STUDIA INFORMATICA 2013
Volume 34 Number 3 (113)

Henryk KRAWCZYK
Politechnika Gdańska, Wydział Elektroniki, Telekomunikacji i Informatyki
Paweł LUBOMSKI
Politechnika Gdańska, Centrum Usług Informatycznych

CoRBAC – KONTEKSTOWO ZORIENTOWANY MODEL BEZPIECZEŃSTWA

Streszczenie. Zaproponowano uogólniony model kontroli dostępu do usługowych systemów internetowych, uwzględniający różne kategorie kontekstu. Określono wpływ kontekstu na model, a także na architekturę systemu bezpieczeństwa. Podano przykład implementacji modelu i architektury bezpieczeństwa dla zestawu usług dotyczących e-uczelni i wstępnie oszacowano zalety takiego rozwiązania.

Słowa kluczowe: bezpieczeństwo, kontekst, model RBAC, kontrola dostępu, usługi

CoRBAC – CONTEXT-ORIENTED ROLE BASED ACCESS CONTROL

Summary. A generalized model of the access control to web-based service-oriented e-university system is proposed. Different kind of context and its impact on the security model and architecture is defined. In consequence the implementation of such an architecture is presented for e-university system based on specialized services. The benefits of such a solution have been pre-estimated.

Keywords: security, context, RBAC model, access control, services

1. Wprowadzenie

Kontrola dostępu użytkowników jest istotną funkcją systemów informatycznych. Oprócz klasycznych rozwiązań typu RBAC [4] stosuje się nowe podejście, polegające na uwzględnianiu kontekstu związanego z realizowanymi funkcjami systemu. Xu Feng i in. zaproponowali formalny model context-aware service-oriented role based access control (CSRBAC)

[13]. Wiąże on użytkowników, role, uprawnienia, sesje, konteksty oraz usługi operując w sferze web serwisów. Definiuje również procedurę aktywacji roli, która wyznacza, czy dana rola/uprawnienie może zostać przyznane użytkownikowi. Modyfikacją tej pracy jest model CGRBAC (RBAC model for global services and context) [14]. Przewiduje on mapowanie ról specyficznych dla poszczególnych dostawców usług na tzw. globalne role – uniwersalne pomiędzy dostawcami usług. R. Bhatti, E. Bertino i A. Ghafoor zaproponowali model XML-based Generalized Temporal Role Based Access Control (X-GTRBAC) [15]. Definiuje on format zapisu warunków z wykorzystaniem notacji XML oraz algorytm decydujący na podstawie kontekstu o przyznaniu dostępu. J. W. Woo i in. w [16] proponują rozszerzenie modelu RBAC o dynamiczne przydzielanie ról na podstawie zaufania pomiędzy usługami (w komunikacji usługa – usługa). Zaufanie to jest wyznaczane na podstawie reputacji usługi oraz satysfakcji z wcześniejszych wywołań.

Opisane rozwiązania nie wskazują jednak mechanizmów pozyskania kontekstu (metod analizy bieżącego kontekstu). Jedynie praca [17] sygnalizuje, że jest to trudne i skomplikowane. Określają one kontekst w sposób opisowy. Procedury dostępu natomiast są „punktowe" – nie wiążą ze sobą poszczególnych wywołań usługi i nie analizują relacji pomiędzy nimi (w powiązaniu z kontekstem). Dodatkowo, rozwiązania te pozostają w sferze koncepcji, bez implementacji.

W artykule wzięto pod uwagę systemy internetowe, realizujące swoje funkcje poprzez dostępne w ich środowisku usługi informacyjne. Dla tej klasy systemów podano ogólny model bezpieczeństwa, a także architekturę, implementującą taki model. Istotną sprawą w przedstawionych rozwiązaniach jest również fakt implementacji i wdrożenia tego modelu w praktyce na przykładzie systemu e-uczelni.

Taki system został zaimplementowany i wdrożony na Politechnice Gdańskiej w postaci platformy IP^2. Jest to rozproszony system internetowy o architekturze usługowej. Pozwala ona na uruchamianie na niej wielu aplikacji wspierających działalność zarówno dydaktyczną, jak i naukową uczelni. Główny dostęp użytkownika odbywa się poprzez portal Moja PG [1], ale możliwe jest korzystanie z platformy za pomocą jednego z wielu zintegrowanych systemów. Całość wykonana jest w technologiach otwartego oprogramowania (ang. *open source*), w tym głównie Java Enterprise Edition [2]. Jak każdy system internetowy charakteryzuje się cienkim klientem zlokalizowanym w przeglądarce WWW użytkownika (z dosyć intensywnie wykorzystywaną technologią AJAX i JavaScript). Aktualnie system ma prawie 30 000 aktywnych użytkowników, a przetwarza dane dotyczące przeszło 80 000 osób. W związku z tym, zapewnienie odpowiedniego bezpieczeństwa jest sprawą niezwykle ważną, ale również bardzo trudną. Poniżej zaproponowano nową koncepcję, którą wykorzystano praktycznie podczas budowy e-uczelni na Politechnice Gdańskiej.

2. Model bezpieczeństwa zorientowany kontekstowo

Wraz z postępującą informatyzacją społeczeństwa i proporcjonalnie rosnącym zagrożeniem dla bezpieczeństwa systemów standardowe modele kontroli uprawnień powinny ewaluować do wersji bardziej dynamicznych, dzięki czemu użytkownik, poza krótkim przedziałem czasu, nie ma pełnego kompletu uprawnień, szczególnie tych najbardziej krytycznych [5]. Niezwykle istotny jest tu aspekt bezpiecznego uwierzytelniania cyfrowych tożsamości, na podstawie których użytkownicy wykonują akcje w systemach [6]. Dalszym rozwinięciem jest kontekstowa kontrola dostępu do zasobów i operacji na nich, która wiąże poziom uprawnień z bieżącą sytuacją w środowisku pracy użytkowników [7], [8].

Przyjmijmy, że kontekst jest to zbiór wyszczególnionych warunków w systemie, które tworzą tło działań użytkownika. W aspekcie bezpieczeństwa systemu, kontekst działań użytkownika można podzielić na kilka typów. W pierwszej kolejności jest to moment czasu wykonania operacji przez użytkownika. Następnie istotna jest lokalizacja fizyczna i/lub logiczna użytkownika [9]. Kolejnym aspektem jest deklarowany przez użytkownika cel jego działań. Wiąże się to przeważnie z nadaniem dodatkowych uprawnień w sytuacjach wyjątkowych. Bardzo często wpływ mają wcześniejsze operacje wykonane w systemie, w ramach pewnego scenariusza działań i sesji użytkownika. To właśnie scenariusze (mniej lub bardziej złożone) określają zbiór dopuszczalnych operacji użytkownika. Logowanie operacji użytkownika pozwala dodatkowo zbudować profil jego działań, na podstawie którego możliwe jest wychwytywanie i blokowanie sytuacji wyjątkowych, np. użytkownik, który zawsze loguje się do systemu z Polski chce nagle zalogować się z Chin.

Ostatnim typem kontekstu, który wykorzystywany jest często w dużych systemach o charakterze ewidencyjnym, jest powiązanie użytkownika z obiektami i operacjami, jakie może na nich wykonać. Są to relacje:

- użytkownik – operacje,
- użytkownik – obiekty,
- obiekty – operacje.

Określają one dopuszczalny zakres działań użytkownika na określonym zbiorze obiektów. W wyniku tego działania użytkownik nie ma pełni uprawnień do wszystkich obiektów w systemie – są one dynamicznie zawężane i przydzielane do określonych podzbiorów.

Wszystkie te typy kontekstu osadzone są w bieżącym stanie systemu i są ściśle ze sobą powiązane, co powoduje, że interferują na siebie wzajemnie [7]. Bieżący stan systemu określa również aktualny, globalny tryb pracy: normalny lub sytuacji wyjątkowej (np. prace serwisowe). W ten sposób możliwe jest przełączanie pomiędzy kilkoma politykami bezpieczeństwa, które przekładają się na reguły dostępu do usług.

Uwzględnienie tych różnych parametrów powiązanych z wykonywaną operacją pomaga zwiększyć wykrywalność i odfiltrować próby ataku na system, co w efekcie podnosi poziom bezpieczeństwa tego systemu. Przekłada się to na wzrost zaufania do systemu, oczywiście przy jednoczesnym założeniu, że nie ogranicza się w ten sposób jego użyteczności.

W tabeli 1 przedstawiono zestawienie możliwych rodzajów kontekstu dla różnego typu elementów. Mamy więc miejsce i czas pracy użytkownika oraz jego uprawnienia. Posiadamy ograniczone czasowo role i uprawnienia, które dodatkowo podlegają zmianom. Mamy w końcu scenariusze działań oraz sytuacje lub stany wyjątkowe.

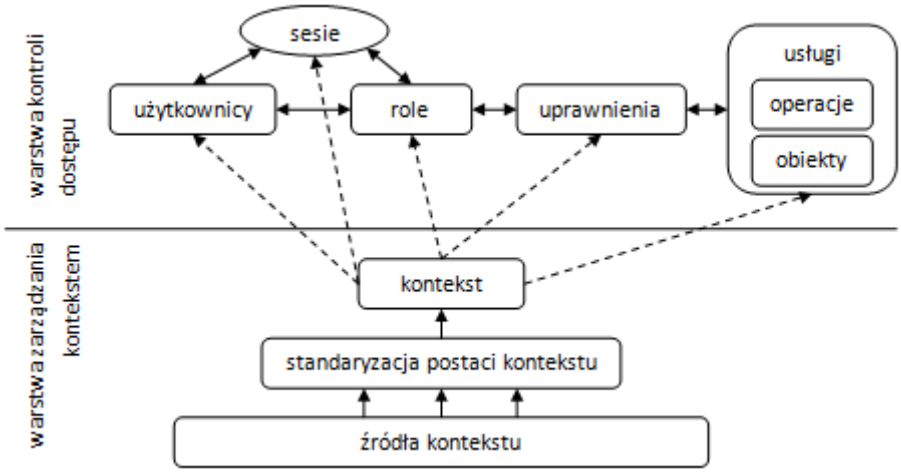
Tabela 1

Rodzaje kontekstu dla różnych typów elementów

Element	**Kontekst**
użytkownik	miejsce, czas, uprawnienia
rola użytkownika	okres roli, zmiana roli
uprawnienia użytkownika	zmiana uprawnień, wyjątki
operacje (wywołania usług)	sesja użytkownika, typowe scenariusze działań – odchyłki, wyjątki, ważność scenariuszy

W [4] przedstawiono formalny opis tradycyjnego modelu Role Based Access Control (RBAC). Context-oriented Role Based Access Control (CoRBAC) jest jego rozszerzeniem o kontekst działań użytkownika. Analogicznie do tradycyjnego modelu RBAC, opiera się on na przyporządkowaniach:

- UŻYTKOWNICY × ROLE × KONTEKST
- UPRAWNIENIA × ROLE × KONTEKST
- UPRAWNIENIA × OPERACJE × KONTEKST

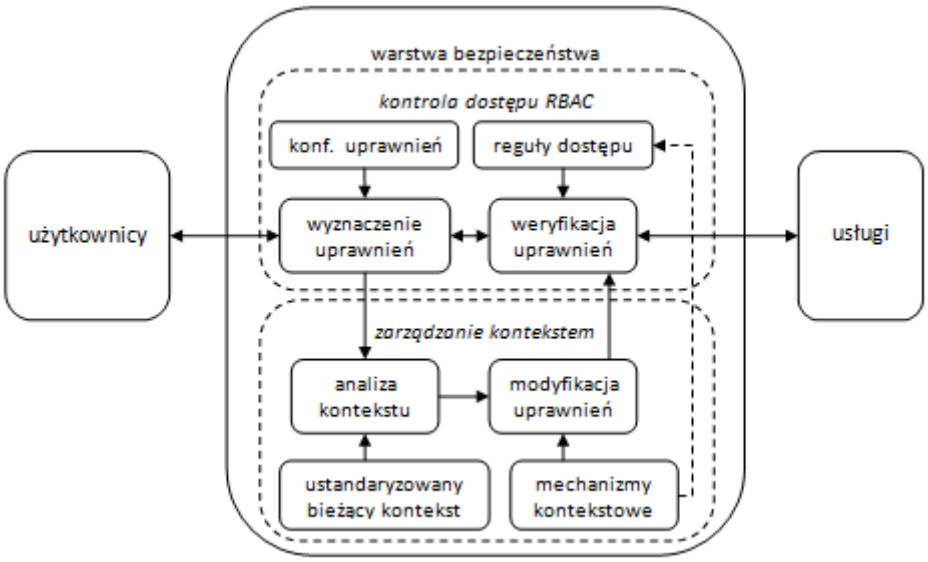


Rys. 1. Zorientowany kontekstowo model bezpieczeństwa (CoRBAC)
Fig. 1. The context-oriented security model (CoRBAC)

Koncepcję modelu schematycznie przedstawiono na rys. 1. Opierając się na pracy D. Kulkarni i A. Tripathi [18] linią przerywaną wskazano również możliwe miejsca uwzględniania kontekstu.

3. Architektura bezpieczeństwa w modelu CoRBAC

Na podstawie modelu CoRBAC zaprojektowano warstwę bezpieczeństwa, realizującą kontrolę dostępu w systemie usługowym. Tak jak w tradycyjnym modelu RBAC [4], w środowisku usługowym kontrola uprawnień odbywa się na poziomie dostępu do usługi. W celu podkreślenia różnicy pomiędzy klasycznym podejściem w modelu RBAC oraz proponowanym CoRBAC w warstwie bezpieczeństwa wyróżniamy dodatkowy komponent zarządzania kontekstem, zaprezentowany schematycznie na rys. 2.



Rys. 2. Architektura warstwy bezpieczeństwa usług w modelu CoRBAC
Fig. 2. The architecture of a security layer in the CoRBAC model

Warstwa bezpieczeństwa składa się z dwóch komponentów: przedstawionego w górnej części, który realizuje tradycyjną kontrolę dostępu, zgodnie z modelem RBAC, oraz jego rozszerzenie o analizę kontekstu i wykorzystujące ją mechanizmy bezpieczeństwa, przedstawione w dolnej części schematu. Wprowadzone logowanie wszystkich operacji oraz stosowanie wewnątrzsystemowych mechanizmów audytowych jest jedną z podstaw wyznaczania kontekstu działania użytkownika w zakresie wiązania ze sobą poszczególnych wywołań usług i sesji użytkownika.

Poniżej zaproponowano i omówiono na przykładach mechanizmy bezpieczeństwa, uwzględniające poszczególne typy kontekstu. Przedstawiono jedynie przykładowe mechanizmy – ich zbiór jest zdecydowanie szerszy.

3.1. Kontekst przestrzenny

Przyjmijmy podział przestrzeni, w której mogą znajdować się logicznie użytkownicy, na dwa obszary – użytkowników łączących się z systemem z sieci uczelnianej (sieć PG) oraz

sieci zewnętrznej (Internet). W stosunku do tradycyjnego modelu RBAC, dodajemy dodatkowe powiązanie: sieć, z której łączy się użytkownik – uprawnienia (uprawnienia przypisane do sieci) oraz regułę: wynikowe uprawnienia użytkownika są częścią wspólną przypisanych mu uprawnień (poprzez role) oraz uprawnień przypisanych do jego lokalizacji (sieci, za pomocą której łączy się z systemem). Sieć logiczna pełni w tym przypadku rolę wyznacznika lokalizacji użytkownika.

3.2. Zmiana kontekstu przestrzennego

Zupełnie innym podejściem jest obserwacja zmiany kontekstu przestrzennego w czasie. W takim przypadku lokalizacja użytkownika nie jest określana sztywno poprzez sieć, z której się łączy, a z wykorzystaniem bazy geolokalizacji adresów IP. W tym podejściu nie jest istotna sama lokalizacja użytkownika, a prędkość jej zmiany w czasie.

Przykładowo, użytkownik wykonuje operację w systemie z określonego IP, a następnie po krótkim czasie wykonuje kolejną operację z adresu IP, zlokalizowanego w stosunku do poprzedniego w określonej odległości. W momencie przekroczenia granicznej wartości stosunku odległości do czasu system blokuje dostęp.

3.3. Kontekst czasu

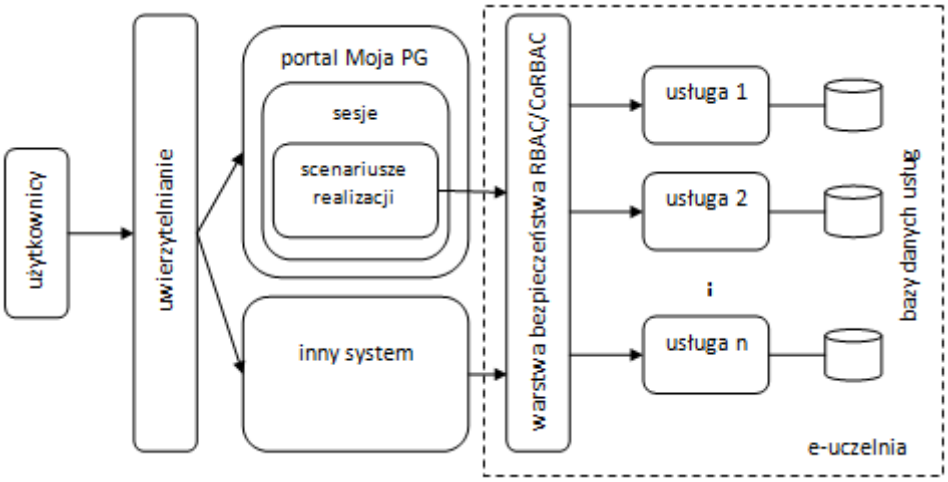
Kontekst czasu rozpatrujemy jako moment wykonania operacji w systemie. Możemy go wykorzystać wielorako. Pierwszym przykładem użycia jest ustalenie czasu, w jakim można wykonać jakąś operację, czyli uprawnienie do niej może zostać pozytywnie zweryfikowane. Może być to definiowalne jako okresowy przedział czasu, np. w godzinach 07:00-15:00 (lub wersja bardziej skomplikowana poprzez dodanie warunku – w dni robocze). Można też stworzyć bezwzględny przedział czasu, np. od godz. 08:00 1.01.2012 do godz. 15:00 31.12.2012. Innym przykładem jest wykorzystanie czasowości przypisania komuś danej roli (np. na czas zastępstwa).

4. Ocena bezpieczeństwa systemu e-uczelnia

Problem pomiaru bezpieczeństwa systemów informatycznych nie jest banalny. Najczęściej spotykanym podejściem do zagadnienia jest pomiar ryzyka, wiążącego się z używaniem oprogramowania. Dotyczy to zarówno bezpieczeństwa w zakresie nieautoryzowanego dostępu (ang. *security*), jak i utrzymania ciągłości działania (ang. *safety*). Jedną z miar może być

liczba rzeczywistych włamań oraz ich dalsze konsekwencje pod warunkiem, że wszystkie systemy są atakowane w podobny sposób, co w praktyce nie jest zawsze spełnione [10].

Pomiar, niezależnie od jego dziedziny, żeby był obiektywny i powtarzalny, musi opierać się na metrykach. Właśnie wyznaczenie tych metryk stwarza największą trudność. Bardzo istotny jest właściwy dobór metryk, żeby nie doprowadzić do niezamierzonego, fałszywego, bądź częściowego obrazu całości [11]. Ze względu na specyfikę zagadnienia bardziej użyteczne będą metryki relatywne w stosunku do arbitralnie dobranych skal. Często nie da się ich przedstawić w postaci liczbowej – wymagane jest operowanie na trendach: lepiej, gorzej, mniej, więcej [12].



Rys. 3. Architektura platformy IP^2 systemu e-uczelnia
Fig. 3. The IP2 platform architecture of the e-university system

Skupiając się na bezpieczeństwie w obszarze kontroli przed nieautoryzowanym dostępem i operacjami w systemie najczęstszym podejściem jest sprawdzanie tzw. checklisty – listy potencjalnych podatności, występujących w analogicznych systemach. Każda wykryta podatność powinna być oceniana pod kątem ryzyka, jakie niesie. Ryzyko to jest oceniane jako konsekwencje wystąpienia zagrożenia i może być rozpatrywane w różnych płaszczyznach. Jest to podstawa przeprowadzonego audytu bezpieczeństwa, który przyjęto jako procedurę pomiarową, pozwalającą oszacować poziom bezpieczeństwa. Został on przeprowadzony w środowisku o architekturze przedstawionej na rys. 3. Rozwiązanie takie umożliwia przełączanie warstwy bezpieczeństwa pomiędzy działaniem w trybie zgodnym z tradycyjnym modelem RBAC a modelem CoRBAC, co umożliwia analizę porównawczą.

Przyjęto, że bezpieczeństwo jest wprost proporcjonalne do liczby zastosowanych mechanizmów bezpieczeństwa, które zmniejszają liczbę potencjalnych zagrożeń (im mniej potencjalnych zagrożeń, niwelowanych przez zastosowane mechanizmy bezpieczeństwa, tym bezpieczniejszy system). Na potrzeby analizy wyników audytu przekształcono powyższą definicję do wzoru o postaci:

$$pb = 1 - \frac{lwz1 \cdot w1 + lwz2 \cdot w2 + lwz3 \cdot w3}{lpz1 \cdot w1 + lpz2 \cdot w2 + lpz3 \cdot w3}, \quad (1)$$

gdzie: *pb* oznacza poziom bezpieczeństwa, *lwz* – liczbę wykrytych zagrożeń odpowiednio poziomu od 1 do 3, *lpz* – liczbę wszystkich potencjalnych zagrożeń odpowiednio poziomu od 1 do 3, *w* – wagę odpowiednio poziomu od 1 do 3. Ostatni przeprowadzony audyt wykazał istnienie w systemie 8 zagrożeń średniego i 12 najniższego poziomu. Nie zidentyfikowano zagrożeń najwyższego poziomu. W odniesieniu do listy OWASP [3] poziom bezpieczeństwa wynosi 0,81 w skali od 0 do 1.

5. Podsumowanie

Ze względu na powszechną dostępność używanych systemów i narażenie ich na potencjalne ataki, należy stosować bardziej dynamiczne polityki bezpieczeństwa. Zastosowanie kontekstowo zorientowanego systemu bezpieczeństwa pozwala na zwiększenie bezpieczeństwa systemu, ponieważ zmniejsza liczbę potencjalnych zagrożeń. Należy zwrócić uwagę, że kontekst odgrywa zasadniczą rolę w sferze kontroli dostępu (ang. *security*), natomiast problemem jeszcze pozostaje uwzględnienie go w sferze zapewnienia ciągłości działania (ang. *safety*). Oprócz poprawności merytorycznej stosowanych mechanizmów, niezwykle istotny jest prawidłowy ich projekt techniczny i implementacja, tak aby powodowały jak najmniejszy dodatkowy koszt operacji, przez co były jak najmniej uciążliwe dla użytkownika.

Zaproponowany kontekstowo zorientowany system bezpieczeństwa został zaimplementowany w platformie IP2, która jest z powodzeniem wykorzystywana na Politechnice Gdańskiej od ponad 3 lat. System w tym czasie przeszedł pozytywnie audyt bezpieczeństwa, przeprowadzony przez zewnętrzną firmę audytującą. Był on podstawą do stwierdzenia wzrostu bezpieczeństwa. Dodatkowo, od czasu uruchomienia platformy nie zarejestrowano żadnych, zakończonych sukcesem, prób przełamania zabezpieczeń. Zaproponowano również rozszerzenie procedur audytowych o weryfikację zabezpieczeń z uwzględnieniem kontekstu działań użytkownika.

BIBLIOGRAFIA

1. Politechnika Gdańska: Moja PG. https://moja.pg.gda.pl
2. Oracle: Java Enterprise Edition. http://www.oracle.com/technetwork/java/index.html
3. OWASP Testing Guide v3. https://www.owasp.org/index.php/OWASP_Testing_Project

4. Benantar M.: Access Control Systems. Security, Identity Management and Trust Models. Springer-Verlag, 2006.
5. Lund M. S., Solhaung B., Stolen K.: Evolution in relation to risk and trust management. IEEE Computer, May 2010, p. 49-55.
6. Craig W. T., Dale R. T.: Identity Management. IEEE Internet Computing, IEEE Computer Society, May/June 2007, p. 82-85.
7. Cuppens F., Cuppens-Boulahia N.: Modeling contextual security policies. International Journal of Information Security, Vol. 7, Springer-Verlag, July 2008.
8. Maamar Z., Benslimane D., Narendra N. C.: What can Context do for Web Services? Communications of the ACM, December 2006, p. 98-103.
9. Krawczyk H., Lubomski P.: Generalized access control in hierarchical computer network. Zeszyty naukowe Wydziału Elektroniki, Telekomunikacji i Informatyki Politechniki Gdańskiej, tom 18, 2010, s. 217-222.
10. Payne S.C.: A Guide to Security Metrics. SANS Security Essentials GSEC Practical Assignment Version 1.2e, July 2006.
11. Hauser J.R., Katz G. M.: Metrics: you are what you measure! European Management Journal, April 1998, p. 517-528.
12. Hinson G.: Seven myths about information secuirty metrics. ISSA Journal, July 2006.
13. Feng X., Jun X., Hao H., Li X.: Context-Aware Role-Based Access Control Model for Web Services. Grid and Cooperative Computing – GCC 2004 Workshops SE – 54. Springer Berlin Heidelberg, Vol. 3252, 2004, p. 430-436.
14. Haibo S., Fan H.: A context-aware role-based access control model for Web services. IEEE International Conference on e-Business Engineering (ICEBE'05), 2005, p. 220-223.
15. Bhatti, R., Bertino, E., & Ghafoor, A.: A Trust-Based Context-Aware Access Control Model for Web-Services. Distributed and Parallel Databases, Springer US, Vol. 18(1), 2005, p. 83-105.
16. Woo J.W., Hwang M.J., Lee C.G., Youn H.Y.: Dynamic Role-Based Access Control with Trust-Satisfaction and Reputation for Multi-agent System. 2010 IEEE 24th International Conference on Advanced Information Networking and Applications Workshops, p. 1121-1126.
17. Damián-Reyes P., Favela J., Contreras-Castillo J.: Uncertainty Management in Context-Aware Applications: Increasing Usability and User Trust. Wireless Personal Communications, Vol. 56(1), 2009, p. 37-53.
18. Kulkarni D., Tripathi A.: Context-Aware Role-based Access Control in Pervasive Computing Systems. SACMAT'08, 2008.

Wpłynęło do Redakcji 11 marca 2013 r.

Abstract

The paper presents a generalized model of the access control to the web-based e-university system. It's an extension of the standard Role Based Access Control model taking into account the context of users' activities. There is defined context and its impact on security policy. The context consists of the user's current location (logical or physical), the moment of time of the operation execution, the purpose and action scenario, the users' relationship with the objects and operations and the general state of the system. This solution increases the level of security without considerable loss of the performance of the system. The proposed security system was implemented and introduced in IP^2 platform which is in use at Gdańsk University of Technology. The platform has nearly 30,000 active users and works without unauthorized access up to now.

Adresy

Henryk KRAWCZYK: Politechnika Gdańska, Wydział Elektroniki, Telekomunikacji i Informatyki, ul. Narutowicza 11/12, 80-233 Gdańsk, Polska, hkrawk@pg.gda.pl
Paweł LUBOMSKI: Politechnika Gdańska, Centrum Usług Informatycznych, ul. Narutowicza 11/12, 80-233 Gdańsk, Polska, lubomski@pg.gda.pl