy operatorami i użytkownikami, wpływające na ich wspólną przyszłość.
(e) Zaufanie (w sensie socjologicznym) może być delegowane i reprezentowane przez techniczne elementy systemu informatycznego. Dotyczy to w szczególności elementów używanych do zagwarantowania bezpieczeństwa.
(f) Możliwe jest odwzorowania i zaprojektowanie struktury relacji bazujących na zaufaniu (uzupełnionych o kontrolę i ryzyko) która odpowiada społecznym oczekiwaniom dotyczących systemów godnych zaufania.
(g) Techniczne wymagania projektowe są konsekwencją istnienia takiej struktury i mogą być zdefiniowane dla danego systemu w oparciu o analizę tej struktury.
(h) Istnieją również alternatywne podejścia do systemów informatycznych godnych zaufania, lecz żaden z nich nie gwarantuje długoterminowej stabilizacji związku pomiędzy operatorami i użytkownikami.

Teoria i model opracowany przez habilitanta zawiera następujące oryginalne elementy.

(1) Model opisuje unikalne, interdyscyplinarne podejście do modelowania systemów socjo-technicznych. Pozwala on na zintegrowane modelowanie występujących w nich interakcji, umożliwiając użycie terminologii nauk społecznych do opisu technologii i terminologii technicznej do opisu zjawisk społecznych. Dzięki temu umożliwia on wspólną pracę informatyków i socjologów.
(2) Jest to pierwszy model który wyjaśnia istnienie szeregu niezgodnych ze sobą podejść do systemów godnych zaufania i pozwala na ich systematyzację. Wykazuje on że tylko jedno podejście jest stabilne długoterminowo.
(3) Teoria i model są niezależne od funkcji przypisanych systemowi i nie wymagają one aby system spełniał jakąkolwiek specyficzną funkcję, maksymalizował jakikolwiek zysk lub służył specyficznym celom społecznym. Pozwala to na analizę dużej grupy systemów, w tym także tych które nie były dotychczas szczegółowo analizowane ze względu na ich odczuwany antyspołeczny charakter.
(4) Teoria postuluje iż zaufanie, jakkolwiek niewątpliwie korzystne, nie jest konieczne dla wszystkich elementów działającego systemu informatycznego. Możliwe jest także operowanie przy użyciu kontroli, używając analizy ryzyka przy podejmowaniu decyzji. Dzięki temu teoria pozwala na bezstronną, pozbawioną emocji, analizę zaufania, szczególnie biorąc pod uwagę istniejące praktyki przemysłowe.
(5) Model dostarcza strukturę i formalizację które pozwalają na systematyczną analizę szeregu zjawisk znanych ze współczesnych systemów informatycznych. Zjawiska takie jak wirtualizacja tożsamości, inwigilacja elektroniczna, systemy cyber-techniczne czy też odczuwalne braki w bezpieczeństwie systemów informatycznych mogą być wyjaśnione w ramach modelu.
(6) Model oraz teoria umożliwiają przeprowadzenie szeregu istotnych analiz dotyczących przyszłości systemów. Między innymi mogą być one używane do przewidywania stopnia społecznej akceptacji systemów informatycznych, do wyszukiwania ich słabych punktów, do polepszenia ich bezpieczeństwa oraz dla usprawnienia zarządzania ryzykiem.

Omówienie dorobku naukowego

Teoria systemów informatycznych godnych zaufania jest tematem trzech monografii [1], [2] i [4] opublikowanych w przeciągu sześciu lat. Monografie te są omówione poniżej w kolejności chronologicznej.

Cofta, P. (2007) Trust, Complexity and Control: Confidence in a Convergent World. John Wiley & Sons.

Pierwsza monografia [4] podsumowuje dotychczasowe wyniki badań i postuluje model w którym zaufanie do systemów socjo-technicznych jest uzupełnione elementem kontroli. Model ten ma szereg zalet: może być on stosowany do modelowana znacznej klasy systemów socjo-technicznych, pozwala na modelowanie rzeczywistych sytuacji, a także obejmuje analizę systemów o różnej wielkości i na różnym stopniu szczegółowości. Podstawowym tematem monografii jest formalizacja decyzji dotyczącej zaufania wiodąca do wymagań dotyczących architektury systemów informatycznych. Monografia wprowadza szereg pojęć i koncepcji które były stosowane w późniejszych monografiach.

Monografia składa się z 16 rozdziałów i jest podzielona na trzy części. Trzynaście rozdziałów zostało specjalnie napisanych na potrzeby tej monografii podczas gdy trzy rozdziały bazują na wcześniejszych publikacjach, poszerzonych i uaktualnionych na potrzeby monografii.

Pierwsza część monografii jest poświęcona wprowadzeniu do tematu oraz formalizacji modelu. Rozdział pierwszy definiuje problem, wprowadza terminologię i formalną notację stosowaną w monografii. Zawiera on także przegląd literatury. Rozdział 2 wprowadza formalny model w którym zaufanie jest uzupełnione kontrolą i definiuje jego hierarchiczną naturę. Trzeci rozdział dyskutuje istniejące metody pomiaru zaufania i wprowadza formalną notację stosowaną dla opisania wyników takich pomiarów, stosowaną w modelu. Rozdział 4 porównuje model z istniejącymi modelami zaufania (rozszerzając prace z [22]), demonstrując iż model postulowany w monografii jest ich generalizacją. Rozdział 5 dyskutuje czasową charakterystykę zaufania, wprowadzając pojęcie wieloetapowego procesu zaufania, i dyskutując to pojęcie z punktu widzenia teorii gier. Rozdział 6 dyskutuje i formalizuje nieufność, bazując na [24].

Druga część monografii jest poświęcona analizie wpływu komunikacji cyfrowej na zaufanie w kontekście przedstawionego modelu. Rozpoczyna się ona od rozdziału 7 który dyskutuje wpływ technologii cyfrowej na budowę zaufania. Temat ten będzie później rozwijany w [1] i [2]. Rozdział ten wprowadza tezę iż zaufanie w systemach technicznych jest odwzorowaniem zaufania społecznego i ustanawia podstawy socjo-technicznego podejścia do problemu. Następny rozdział analizuje bezpieczeństwo systemów informatycznych z punktu widzenia modelu. To pierwsze praktyczne zastosowaniu modelu demonstruje fundamentalną i niezastępowalną wartość zaufania. Rozdział 9 ukazuje zastosowanie modelu do modelowania sieciowych struktur zaufania, dyskutując przy tym problem przechodności zaufania. Przedstawia on klasyfikację struktur sieciowych i wyniki modelowania i symulacji. Rozdział 10 używa modelu do systematycznej analizy możliwych ataków na systemy bazujące na zaufaniu. Ostatni rozdział tej części monografii proponuje użycie technologii, inspirowanej modelem, do naprawy relacji bazujących na zaufaniu.

Rozdział 12 otwiera ostatnią część monografii poświęconą związkom pomiędzy modelem zaufania i różnymi aspektami zintegrowanej komunikacji cyfrowej. Ukazuje on iż podstawy pojęć 'zaufania' i 'bycia godnym zaufania' przypuszczalnie nie ulegną zmianie, lecz że sposób ich wyrażania będzie inny. Rozdział 13 bazuje na [26]. Dyskutuje on handel elektroniczny i możliwości ustanowienia i utrzymania zaufania przy użyciu komunikacji cyfrowej. Rozdział ten był wykorzystany później w nieopublikowanych pracach dla eBay. Rozdział 14 analizuje problem prywatności w zintegrowanej komunikacji cyfrowej. Wykorzystuje on model do zaproponowania protokołu identyfikacji który zachowuje prywatność. Następny rozdział analizuje zarządzanie zaufaniem, pokazując iż model może

być w przyszłości stosowany do usprawnienia niektórych aspektów zarządzania zaufaniem. Ostatni rozdział 16 studiuje potencjalne ekonomiczne skutki zastosowania modelu do zapewnienia bezpieczeństwa zintegrowanej komunikacji.

Cofta, P. (2011) The Trustworthy and Trusted Web. Now Publishers.

Pierwsza monografia postulowała że tylko ci którzy są godni zaufania (zarówno ludzie jak i technologie) powinni być nim obdarzeni. W związku z tym druga monografia [2] przenosi ciężar analizy z problemu zaufania na problem bycia godnym zaufania. Obejmuje ona szczegółową socjo-techniczną analizę pojęcia bycia godnym zaufania, w szczególności w odniesieniu do internetu i globalnych systemów informatycznych. Przedstawia ona unikalny socio-techniczny model i studiuje struktury zaufania zgodne z tym modelem. Model zaproponowany w monografii pozwala na systematyczną analizę szeregu pozornie sprzecznych podejść do systemów informatycznych godnych zaufania. Pokazuje on że tylko jedno podejście jest stabilne i że to podejście powinno być podstawą metodologii tworzenia systemów informatycznych godnych zaufania.

Druga monografia składa się z dziewięciu nowych, specjalnie dla niej napisanych rozdziałów. Należy podkreślić tutaj nietypowy związek czasowy pomiędzy tą oraz ostatnią monografią. Ostatnia monografia [1] jest w istocie wstępem do monografii omawianej w tym miejscu. Jednakże wstęp ten został wydany później niż monografia do której się on odnosi.

Pierwszy rozdział opisuje zakres, oraz precyzuje tezy i definicje używane w monografii. Drugi rozdział zawiera przegląd literatury związanej z tematem, włącznie z przeglądem bieżących projektów badawczych. Rozdział ten wprowadza również systematyką podejść do zaufania która będzie wykorzystywana w kolejnych rozdziałach. Trzeci rozdział zawiera krótkie wprowadzenie do socjo-technicznego modelu społeczeństwa i technologii stosowanego w monografii. Rozdział ten wprowadza fundamentalne pojęcia takie jak rozróżnienie pomiędzy operatorami i użytkownikami technologii i strukturalizuje relacje oparte na zaufaniu. W związku z tym iż pełen model został opublikowany później, w monografii [1], rozdział ten czyni monografie niezależnymi od siebie.

Rozdział 4 analizuje pytanie czy bycie godnym zaufania może być przypisane technologii. Dyskutuje on tezę zaprezentowaną w [4] iż zaufanie do technologii jest reprezentacją zaufania do systemu społecznego który operuje tą technologią. Rozdział 5 dyskutuje atrybuty zaufania i bycia godnym zaufania, w szczególności różne formy zależności czasowej, szerzej opisane w [9]. Następny rozdział demonstruje iż struktury zaufania zidentyfikowane w rozdziale drugim są zgodne ze strukturami zdefiniowanymi przez model i że znajdują one odbicie w praktyce. Rozdział 7 przedstawia wpływ sformułowanego modelu na proces projektowania systemów informatycznych godnych zaufania. Postuluje on iż podstawowym celem tych systemów jest stabilizacja związku pomiędzy operatorami i użytkownikami systemu. Na tej podstawie rozdział definiuje pożądane cechy takiego systemu. Kolejny rozdział analizuje charakterystyki czasowe zaufania w kontekście technologii informatycznych. Końcowy rozdział 9 prezentuje wnioski i zamyka monografię.

Cofta, P. (2013) The Foundations of a Trustworthy Web. Now Publishers.

Ostatnia, trzecia monografia [1] przedstawia wyczerpujący opis modelu stosowanego w drugiej. Ten socjo-techniczny model, opracowany przez habilitanta, koncentruje się na modelowaniu zależności pomiędzy społeczeństwem a systemami informatycznymi. Jest on o wiele bardziej szczegółowy w porównaniu ze skrótowym opisem zawartym w [2].

Model ten bazuje w znacznym stopniu na teorii systemów społecznych, teorii rzeczywistości społecznej i semiotyce. Jakkolwiek podstawowym celem monografii była prezentacja tego modelu, zawiera ona również rozszerzoną dyskusję dotyczącą technicznych cech internetu które mogą uczynić go bliższym potrzebom społecznym w sensie analizowanej teorii.

Monografia składa się z 14 rozdziałów napisanych specyficznie na jej potrzeby, tylko w jednym miejscu nieznacznie bazując na [19]. Pierwszy rozdział wprowadza terminologię stosowaną w monografii oraz dyskutowane w niej tezy. Jako że monografia bazuje w znacznym stopniu na specyficznej teorii systemów społecznych, drugi rozdział dyskutuje zalety i ograniczenia tego podejścia, demonstrując iż wybrany model jest szczególnie odpowiedni dla tego typu analizy.

Trzeci rozdział stanowi wprowadzenie do tego modelu i do innych potrzebnych teorii, dyskutowanych w kontekście współczesnych systemów informatycznych. Następny rozdział pozycjonuje proponowaną teorię w kontekście dynamiki zmian w systemach socjo-technicznych. Kolejny rozdział wprowadza podstawowy element monografii, zunifikowany model rzeczywistości społecznej i internetu opracowany przez habilitanta.

Kolejne rozdziały dotyczą bardziej szczegółowej analizy modelu. Wpływ systemów informatycznych na trzy typy systemów społecznych jest analizowany w rozdziałach 6, 7 i 8. Habilitant wykazał tutaj iż wpływ systemów informatycznych na systemy społeczne zależy od typu systemu społecznego. Zatem analiza konkretnej sytuacji powinna zawsze brać pod uwagę wszystkie typy systemów.

Rozdział 9 dyskutuje wpływ technologii informatycznej na problem tożsamości i identyfikacji. Pokazuje on że tożsamość jest istotnym choć często niedocenianym elementem systemów społecznych (oraz modelu) oraz że technologie informatyczne mają na nią znaczny wpływ. Choćby z tego tylko powodu analiza modelu powinna zawierać dyskusję dotyczącą tożsamości. Rozdział 10 wprowadza formalny opis modelu, stosując notację zbliżoną do współczesnych języków programowania, z myślą o przybliżeniu modelu profesjonalnym informatykom - projektantom, twórcom i operatorom systemów informatycznych.

Rozdziały 11, 12 i 13 zawierają szczegółową propozycję dotyczącą zbudowania internetu godnego zaufania - propozycję która w dużej mierze inspirowała habilitanta tak jak inspirowała ona szereg innych profesjonalistów. Rozpoczyna się ona od dogłębnej analizy celu istnienia internetu (rozdział 11) która demonstruje iż internet godny zaufania jest możliwy, lecz może on wyglądać inaczej niż jest to obecnie oczekiwane. Rozdział 12 zawiera praktyczne zalecenia projektowe dotyczące takiego internetu. Rozdział 13 dyskutuje rozdźwięk pomiędzy obecnym stanem internetu i stanem wynikającym z zastosowania teorii. Ostatni rozdział podsumowuje i zamyka monografię.

5. Omówienie pozostałych osiągnięć naukowo - badawczych (artystycznych).

Osiągnięcia naukowo-badawcze przedstawione poniżej zostały uzyskane po doktoracie. Wcześniejsze osiągnięcia nie są uwzględnione nawet jeżeli były związane z przedstawionym tematem prac.

Przez większość swojej kariery naukowej habilitant pracował w przemysłowych ośrodkach

badawczych. Z tego powodu część jego prac ma charakter tajny lub poufny. Szczegóły tych prac nie są tutaj omawiane.

Działalność naukowo-badawcza

Zainteresowanie habilitanta problemem zaufania w kontekście systemów informatycznych sięga roku 1999. Pozornie prosty problem systemów informatycznych godnych zaufania wymagał szczegółowych, interdyscyplinarnych badań które zajęły prawie 15 lat. Jakkolwiek w tym czasie uwaga habilitanta przesuwała się pomiędzy różnymi wątkami badań, ich zasadniczy cel pozostawał niezmienny. Poniższy rozdział przedstawia przegląd osiągnięć naukowo-dawczych habilitanta które doprowadziły do seri monografii omówionych wcześniej w tym wniosku.

Załączona lista dorobku naukowego zawiera ponad 60 pozycji (wliczając patenty i prezentacje). W zawiązku z tym konieczne było wprowadzenie pewnej struktury prezentacji tego dorobku. Ze względu na złożoność problemu naukowego, habilitant podchodził do niego z wielu stron aby ostatecznie uzyskać spójny zestaw tez naukowych. Z tego powodu poniższe omówienie dorobku naukowego jest podzielone na szereg wątków badawczych które razem tworzą teorię systemów informatycznych godnych zaufania. Szczegółowe omówienie poszczególnych prac jest podane w załączniku.

Jakkolwiek habilitant był w stanie zachować niezależność badawczą w temacie kierunku badań, formy publikacji w dużej mierze były determinowane przemysłowym środowiskiem pracy habilitanta. Z tego powodu, szczególnie w początkowym okresie prac, publikacje mają formę patentów i standardów a nie artykułów czy publikacji konferencyjnych.

Poniższe zestawienie uwzględnia sześć wątków badawczych i opisuje dorobek badawczy osiągnięty w ramach każdego z nich. Koncepcyjnie, wątki 1, 2 i 3 są najwcześniejsze. Wątki 4 i 5 stanowią centralną część dorobku, zbudowaną w oparciu o osiągnięcia wcześniejszych wątków badawcze. Ostatni wątek 6 jest bieżącym, potencjalnie praktycznym, zastosowaniem tematu 5.

Wątek 1. Bycie godnym zaufania jako cecha elementu systemu

Jest to historycznie pierwszy wątek zainteresowań habilitanta. Wątek ten koncentruje się na wykorzystaniu zaufania do elementów systemów informatycznych. Zakłada on, że system informatyczny godny zaufania można skonstruować poczynając od jednego elementu godnego zaufania, zakładając że taki element może podejmować decyzje dotyczące współpracy z pozostałymi elementami. Taki element jest obdarzony zaufaniem (i reprezentuje zaufanie) projektantów i użytkowników systemu.

Podejście reprezentowane w tym wątku bazuje na podejściu znanym z badań nad bezpieczeństwem systemów informatycznych. Podstawowa różnica polega na akcentowaniu przez habilitanta konieczności wykazania iż element jest godny zaufania przez wszystkie zainteresowane strony, a nie że jest on obdarzony ślepym zaufaniem.

Ze względu na przemysłowy charakter badań, wczesne prace miały głównie format patentów i standardów przemysłowych a nie publikacji naukowych. Typowym przykładem podejścia jest patent [40] opisujący metodę pozwalającą jednemu modułowi oprogramowania wybrać inny moduł realizujący pożądaną funkcję w oparciu o ocenę zaufania do tego modułu. Zbliżony do niego patent [41] przedstawia metodę zwiększenia zaufania do oprogramowania poprzez zastosowanie podpisu cyfrowego. Metody ta stały

się popularne wraz z rozwojem Internetu gdzie zaufanie stało się ważnym czynnikiem wyboru dostawcy usług (n.p. Web Services) oraz z rozwojem systemó operacyjnych godnych zaufania.

Patent ten jest uznawany przez jego właściciela za ważny, gdyż większość platform dostarczających usługi internetowe potencjalnie z niego korzysta. Ze względu na dobro publiczne związane z rozwojem usług internetowych, właściciel patentu nie zdecydował się na dochodzenie swych praw.

Patent [39] wprowadza do tematyki badań element ludzki, pozwalając technologii wspomagać (lecz nie zastępować) proces decyzyjny. Patenty te prezentują sposoby przy użyciu których urządzenia techniczne mogą prezentować swoją ocenę zaufania technologii otaczającej człowieka. Patenty te są związane z publikacją [29] która opisuje urządzenie i sposób jego działania.

Zarówno patenty jak i publikacja są charakterystyczne dla ówczesnego kierunku prac w którym habilitant był zainteresowany wykorzystaniem telefonów komórkowych jako osobistych urządzeń godnych zaufania. Koncepcja ta jest nadal aktywnie rozwijana przez szereg firm. Pozostałe elementy tych prac były opatentowane osobno i nie są tutaj przedstawione.

Standaryzacja [64] i prezentacja [57] koncentrują się na innym aspekcie tego samego nurtu badań. Habilitant analizował tutaj możliwości i ograniczenia płynące z użycia istniejących elementów godnych zaufania (głównie karty SIM) do zbudowania urządzeń mobilnych i systemów informatycznych godnych zaufania. Opracowany standard jest nadal stosowany w szeregu telefonów.

Udział w tym konkretnym standardzie jest również istotny z innego punku widzenia. Po raz pierwszy habilitant użył tutaj idei architektury zaufania i jej socjo-technicznej zgodności. Jakkolwiek idea ta została opracowana tylko w formie wewnętrznej publikacji, miała ona istotny wpływ na wynik standaryzacji i na sam jej proces.

Patent [35] koncentruje się na wykorzystaniu elementu godnego zaufania istniejącego w urządzeniu mobilnym poprzez szereg aplikacji które mogą nie ufać sobie wzajemnie. Patent ten został wykorzystany przy projektowaniu specjalnej wersji karty SIM.

Idea 'łączenia domen zaufania' [30] skonsolidowała wyniki wcześniejszych prac. Dała ona początek koncepcji socjo-technicznej architektury w której domeny definiowane przez niezgodne opinie na temat zaufania mogą współpracować pod warunkiem iż istnieje element który jest obdarzony zaufaniem przez więcej niż jedną domenę. Zgodnie z ówczesnym zainteresowaniem habilitanta, rola ta miała przypaść telefonowi komórkowemu.

Publikacja ta rozpoczęła cykl prac nad strukturalizacją różnych koncepcji zaufania, zarówno w sensie społecznym jak i technicznym. Wpłynęła ona również na badania dotyczące architektur zaufania i na strukturę TERM - narzędzia pozwalającego na uchwycenie struktur zaufania.

Patent [37] a także publikacja [27] przeniosły ciężar badań ze statycznej architektury systemu w kierunku analizy dynamiki relacji pomiędzy elementami systemu. Bazując na [30], prace te postulują istnienie specyficznego protokołu który powinien wspomagać utrzymanie zaufania w przeciągu dłuższego okresu czasu. Zakładają one iż elementy

systemu będą również w stanie zmienić swoje decyzje pod wpływem nowych dowodów. Prace te są pierwszym miejscem w którym habilitant zainteresował się nieufnością jako przeciwieństwem zaufania. Zainteresowanie to z czasem doprowadziło do głębszych badań nad tym zjawiskiem.

Po kilkuletniej przerwie habilitant kontynuował ten kierunek badań, ponownie w formie patentów. Patent [38] pokazuje jak zaufanie związane z kartą SIM może objąć cały telefon komórkowy. Patenty [34], [33] i [32] oraz [36] pokazują jak zaufanie związane z jedną kartą SIM może być rozszerzone na całą grupę urządzeń.

Niedawny patent [31] ponownie wykorzystuje ideę systemu godnego zaufania zbudowanego na podstawie elementu godnego zaufania. Tym razem obszarem zainteresowań habilitanta są energie odnawialne. Patent postuluje wyposażenie paneli słonecznych we wbudowane układy elektroniczne które przekształciłyby panele w samozasilające, godne zaufania elementy systemu informatycznego. Takie panele mogłyby same podejmować decyzje dotyczącą współpracy z innymi elementami systemu energetycznego.

Patent ten stał się podstawą utworzenia małej firmy która pracuje nad jego wdrożeniem. Zalety tego patentu są doceniane przez wzrastającą liczbę potencjalnych klientów.

Wątek 2. Bycie godnym zaufania jako cecha socjo-technicznej architektury systemu

Ten wątek badań analizuje zaufanie (a także bycie godnym zaufania) jako strukturalną cechę systemu, w szczególności systemu socjo-technicznego takiego jak system informatyczny. Bazuje on na koncepcji 'architektury zaufania', t.j. takiej technicznej architektury która jest strukturalnie zgodna z odpowiadającą jej strukturze społecznego zaufania. Zgodność tych struktur przejawia się tym iż nikt nie jest zmuszony do ufania poprzez system informatyczny elementom które nie są z jego punktu widzenia godne zaufania w sensie społecznym.

W ramach tego wątku badań habilitant zdefiniował formalnie cechy struktury systemów informatycznych które powinny spowodować uznanie ich za godnych zaufania. Ponadto habilitant wykonał szereg badań dotyczących poszczególnych obszarów zastosowań informatyki (n.p. zarządzanie tożsamością). Badania te miały na celu zweryfikowanie istnienia strukturalnej zgodności i wypracowanie zaleceń dla projektantów systemów.

Badania przeprowadzone w ramach tego wątku badawczego były początkowo inspirowane pracami nad standardem [64], ale szybko przekształciły się w niezależny wątek badawczy. Początkowo struktury zaufania były interpretowane w terminach socjologicznych które powinny być odtworzone przez struktury techniczne. Z tego powodu dyskusja na temat technicznych własności systemów była poprzedzana dyskusją na temat społecznej struktury zaufania zawiązanego z danym systemem. Podobnie techniczny model systemu był poprzedzany modelem społecznego zaufania.

To podejście było przetestowane przez habilitanta dwukrotnie [63] [66] w związku z dwoma międzynarodowymi standardami których habilitant był współautorem. W obu wypadkach badania wykazały niezgodność pomiędzy zakładaną strukturą zaufania społecznego i planowaną strukturą zaufania odwzorowanego w technologii. Wyniki badań pozwoliły na wprowadzenie zmian do planowanej architektury technicznej zwiększając w ten sposób bezpieczeństwo systemów informatycznych i powiększając szanse ich społecznej akceptacji.

Badania habilitanta nad ewolucją systemów społecznych i technicznych wykazały iż nie tylko społeczne struktury zaufania powinny definiować techniczną architekturę systemu, lecz również że techniczne zaufanie może przedefiniowywać struktury społeczne. Ta propozycja nadała początek badaniom nad systemami 'zaprojektowanymi dla zaufania' (ang. 'designed for trust') [14] [15]. W tych systemach społeczne i techniczne cechy systemów mogą być analizowane równocześnie w celu doprowadzenia do selektywnego wzrostu uzasadnionego zaufania (t.j zaufania tym elementom które są godne zaufania). Prace te pokazały również iż dalszy postęp jest możliwy tylko poprzez sformułowanie zunifikowanego socjo-technicznego modelu zaufania, dając początek osobnemu wątkowi badawczemu.

Rozdział książki [8] przedstawia wyniki tego tematu badawczego w sposób najbardziej kompletny. Formalizuje on socjo-techniczne cechy systemów i dzięki temu pozwala on na analizę szerokiej klasy systemów. Habilitant zastosował tą teorię do analizy systemów informatycznych służących zarządzaniu tożsamością [16]. Wyniki analizy pozwoliły na wykazanie niezgodności w strukturach zaufania które mogłyby uniemożliwić akceptację nowego systemu kart identyfikacyjnych. Metodologia użyta w tej analizie została sformalizowana w [7] poprzez powiązanie jej z metodologią systemów miękkich (ang. soft systems).

Niedoskonałością tej metodologii było to, iż wprowadzała ona nieciągłość do praktyki projektowania systemów informatycznych. Analiza zaufania nie była zgodna z ustaloną praktyką analizy ryzyka i wymagała specjalistycznych umiejętności. Wyzwanie to wymagało zmodyfikowania metodologii w taki sposób aby była ona bardziej zgodna z praktyką.

Do pewnego stopnia zostało to osiągnięte poprzez wpisanie tej metodologii w kontekst modelowania bezpieczeństwa systemów informatycznych a także poprzez wykazanie jej szerszej przydatności w zarządzaniu przedsiębiorstwem [6], [12]. Proces ten jest obecnie kontynuowany w postaci osobnego wątku badawczego - TERM.

Wątek 3. Społeczna percepcja technicznych systemów godnych zaufania

Społeczna definicja zaufania posiada wiele rozbieżnych interpretacji które utrudniają jednoznaczną identyfikację technicznych cech czyniących system informatyczny godnym zaufania. Z tego powody habilitant uznał za konieczne aby przeanalizować różnorodne podejścia do społecznego zaufania w celu wyłonienia ich cech wspólnych.

Prace związane z tym wątkiem badawczym mają postać studiów nad poszczególnymi obszarami zainteresowań. Ich forma jest różnorodna, od analizy teoretycznej poprzez studia etnograficzne i modelowanie do praktycznych interwencji. Wyniki prac tego tematu badawczego mają silny wpływ na teorię systemów godnych zaufania, szczególnie na model przedstawiony w [2].

Handel elektroniczny jest tym obszarem zainteresowań habilitanta który jest szczególnie interesujący z puktu widzenia badań nad zaufaniem. Akceptacja tranzakcji w handlu elektronicznym zależy nie tylko od zaufania do technologii używanych systemów informatycznych, lecz także od zaufania do organizacji i ludzi którzy operują i używają tych systemów. W ramach serii publikacji [23], [25], [26], [53] habilitant dokonał analizy tego obszaru zastosowań, sformułował i zweryfikował specyficzne modele [4] i zaproponował szereg zmian mających na celu poprawienie struktur zaufania. Habilitant dokonał również

(niepublikowanej) interwencji w procesy jednej z największych firm zajmujących się handlem elektronicznym.

Zainteresowania habilitanta cały czas skupiały się na technologii komunikacji mobilnej. Z tego powodu prezentacja [51] analizowała rynek aplikacji mobilnych z punktu widzenia zaufania. Wirtualizacja systemów informatycznych i jej wpływ na zaufanie została zanalizowana w prezentacji [54].

Osobna grupa prac jest poświęcona związkom pomiędzy zaufaniem i innymi pojęciami społecznymi. Celem tych prac było rozpoznanie różnic i wzajemnych zależności pomiędzy tymi pojęciami. Tożsamość i zarządzanie tożsamością było tematem prac [21], [50] i [59]. Zależności pomiędzy prywatnością i zaufaniem zostały przeanalizowane w [20] i [52]. Nieufność została przeciwstawiona zaufaniu w [24]. Praca [19] przedstawiająca analizę zaufania do wybranej firmy wprowadziła elementy analizy użyte później w teorii systemów godnych zaufania, szczególnie w modelu przedstawionym w [1]

Seria prac etnograficznych [11], [13], [18] [56] wzbogaciła obserwacje dotyczące społecznych struktur zaufania. Pozwoliła ona również na przetestowanie wczesnych hipotez poprzez projektowanie interakcyjne systemów informatycznych używanych w badaniach. Wykazała ona znaczną różnorodność społecznych heurystyk dotyczących oceny zaufania, wskazując na konieczność teorii systemów godnych zaufania która będzie zbudowana w oparciu o zaawansowaną teorię społeczną.

Interesująca auto-etnograficzna prezentacja [55] analizuje zaufanie w ramach interdyscyplinarnego zespołu badawczego który uczynił zaufanie tematem swych badań. Jakkolwiek praca ta, a także prace [48] i [49] odchodzą od głównego nurtu badań nad systemami informatycznymi, to pozwoliły one do wykazania iż teoria rozwijana przez habilitanta ma potencjalnie zasięg wykraczający poza systemy infromatyczne. Niedawno opublikowany dokument [58] kontynuuje tą linię prac.

Książka [3] dokumentuje wyniki obszernych badań etnograficznych dotyczących stosunków pomiędzy społeczeństwem i technologią informatyczną, ze szczególnym uwzględnieniem zaufania i systemów godnych zaufania. Badania te miały istotny wpływ na szereg elementów teorii i były głównym źródłem danych empirycznych służących jej weryfikacji. Badania te (a także książka) były często używane przez rząd Wielkiej Brytanii w czasie dyskusji nad społeczną akceptacją technologii.

Rozdział w encyklopedii [5] może służyć jako krótkie podsumowanie ukazujące różnorodność podejść do zaufania które były analizowane przez habilitanta. Jest on kontynuacją prac nad modelowaniem zaufania przedstawionych w [2] a także etnograficznych studiów prezentowanych w [3].

Wątek 4. Modelowanie zaufania

Dalszy rozwój badań habilitanta był ograniczony poprzez brak właściwego formalnego, zunifikowanego modelu systemów godnych zaufania, zbudowanego w oparciu o socjologię lecz pozwalającego na wnioskowanie w sferze technicznej. Jakkolwiek wcześniejsze prace takie jak [7] czy [8] postulowały pewne modele formalne, to nie pozwalały one na uwzględnienie różnorodności heurystyk związanych z zaufaniem. Spowodowało to konieczność osobnego wątku badawczego poświęconego specjalnie modelom zaufania.

Początkowo prace były skoncentrowane na modelowaniu procesu decyzyjnego wiodącego do decyzji o zaufaniu. Celem ich było uchwycenie różnorodności heurystyk i sformalizowanie ich w stopniu pozwalającym na automatyzację wspomagania decyzji [28]. Podejście to wyrastało z koncepcji architekturę zaufania i poszerzało badania nad elementami godnymi zaufania. Szereg studiów (niepublikowanych) kontynuowało to podejście które obecnie ma wpływ na TERM.

Seria dokumentów [60], [61] i [62] pozwoliła habilitantowi na sformułowanie problemu i na przeanalizowanie socjo-technicznej natury tego problemu. Są one łącznikiem pomiędzy wcześniejszymi pracami nad procesem podejmowania decyzji a późniejszymi, skoncentrowanymi na modelowaniu całości procesów związanych z zaufaniem. Dokumenty te były użyte przez habilitanta do ukierunkowania badań swojej grupy badawczej.

Osobna seria publikacji analizowała istniejące modele zaufania w celu wychwycenia elementów wspólnych które mogłyby stać się podstawą zunifikowanego modelu. Systematyczna analiza porównawcza przedstawiona w [22] doprowadziła do bardziej szczegółowej analizy przedstawionej w [4]. Alternatywne podejście bazujące na teorii gier [9] pozwoliło na rozróżnienie pomiędzy różnymi dynamikami relacji opartych na zaufaniu, przyczyniając się do wzbogacenia modelu.

Pierwsze zunifikowane podejście do modelowania jest przedstawione w [17]. Jest cechą charakterystyczną tego modelu iż zarówno społeczeństwo jak i system informatyczny są modelowane razem z użyciem jednolitej terminologii. Model ten stanowi intelektualną podstawę modelu prezentowanego w [1], oraz teorii systemów godnych zaufania.

W celu opracowania pełnego zunifikowanego modelu, habilitant podjął znaczne studia w dziedzinie teorii formalnych modeli społecznych. Celem było wyszukanie modelu który pozwoliłby na kontynowanie podejścia zapoczątkowanego w [17]: zunifikowanego modelu gdzie społeczeństwo i system informatyczny mogą być dyskutowane jednocześnie. Model opracowany przez habilitanta został ostatecznie przedstawiony w [1], wraz z dyskusją dotyczącą motywacji, alternatywnych rozwązań oraz uzasadnienia wyboru.

Wątek 5. Teoria systemów godnych zaufania

Wątek ten jest podtawą wniosku habiliatyjnego i został szegółowo omówiony wcześniej.

Wątek 6. Zarządzanie ryzykiem z uwzględnieniem zaufania

Teoria systemów informatycznych godnych zaufania satysfakcjonuje oczekiwania naukowe, lecz jest ona zbyt odległa od praktyki projektów informatycznych. Z tego powodu habilitant skierował obecnie swoje zainteresowania w stronę praktycznego zastosowania opracowanego modelu. Bazując na swoich wcześniejszych obserwacjach, habilitant zadecydował iż najlepsza droga do przybliżenia modelu bazującego na analizie zaufania wiedzie poprzez zarządzanie ryzykiem dla potrzeb bezpieczeństwa systemów informatycznych. Zarządzanie ryzykiem jest dobrze znaną praktyką zaakceptowaną zarówno przez projektantów jak i operatorów systemów. Podstawowy problem polega na tym, iż zarządzanie ryzykiem ignoruje problem zaufania.

Bieżący wątek badań habilitanta koncentruje się na zarządzaniu ryzykiem z uwzględnieniem zaufania (ang. Trust-Enhanced Risk Management: TERM). Jest to metodologia opracowana przez habilitanta która wprowadza zaufanie jako równoprawny

składnik analizy bazującej dotychczas na pojęciach ryzyka i kontroli. Metodologia ta pozwala na wprowadzenie analizy zaufania bez znacznego modyfikowania istniejących procesów. Metodologia TERM składa się z matematycznie sformalizowanej analitycznej bazy uzupełnionej szeregiem narzędzi organizacyjnych.

TERM bazuje na obserwacji habilitanta która została uwzględniona w [4] i w pełni wyrażona w [1]: najpełniejsza analiza zaufania powinna zawierać również analizę jednego z jego przeciwieństw. Dla potrzeb projektowania systemów informatycznych typowym przeciwieństwem jest kontrola. Dla potrzeb podejmowania decyzji jest to ryzyko. Z tego powodu TERM bazuje na łącznej analizie zaufania, kontroli i ryzyka.

Celem TERM jest umożliwienie szybkiej analizy konkretnej sytuacji, n.p decyzji projektowej, architektury systemu lub też usprawnień bezpieczeństwa systemów informatycznych. W tych sytuacjach TERM pozwala na pogłębioną socjo-techniczną analizę sytuacji bez potrzeby angażowania ekspertów. Dotychczasowe eksperymenty wykazały iż TERM pozwala na osiągnięcie wyników które wzbogacają i uzupełniają typową analizę ryzyka.

TERM pozwala na opisanie analizowanej sytuacji w terminach struktury zaufania uzupełnionego o kontrolę, w sposób wprowadzony przez [4]. Narzędzia wspomagające, opracowane na podstawie badań habilitanta nad społeczną oceną zaufania (wprowadzone w [3] i rozbudowane w [2]) pozwalają na ocenę czy specyficzny element jest wystarczająco godny zaufania. Na tej podstawie analiza może wskazać niepożądane struktury, sytuacje nieuzasadnionego zaufania lub też niepożądane elementy systemu. Formalny model stosowany przez TERM jest używany zarówno w czasie konstruowania modelu jak i do jego analizy.

Ponieważ badania nad TERM są nadal w stosunkowo wczesnej fazie, były one prezentowane dotychczas tylko w formie serii prezentacji konferencyjnych [43], [44], [42], [45], [46] dokumentujących stopniowy postęp prac. Przykład praktycznego zastosowania TERM do analizy zaufania w zarządzaniu bezpieczeństwem krytycznej infrastrutury jest przedstawiony w [9]. Szczegółowe publikacje opisujące TERM są obecine w fazie przygotowawczej.

W opinii habilitanta TERM jest szczególnie istotny w zastosowaniach do systemów cyber-technicznych (ang. cybertechnical systems), znanych również jako systemy inteligentne (ang. smart systems), t.j, do systemów gdzie tradycyjne technologie są uzupełniane poprzez technologie informatyczne. Analiza ryzyka w tych systemach napotyka problemy wynikające z różnej interpretacji i niezrozumienia pomiędzy tradycyjną technologią oraz informatyką. Swoje obserwacje habilitant zaprezentował na konferencji [47] oraz w trakcie prowadzenia szeregu innych międzynarodowych konferencji.

Prowadzenie i udział w programach badawczych

Podczas swojej pracy w firmach Elektrobit, NEP i Nokia (do roku 2004) habilitant brał udział w szeregu wewnętrznych programach badawczych. Programy te głównie dotyczyły handlu elektronicznego, płatności mobilnych, bezpieczeństwa urządzeń przenośnych oraz internetu mobilnego. Z punktu widzenia pracy naukowej istotny jest udział habilitanta w dwóch pierwszych europejskich projektach płatności mobilnych (w Schiphol i Ennis), udział w standaryzacji internetu mobilnego (WAP/OMA) i środowiska Java (JSR177), czy też udział w pierwszym projekcie portfela elektronicznego.

W czasie pracy w Media Lab Europe (2004-2005) habilitant prowadził swoją własną grupę badawczą 'Trusted Technologies' oraz swój własny projekt badawczy o tym samym tytule. Ponadto habilitant brał udział w projekcie badawczym 'TRUST-E: Teaching and Research in a Ubiquitous Secure Telecommunications Environment' realizowanym przy współpracy z Trinity College Dublin.

W czasie pracy w British Telecom (2005-2012) habilitant zarządzał i uczestniczył w szeregu wewnętrznych programach badawczych z dziedziny bezpieczeństwa zintegrowanej komunikacji ruchomej. Ponadto prowadził on projekt wiążący techniczne i społeczne oczekiwania dotyczące zaufania. Propozycje projectów badawczych złożone pod jego kierownictwem, dotyczące nowych metod zarządzania ryzykiem (wartość ok. £1.000.000) zostały pozytywnie zaakceptowane.

Jako dyrektor techniczny Trusted Renewables (od 2012) habilitant zarządza i uczestniczy w projektach badawczych sponsorowanych na szczeblu krajowym. Habilitant zarządzał kilkoma projektami badawczymi o przeciętnej wielkości £50.000 dotyczącymi n.p. bezpiecznych płatności mobilnych dla osób starszych. Obecnie habilitant bierze udział w krajowym projekcie 'Internet of Things' jako ekspert w dziedzinie bezpieczeństwa i zaufania (wartość projektu ok. £1.000.000).

Wizyty naukowe

W latach 1990-1991 habilitant był zatrudniony na Uniwersytecie Oulu (Finlandia) jako 'Visting Professor'. Jego pobyt był wynikiem porozumienia ramowego pomiędzy Uniwersytetem Oulu i Politechniką Gdańską. W czasie pobytu habilitant uczestniczył w szeregu projektów badawczych związanych z integracją internetu oraz zbierał materiały do dalszych badań naukowych.

Konferencje, działalność edytorska i recenzje

Habilitant był członkiem Komitetów Programowych szeregu międzynarodowych konferencji dotyczących zaufania, bezpieczeństwa i prywatności, w tym IFIPTM (2008 i 2009), TrustID (2011) i PST (2012). Działalność ta jest związana z recenzowaniem prac nadesłanych na konferencje. Habilitant prowadził i współprowadził szereg międzynarodowych konferencji takich jak n.p. 'ETSI workshop on Smart Cities' (3-4 June 2013).

Obecnie habilitant jest stałym doradcą corocznej międzynarodowej konferencji "Smart Grid Smart Cities" którą również prowadził w latach 2010-2013.

Przez szereg lat habilitant był edytorem (Associate Editor) międzynarodowego czasopisma naukowego 'Electronic Commerce Research Journal' (publikowany przez Springer)

Habilitant działał również jako recenzent-ekspert dla EU oceniając wnioski badawcze w ramach puli FP7 (call 5 objective 1.4: Trustworthy ICT) a także jako recenzent indywidualnych projektów finansowanych z funduszy europejskich takich jak projekt SWEB (mobile government services).

Patenty i standardy

W związku z przemysłowym charakterem środowiska pracy habilitanta, zarówno patenty jak i udział w komitetach standaryzacyjnych stanowią istotny element dorobku naukowego, pomimo większego znaczenia przypisywanemu praktycznemu wykorzystaniu takich prac,

w szczególności w porównaniu z publikacjami naukowymi.

Habilitant jest autorem i współautorem szereg patentów. Patenty związane z prezentowanym tematem badawczym są omówione bardziej szczegółowo w tym wniosku. Wagę patentów opracowanych przez habilitanta podkreśla fakt iż dwukrotnie w swojej karierze był on uhonorowany nagrodami za działalność patentową: w roku 2000 (Inventor of the Year) i w roku 2008 (nominacja do Sir Alan Rudge Award for Future Innovation).

Habilitant był również szefem grupy roboczej, edytorem i współautorem szeregu międzynarodowych standardów takich jak WAP/OMA (EFI), JSR 177 czy OSGi/JSR232. Standardy te są nadal wykorzystywane w przemyśle.

Obecnie habilitant jest członkiem grupy roboczej SG-CG/SGIS pracującej nad nową wersją europejskiego standardu bezpieczeństwa systemów informatycznych dla nowoczesnych sieci energetycznych (EU mandate M/490), finansowanego głównie z projektu FINSENY (Future Internet for Smart Energy).

Przewody doktorskie

Habilitant był promotorem pomocniczym (zazwyczaj reprezentującym przemysł) w następujących przewodach doktorskich.

Michalis Pavlidis: A Meta-model for Trustworthiness of Information Systems. (2013). University of East London, UK

Natasha Dwyer: Traces of Digital Trust: An Interactive Design Perspective. (2011). Promotor: Dr Tom Clark i Dr Dave Randall Victoria University, Melbourne, Australia

Mohamed Jamal Al-Laban: Jednolite ujęcie parsingu dla gramatyk bezkontekstowych. (1990). Promotor: Prof. A. W. Mostowski. Politechnika Gdańska, Polska

Popularyzacja badań

Habilitant aktywnie propaguje naukę wykorzystujące nowe środki przekazu. Jest on jednym z edytorów Wikipedii (hasła 'zaufanie', 'zarządzanie zaufaniem' i zbliżone). Posiada on swoją stronę (http://cofta.eu) oraz blog (http://trusterm.com) gdzie popularyzuje on swoje badania nad zaufaniem a w szczególności metodologię TERM.

W przeszłości habilitant był jednym z członków-założycieli Polskiego Towarzystwa Informatycznego (Koło Gdańsk) gdzie koncentrował się on na popularyzacji edukacji informatycznej.

Habilitant jest aktywnym członkiem BCS/SCoE (British Computer Society Security Community of Experts). W ramach tej grupy popularyzuje on badania nad zaufaniem poprzez współudział w opracowaniach BCS na istotne tematy takie jak kształcenie informatyczne, prywatność, kopiowanie danych itp.

Od 22 lat habilitant jest członkiem IEEE (Institute of Electrical Engineers). W roku 2010 jego profesjonalny dorobek (w tym popularyzacja nauki) został wyróżniony promocją na stopień Senior Member.

Załącznik A. Publikacje

Poniższe publikacje dotyczą tylko monotematycznego zestawu osiągnięć badawczych. Przy każdej publikacji omówiono jej cel, osiągnięte wyniki oraz ich wykorzystanie. W pracach gdzie habilitant był współautorem opisano wkład własny habilitanta oraz udział procentowy.

Książki i monografie książkowe

[1] Cofta, P. (2013) The Foundations of a Trustworthy Web. Now Publishers.

Monografia opisująca szczegółowy model systemów informatycznych godnych zaufania oraz metod projektowania takich systemów na potrzeby internetu. Jedna z podstaw obecnej pracy naukowej habilitanta.

[2] Cofta, P. (2011) The Trustworthy and Trusted Web. Now Publishers.

Monografia wprowadzająca analityczną metodologię badań nad zaufaniem wiodącą do systematycznej analizy porównawczej zaufania i do pojęcia zaufania systemowego. Jedna z podstaw obecnej pracy naukowej habilitanta.

[3] Lacohee, H., Cofta, P., Phippen, A., Furnell, S. (2008) Understanding Public Perceptions: Trust and Engagement in ICT-Mediated Services. International Engineering Consortium.

Wysoko ceniona pozycja obejmująca praktyczne studia nad stosunkami pomiędzy społeczeństwem a technologią informatyczną.

[4] Cofta, P. (2007) Trust, Complexity and Control: Confidence in a Convergent World. John Wiley & Sons.

Monografia wprowadzająca formalny model podejmowania decyzji oparty na dualiźmie zaufania i kontroli, wraz z prezentacją zastosowań modelu związanych ze współczesną technologią informatyczną.

Rozdziały w książkach

[5] Cofta, P., Lacohee, H. (2014) Trusted and trustworthy information technology. In: Khosorow-Pour, M. (Eds.). Encyclopedia of Information Science and Technology, Third Edition. IGI Global. (zaakceptowana)

Systematyczny przegląd różnorodnych podejśc do definiowania zaufania i bycia godnym zaufania w odniesieniu do systemów informatycznych.

[6] Cofta, P., Lacohee, H., Hodgson, P. (2011) Incorporating Social Trust into Design Practices for Secure Systems. In: Mouratidis, H. (Ed.) Software Engineering for Secure Systems: Industrial and Research Perspectives. IGI Global.

Analiza praktyk związanych z bezpieczeństwem systemów informatycznych oraz propozycja włączenia w nie analizy zaufania.

[7] Cofta, P., Lacohee, H. (2010) Trust in identification systems: from empirical observations to design guidelines. In: 'Trust Modelling and management in Digital Environments: From Social Concepts to System Development' by Zheng Yan (Ed.) Information Science Publishing.

Prezentacja systematyczej metody, bazującej na teorii opracowanej przez habilitanta, która pozwala na budowanie wymagań projektowych na podstawie empirycznych obserwacji dotyczących struktur zaufania, z zastosowaniem do systemów zarządzania tożsamością.

[8] Cofta, P. (2009) Designing for Trust. In: Handbook of Research on Socio-Technical Design and Social Networking Systems' by Brian Whitworth and Aldo de Moor (Eds). Information Science Reference,

Rozdział formalizujący strukturalną analizę zaufania i bycia godnym zaufania ('architektury zaufania'), ilustrowany przykładami analizy systemów zarządzania tożsamością.

Publikacje recenzowane (czasopisma i konferencje)

[9] Ward, D., Kourti, N., Lazari, A., Cofta, P. (2014) Trust Building and the ERNCIP community. Int. J. of Critical Infrastructure Protection. (accepted)

Zastosowanie elementów TERM do narzędzi i procesów stosowanych do ochrony krytycznej infrastruktury w Europie.

[10] Cofta, P., Lacohee, H. (2014) Interdisciplinary game-theoretic approach to trust modelling. Int. J. of Applied Industrial Engineering. (zaakceptowana)

Formalizacja dwóch typów relacji bazujących na zaufaniu z użyciem teorii gier.

[11] Dwyer, N., Clark, T., Cofta, P., Randall, D. (2011) Reading Trust and Distrust in Shared Documents: Film Professionals Review Film Reviews. In: Proc. of TP-DIS 2011: Trust and Privacy in Distributed Information Sharing; co-located with: IFIPTM 2011 at the Technical University of Denmark (DTU), Copenhagen, Denmark. Also in: Journal of Internet Services and Information Security (JISIS) vol. 1 no. 4 Nov 2011 pp.110-119

Etnograficzna analiza haurystyk używanych do oceny zaufania w oparciu o szczegółowo zdokumentowane wypowiedzi.

[12] Mouratidis, H., Cofta, P. (2010) Practitioner's challenges in designing trust into online systems. In: Journal of Theoretical and Applied Electronic Commerce Research vol. 5 no.3.

Analiza zaufania do systemów informatycznych z punku widzienia interakcji pomiędzy trzema grupami społecznymi: użytkownikami, operatorami i projektantami w celu zdefiniowania 'design for trust' jako praktycznego obszaru badań interdyscyplinarnych.

[13] Dwyer, N., Clark, T., Randall, D., Cofta, P. (2010) Where everyone knows your name: Trust in a localised media environment. In: Proc. of 4th IFIP WG 11.11 International Conference on Trust Management IFIPTM 2010, June 14-18, 2010, Morioka, Iwate,

Japan

Etnograficzna analiza możliwości oceny zaufania w zamkniętych grupach społecznych posługujących się technologią.

[14] Cofta, P., Hodgson, P. (2009) 'Designing for Trust' for the Future Web. In: Proc. of WebSci'09 Society On-Line, Athens, Greece, 18th–20th March, 2009.

Krótka publikacja (prezentowana jako plakat) wprowadzająca koncepcję projektowana dla zaufania (ang. 'design for trust') i jego zastosowania dla projektowania internetu.

[15] Hodgson, P., Cofta, P. (2009) Towards a methodology for research on trust. In: Proc. of WebSci'09 Society On-Line, Athens, Greece, 18th–20th March, 2009.

Krótka publikacja (prezentowana jako plakat) która dyskutuje pozycję interdyscyplinarnych badań nad zaufaniem i technologią w kontekście współczesnych trendów w naukach społecznych.

[16] Cofta, P. (2009) Towards a better citizen identification system. FIDIS Journal. Identity in the Information Society. Volume 1, Number 1, 39-53. Springer.

Analiza akceptacji technologii w wyniku zaufania z zastosowaniem do systemów zarządzania tożsamością, przedstawiająca metody zwiększenia tego zaufania.

[17] Hodgson, P., Cofta, P. (2008) Society As An Information Network. Proc. of Fourth International Conference on Technology, Knowledge & Society, 18-20 January 2008, Boston, USA. Also International Journal of Technology, Knowledge and Society, Volume 4, Issue 1, pp.1-10.

Wczesny zunifikowany model społeczeństwa i systemów informatycznych zbudowany na teorii autonomicznych agentów dążących do zmniejszenia złożoności komunikacji.

[18] Dwyer, N., Cofta, P. (2008) Understanding the grounds to trust: game as a cultural probe. Proc. of Web 2.0 Trust workshop at the Joint iTrust and PST Conferences on Privacy, Trust Management and Security, June 18-20, 2008, Trondheim, Norway (IFIPTM 2008)

Etnograficzna analiza heurystyk używanych do oceny zaufania w kontekście gier testujących zaufanie.

[19] Cofta, P. (2008) The Googleplex. Proc. of International Conference on Electronic Commerce (ICEC'08) August 19-22, 2008 Innsbruck, Austria.

Szczegółowa analiza zaufania do Google używająca modelu bazującego na dualiźmie zaufania i kontroli, wraz z przewidywaniami dotyczącymi rozwoju tego zaufania.

[20] Cofta, P. (2008) Confidence-compensating privacy protection. Proc. of PST 2008 Sixth Annual Conference on Privacy, Security and Trust, October 1-3, 2008, Fredericton, New Brunswick, Canada.

Analiza zaufania jako metody uzupełaniającej braki w prywatności wraz z propozycją metod ochrony prywatności rekompensującej braki w zaufaniu.

[21] Cofta, P. (2007) Confidence, trust and identity. BT Techology Journal. Vol 25 No 2, April 2007.

Analiza związków pomiędzy zaufaniem, tożsamością i identyfikacją w kontekście systemów zarządzania tożsamością; publikacja wprowadza koncepcję bazującego na zaufaniu poświadzenia tożsamości chroniącego prywatność.

[22] Cofta, P. (2006) Comparative analysis of the complexity-based model of trust. Proc. of AAMAS 06 Fifth International Joint Conference on Autonomous Agents and Multiagent Systems. Hakodate, Japan, 8-12 May 2006.

Analiza porównawcza modelu bazującego na dualiźmie zaufania i kontroli oraz znanych modeli zaufania. Wykazano iż nowy model jest uogólnieniem znanych modeli.

[23] Cofta, P. (2006) Convergence and trust in eCommerce. BT Technology Journal vol 24, no 2, April, 2006.

Analiza wpływu zintegrowanych technologii informatycznych na zaufanie w handlu elektronicznym. Analiza ta zastosowała model bazujący na dualiźmie zaufania i kontroli oraz zaproponowała eliminację niektórych z istniejących braków.

[24] Cofta, P. (2006) Distrust. Proc. of ICEC 2006 The Eighth International Conference on Electronic Commerce, August 14-16, 2006, Fredericton, New Brunswick, Canada.

Systematyczna eksporacja pojęcia nieufności poszerzająca model zazwyczaj stosowany do oceny bycia godnym zaufania bazujący na dualiźmie zaufania i kontroli.

[25] Cofta, P. (2006) Confidence creation framework of eBay. Proc. of Networking and Electronic Commerce Research Conference (NAEC 2006), October 19-22, 2006, Riva Del Garda, Italy.

Zastosowanie modelu bazującego na dualiźmie zaufania i kontroli do analizy mechanizmów budowy zaufania stosowanych przez eBay wraz ze wskazaniem możliwości poprawy tego zaufania.

[26] Cofta, P. (2005) Impact of convergence on trust in e-commerce. Proc. of Networking and Electronic Commerce Research Conference (NAEC 2005), October 6-9, 2005, Riva Del Garda, Italy.

Wczesne podejście do sformułowania zunifikowanego modelu zaufania w oparciu o istniejące modele który mógłby być stosowany do analizy wpływu technologii na zaufanie w handlu elektronicznym.

[27] Yan, Z., Cofta, P. (2005) A Mechanism for Trust Sustainability among Trusted Computing Platforms. in: Sokratis K. Katsikas, Javier Lopez, Günther Pernul (Eds.): Trust, Privacy and Security in Digital Business: Second International Conference, TrustBus 2005, Copenhagen, Denmark, August 22-26, 2005, Proceedings. Lecture Notes in Computer Science 3592 Springer 2005

Publikacja zawierająca teoretyczne podstawy patentu [37]. Opisuje ona system w którym systemy techniczne wyposażone w bezpieczne moduły mogą wymieniać informacje w celu

wsparcia wzajemnego zaufania.

[28] Cofta, P. (2004) Computing Recommendations to Trust. TrustBus 2005. Proc. of Second International Conference, iTrust 2004, Oxford, UK, March 29 - April 1, 2004.

Przegląd modeli oceny zaufania (a także modeli systemów informatyczncyh godnych zaufania) które mogłyby być stosowane w urządzeniu omówionym w [29].

[29] Cofta, P., Crane, S. (2003) Towards the Intimate Trust Advisor. In: Paddy Nixon, Sotirios Terzis (Eds.): Trust Management, First International Conference, iTrust 2003, Heraklion, Crete, Greece, May 28-30, 2002, Proceedings. Lecture Notes in Computer Science 2692 Springer 2003.

Koncepcja urządzenia technicznego które mogłoby automatycznie informować swojego użytkownika w temacie zaufania do otaczającego je środowiska informatycznego.

[30] Yan, Z., Cofta, P. (2003) Methodology to Bridge Different Domains of Trust in Mobile Communications. In: Paddy Nixon, Sotirios Terzis (Eds.): Trust Management, First International Conference, iTrust 2003, Heraklion, Crete, Greece, May 28-30, 2002, Proceedings. Lecture Notes in Computer Science 2692 Springer 2003.

Zastosowanie socjo-technicznego zaufania jako metody pozwalającej na zbudowanie zaufania pomiędzy domenami używającymi niezgodnych definicji zaufania.

Przyznane patenty

[31] Cofta, P., Mallet, C. (2010) Method and Apparatus for secure Energy Delivery. Przyznany w Wielkiej Brytanii as GB 2479324, w trakcie badań w EU, USA, Japonii i Australii

Zintegrowanie modułu elektronicznego godnego zaufania z panelem słonecznym w celu zwiększenia zaufania do jakości pomiaru energii elektrycznej a także w celu zwiększenia bezpieczeństwa.

[32] Piotr Cofta: Method and System for Recursive Authentication in a Mobile Network. (2006) Przyznany w USA jako 8,165,565; w EU jako EP 1 982 547

[33] Piotr Cofta: SIM Based Authentication. Przyznany w EU, w USA jako 8,417,218, w Chinach jako CN101406021.

[34] Piotr Cofta: Methods, Appartuses and Software for Authentication of Devices Temporarily Provided With a SIM to Store a Challege-Response. Przyznany w USA jako US 8,190,127; w Chinach jako CN101406020. W trakcie badań w EU.

Seria trzech patentów opisujących metody budowy technicznego zaufania pomiędzy fizycznie oddzielnymi urządzeniami poprzez wykorzystanie zaufania społecznego oraz karty SIM jako elementu godnego zaufania.

[35] Piotr Cofta, Olli Immonen: Trusted Signature with Key Access Permission. (2004) Przyznany w USA jako US 7,853,793

[36] Lauri Paatero, Cofta Piotr Key Storage Administration. (2006) Przyznany w Korei jako KR 100823631.

Metoda logicznego podziału elementu godnego zaufania (takiego jak n.p karta SIM) aby mógł być on wykorzystywany w domenach mających różne podejście do zaufania bez jego utraty.

[37] Zheng Yan, Piotr Cofta: System and Method to Establish and Maintain Conditional Trust by Stating Signal of Distrust. Przyznany w USA jako 7,634,807

Metoda pozwalająca systemom na utrzymanie i modyfikację poziomu wzajemnego zaufania przy pomocy zaproponowanego protokołu.

[38] Piotr Cofta: Communications Device Monitoring. (2007) Przyznany w USA jako 8,126,507 oraz w EU jako EP EP 1997 052.

Zastosowanie karty SIM (albo alternatywnego elementu godnego zaufania) do oceny i raportowania poziomu zaufania względem urządzenia mobilnego.

[39] Piotr Cofta, Lauri Paatero: Method and System for Visualising a Level of Trust of Network Communication Operations and Connections of Servers. (2003) Przyznany w Korei jako KR100655400. W trakcie badań w EU

Patent wprowadzający nowe metody komunikowania użytkownikowi poziomu technicznego zaufania obliczonego przez urządzenie mobilne.

[40] Piotr Cofta, Olli Immonen, Mikael Linden, Mikko Lukkaroinen: Method for Binding a Program Module. (1999) Przynany w USA jako US 7,263,618

Metoda wywoływania modułów programowych w której poszczególny moduł może wybrać moduły współpracujące z nim na podstawie swojego zaufania do nich.

[41] Linden, M., Immonen, O., Lukkarionen, M., Cofta, P. Network Element and Method for Controlling Access to Low Level Computer System Services. Przyznany w USA jako 7,315,942; w Finlandii jako FI 106 495

Metoda zapewnienia oprogramowania godnego zaufania poprzez zastosowanie podpisu cyfrowego.

Zaproszone prezentacje konferencyjne

[42] Cofta, P., Mallett, C. (2013) Trust-Enhanced Risk Management (TERM) for Smart Systems. Presented at “Telecoms for Smart Grids” annual conference, London, UK.

Dyskusja na temat niedoskonałości typowej analizy ryzyka w zastosowaniach do systemów cyber-technicznych, ukazująca zalety TERM.

[43] Cofta, P. (2013) TERM: Trust-Enhanced Risk Management. Tutorial on “Day-Con2013” Security Conference, Dayton, OH, USA.

[44] Cofta, P. (2014, 2013) TERM: Trust-Enhanced Risk Management. Workshop on “Troopers13” and "Troopers14" Security Conferences, Heidelberg, Germany.

[45] Cofta, P. (2012) Trust: the Unloved Sibling. Keynote presentation on Day-Con2012 Security Conference, Dayton, OH, USA.

[46] Cofta, P. (2012) Security Professionals: Plumbers of Trust. Keynote presentation on Troopers12 Security Conference, Heidelberg, Germany.

Cztery komunikaty w formie prezentacji (w tym jedna prezentowana na sesji całkowicie poświęconej TERM) prezentujące bieżący stan prac nad TERM. Prezentacje te służą weryfikacji metodologii TERM.

[47] Cofta, P. (2011) Resilient against unexpected: are you? Invited presentation on the Smart Grid Smart Cities 2011 Conference, Lisbon, Portugal.

Zarządzanie zaufaniem jako podstawa zabezpieczenia przed skutkami katastrof w systemach cyber-technicznych. Prezentacja skupia się na zaletach analizy zaufania (w tym TERM) i modeli budowy zaufania, kontrastując je z analizą ryzyka.

[48] Cofta, P. (2011) Creation of trust in inter-organisational cooperation. Invited presentation at the ERN-CIP Trust Conference, JRC, Ispra, Italy.

Prezentacja analizująca metody budowy zaufania dla potrzeb międzynarodowej kooperacji pomiędzy operatorami krytycznej infrastruktury w Europie. Wprowadza one model budowy i utrzymania zaufania zastosowane następnie w TERM.

[49] Cofta, P. (2010) If you make it, they may not come: social barriers to an adoption of Smart Grid. Invited presentiation at Smart Grid Smart Cities Smart Future Conference, Amsterdam, The Netherlands.

Analiza akceptacji technologii w oparciu o zaufanie w zastosowaniu do inteligentnych sieci energetycznych. Prezentacja stosuje model operator-użytkownicy wprowadzony później formalnie w [2].

[50] Cofta, P. (2008) Identity and trust: Enabling layers of the future communication landscape. Emerging Communications Conference (eComm2008), Mountain View, California, USA, March 12-14, 2008.

Propozycja utworzenia wyspecjalizowanych warstw komunikacyjnych odpowiedzialnych za zarządzanie tożsamością i zaufaniem w zastosowaniu do przyszłej architektury internetu. Propozycja ta miała wpływ na [1] i [2].

[51] Cofta, P. (2007) From trust to revenue. Telco 2.0, 2nd Industry Brainstorm, 27-29 March 2007, London, UK.

Analiza ekonomicznych zalet zaufania w zastosowaniu do nowych możliwości rynkowych operatorów mobilnych. Użyta w późniejszych pracach nad ekonomicznymi podstawami zarządzania zaufaniem.

[52] Cofta, P. (2007) Surveillance as a crisis of trust. Westminster eForum, London, UK.

Publikacja analizująca związki pomiędzy inwigilacją elektroniczną i zaufaniem, definiująca poziom inwigilacji który nie narusza zaufania. Jest to jedna z publikacji eksplorujących

zależności pomiędzy zaufaniem a jego przeciwieństwami.

[53] Cofta, P. (2007) Trust and control: makers and breakers of e-services. Networking and Electronic Commerce Research Conference (NAEC 2007), November, 2005, Riva Del Garda, Italy.

Zastosowanie modelu bazującego na dualiźmie zaufania i kontroli do analizy do handlu elektronicznego, demonstrująca potencjał analityczny modelu.

[54] Cofta, P. (2006) Trust in a virtual world. Joint EU SecurIST, Mobile & Wireless Workshop, Brussels, Belgium.

Analiza wpływu technologii wirtualizacji na zaufanie wskazująca potencjalne kierunki badań.

[55] Cofta, P., Lacohee, H. (2006) Trust or there and back again: a cautionary tale of an interdisciplinary cooperation. First Research Meeting of Centre for Systems and Services Sciences (CS3), Grenoble, France.

Krótka auto-etnograficzna prezentacja demonstrująca konieczność zaufania w pracach badawczych, na przykładzie interdyscyplinarnych badań nad zaufaniem.

[56] Cofta, P. (2004) Trusting Totalitarian Technologies. VIPER 2004, Basel, Switzerland

Krótka prezentacja dotycząca zaufania do systemów cyber-technicznych i ich negatywnego wpływu na zachowanie prywatności. Sugeruje ona rozwiązanie tego problemy poprzez budowę technologii godnych zaufania.

[57] Chen, Z., Cofta, P., Immonen, O. (2003) Security and Trust Services API for J2ME Technology. JavaPolis 2003. December 03-04. Brussels, Belgium.

Prezentacja standardu JSR177 który miał an celu poprawę zaufania i bezpieczeństwa urządzeń mobilnych. Standard ten jest nadal stosowany w szeregu urządzeń mobilnych.

Raporty

[58] Cofta, P. (2013) Building Trust in Information Security. Whitepaper. The Alliance of Trustworthy Business Experts.

Raport dyskutujący zaufanie do bezpieczeństwa systemów informatycznych w chwili obecnej i postulujący kroki wiodące do poprawy tego zaufania. Jedno z praktycznych zastosowań modelu.

[59] Cofta, P. (2009) Trust assurance: a foundation of identity management. Position paper. Oxford Internet Institute workshop on "A Policy and Legal Framework for Identity Management".

Raport opisujący zasady zarządzania zaufaniem na potrzeby systemów zarządzania tożsamością, ukazujący zastosowalność modelu do analizy konkretnej sytuacji.

[60] Cofta, P. (2004) Challenges in trust. Whitepaper. Media Lab Europe.

[61] Cofta, P. (2004) Trusting Technologies. Position paper. Media Lab Europe.

[62] Cofta, P. (2004) The Phenomenon of a Borderline Trust. Position paper. Media Lab Europe.

Seria trzech raportów pozycjonujących i strukturalizujących badania nad zaufaniem pomiędzy społeczeństwem i technologią, wykorzystane jako podstawa tworzenia nowej grupy badawczej. Zawierają one szereg założeń dotyczących modelowania zaufania.

Standardy

[63] JSR232: Mobile Operational Management. (2004) (członek zespołu)

Standard definiuje użycie standardu OSGi w mobilnym środowisku Java J2ME.

[64] JSR177: Security and Trust Services API for J2ME (2003) (współautor)

Standard definiujący sposób użycia zaufanych aplikacji rezydujących na karcie SIM przez aplikacje pracujące w mobilnym środowisku Java J2ME.

[65] WAP (Wireless Application Protocol) Forum Specification WAP-231-EFI-20011217-a: External Functional Interfaces (2001) (współedytor)

Standard umożliwiający aplikacjom internetu mobilnego (WAP) na dostęp do różnorodnych elementów urządzenia mobilnego, w tym karty SIM.

[66] MeT (Mobile Electronic Transactions) Forum Technical Architecture Specification. (2001) (główny autor i edytor).

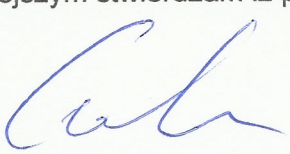
Standard prezentujący architektury techniczne służące budowie zaufania z zastosowaniem do handlu elektronicznego, w szczególności do płatności mobilnych.

Dodatek B. Informacja o wkładzie własnym

Publikacja (odnośnik do listy publikacji)	Opis wkładu własnego habilitanta (jeżeli nie jest on jedynym autorem)	Procentowy wkład habilitanta
[1]		100%
[2]		100%
[3]	Rozdział 1 (metodologia), 2 (analiza problemu) i 9 (rekomendacje). Udział w pozostałych rozdziałach.	30%
[4]		100%
[5]	Metoda analizy, struktura tekstu i większość definicji: 80%.	80%
[6]	Idea zarządzania zaufaniem oraz użyta metoda analizy strukturalnej.	60%
[7]	Założenia teoretyczne, metoda analizy oraz zalecenia projektowe	70%
[8]		100%
[9]	Ramowa koncepcja zastosowania TERM	20%
[10]	Koncepcja dynamiki relacji oraz większość prezentowanego modelu formalnego	80%
[11]	Metoda analizy, część dyskusji oraz ostateczna edycja	35%
[12]	Koncepcja, dyskusja nad tematem oraz definicje	50%
[13]	Metoda analizy oraz ostateczna edycja	35%
[14]	Koncepcja 'design for trust', przegląd i dyskusja	70%
[15]	Oryginalna dyskusja oraz udział w edycji tekstu	30%
[16]		100%
[17]	Oryginalny model oraz jego dyskusja 50%.	50%
[18]	Metoda analizy oraz ostateczna edycja: 35%.	35%
[19]		100%
[20]		100%
[21]		100%
[22]		100%
[23]		100%
[24]		100%
[25]		100%
[26]		100%
[27]	Dyskusja oraz protokół	50%
[28]		100%
[29]	Koncepcja urządzenia oraz część dyskusji	50%
[30]	Założenia oraz dyskusja	50%
[31]	Współautor, równy udział	50%
[32]		100%
[33]		100%
[34]		100%
[35]	Współautor, równy udział	50%
[36]	Współautor, równy udział	50%
[37]	Współautor, równy udział	50%
[38]		100%
[39]	Współautor, równy udział	50%

[40]	Współautor, równy udział	25%
[41]	Współautor, równy udział	25%
[42]	Metodologia TERM, przykłady i dyskusja	80%
[43]		100%
[44]		100%
[45]		100%
[46]		100%
[47]		100%
[48]		100%
[49]		100%
[50]		100%
[51]		100%
[52]		100%
[53]		100%
[54]		100%
[55]	Analityczne podejście oraz część danych	75%
[56]		100%
[57]	Struktura i architektura zaufania	30%
[58]		100%
[59]		100%
[60]		100%
[61]		100%
[62]		100%
[63]	Analiza struktury zaufania oraz wnioski które wpłynęły na analizę bezpieczeństwa systemów informatycznych korzystających z tego standardu.	10%
[64]	Analiza zaufania która zdefiniowała strukturę rozwiązania; niektóre z sekcji standardu.	20%
[65]	Koncepcja współpracy, proponowana architektura a także niektóre z sekcji standardu.	20%
[66]	Struktura standardu, architektura techniczna oraz niektóre sekcje.	50%

Niniejszym stwierdzam iż powyższa tabela jest zgodna ze stanem faktycznym



Piotr Cofta

Dodatek C. Informacja bibliometryczna

Google Scholar		all	since 2009
	citations	275	207
	h-index	9	8
	i10-index	9	8
Web of Science	h-index	2	

Publikacja (odnośnik do listy publikacji)	Cytowania (Google Scholar)	Punkty w klasyfikacji (MNiSW)
[1]		25
[2]	4	25
[3]	7	25
[4]	38	25
[5]		5
[6]	2	5
[7]		5
[8]	5	5
[9]		25
[11]	1	
[12]	3	
[16]	6	
[17]	4	
[19]	3	
[20]	1	10
[21]	19	
[23]	13	
[24]	18	10
[25]	5	
[27]	21	10
[28]	1	10
[29]	9	10
[30]	16	10
[35]	1	
[37]	34	
[39]	4	
[40]	4	
[41]	4	
[55]	2	
[62]	2	

Razem	**205**