BIULETYN INSTYTUTU AUTOMATYKI I ROBOTYKI
NR 28, 2010

Zapewnianie integralności informacji w systemach komercyjnych – model Clarka-Wilsona

Krzysztof LIDERMAN

Zakład Systemów Komputerowych, Instytut Teleinformatyki i Automatyki WAT,
ul. Gen. S. Kaliskiego 2, 00–908 Warszawa
lider@ita.wat.edu.pl

STRESZCZENIE: Artykuł dotyczy tematyki zapewniania ochrony informacji przed utratą integralności na skutek nieuprawnionego lub niewłaściwego przetwarzania. Podstawą rozważań jest model Clarka-Wilsona. Artykuł jest uzupełnieniem informacji zawartych w [5] i [6].

SŁOWA KLUCZOWE: tajność, integralność, model Bella-La Paduli, model Clarka-Wilsona, model Brewera-Nasha

1. Wprowadzenie

Próby formalnego ujęcia tematyki ochrony informacji przetwarzanej w systemach komputerowych podejmowane są od początku lat 70-tych XX wieku. W zależności od przyjętego stopnia restrykcyjności dostępu do chronionej informacji wyróżnia się dwie grupy modeli:

1) modele wykorzystujące „wojskowe" podejście do ochrony informacji, bazujące na klasyfikacji informacji i ściśle ustalonych przywilejach dostępu dla podmiotów. Podstawowymi w tej grupie są:
   - w zakresie tajności – model Bella-La Paduli,
   - w zakresie integralności – model Biby;
2) modele wykorzystujące „komercyjne" podejście do ochrony informacji, gdzie rezygnuje się z klasyfikacji informacji i ściśle ustalonych przywilejów

dostępu dla podmiotów na rzecz dynamicznego przydziału uprawnień i zapobieganiu niepożądanemu przepływowi i gromadzeniu informacji. Podstawowymi w tej grupie są:

- w zakresie tajności – model Brewera-Nasha (*chiński mur*),
- w zakresie integralności – model Clarka-Wilsona.

Niestety, zaimplementowanie w systemach i sieciach komputerowych reguł wynikających z modeli wymienionych w punkcie pierwszym (czyli zbudowanie wielopoziomowego „wojskowego" systemu ochrony informacji) jest niezmiernie trudne i kosztowne. W praktyce okazało się także, a ma to konkretne przełożenie na pieniądze wykładane na badania i zakupy przez przemysł, że w systemach komercyjnych, w odróżnieniu od systemów wojskowych, większą wagę przywiązuje się do integralności niż tajności informacji, a także do tego, kto wykonał jaką transakcję, niż co zobaczył. Dlatego rozwój „bezpiecznych" systemów komputerowych dla przemysłu i organizacji biznesowych poszedł własną drogą – formalnie opisują ją koncepcja „chińskiego muru" i model Brewera-Nasha [3], [6] oraz model Clarka-Wilsona [4].

2. Praca z danymi wrażliwymi w systemach komercyjnych – wymagania na ochronę

Podstawowe zasady, mające zapewnić integralność wrażliwych danych przetwarzanych w systemach informacyjnych firm z sektora finansowego, medycznego, przemysłowego itp. (nazywanych ogólnie *systemami komercyjnymi*), zostały ustanowione jeszcze w czasach „przedkomputerowych". W myśl tych zasad należy stosować:

1) dobrze opisane reguły przetwarzania danych (ang. *well-formed transaction*),
2) separację obowiązków pracowników (SoD, ang. *separation of duty*).

Pierwsza z wymienionych zasad ma zapewnić, że pracownik nie będzie przetwarzał danych w sposób dowolny, tylko zgodnie z ustalonymi regułami, a wszelkie manipulacje na danych będą odnotowywane dla celów kontrolnych (tzw. audit-log)[1]. Przykładem wdrożenia tej zasady w systemach rozliczeń księgowych jest rozbicie transakcji na uzupełniające się procesy i prowadzenie zapisów przebiegu transakcji (procesów) w co najmniej dwóch

[1] W przypadku działań na dokumentach papierowych, implementacja tej zasady sprowadza się do nakazu nanoszenia w nich wszelkich zmian bez wymazywania poprzednich zapisów, w sposób utrudniający takie działanie (w praktyce: zapisy wykonywane atramentem i skreślenia zamiast wymazywania).

oddzielnych księgach. Zapisy te podczas kontroli są składane i porównywane w celu wykrycia ewentualnych nadużyć czy niezgodności.

Druga z zasad (SoD) ma zapobiegać nadużyciom, które mogą powstać wtedy, gdy jeden pracownik przeprowadza całą transakcję. Zasada SoD wymusza podział transakcji na rozdzielne etapy wykonywane przez **różnych** pracowników, przy czym kolejny etap nie może być zrealizowany, o ile działania na poprzedzających go etapach nie zostały wykonane poprawnie. W praktyce zasada SoD wymusza zaangażowanie w wykonanie każdej transakcji co najmniej dwóch osób[2].

Nadużycia w przypadku wdrożenia tej zasady są możliwe, ale wymagają zmowy zaangażowanych w transakcję pracowników. Żeby taką zmowę utrudnić, angażuje się w wykonywanie transakcji większą liczbę osób oraz przeprowadza rotację pracowników zaangażowanych w wykonywanie transakcji. Innym zastosowaniem zasady SoD jest wdrożenie przepisów zakazującej osobie ustanawiającej reguły przeprowadzania transakcji (lub dopuszczającej te reguły do praktycznego użycia w firmie) wykonywania takich transakcji.

Zastosowanie opisanych zasad w odniesieniu do danych przetwarzanych w systemach komputerowych wymaga specjalnej interpretacji i implementacji. Wdrożenie zasady „dobrze opisanych reguł przetwarzania informacji" oznacza, że dane mogą być przetwarzane tylko przez dopuszczony do użytku, na podstawie określonych wymagań, zbiór programów. Te programy muszą mieć sprawdzoną i zatwierdzoną konstrukcję – w praktyce oznacza to nadzorowany proces wytwarzania oprogramowania i/lub inspekcję kodu w celu znalezienia np. ukrytych kanałów wycieku informacji. Muszą także być pod nadzorem, przez uprawnione osoby, dostarczane, instalowane i, w razie potrzeby, modyfikowane. Wdrożenie zasady SoD oznacza, że użytkownicy mają prawo do uruchamiania tylko ściśle określonych programów, a przyporządkowanie użytkownik – program odbywa się przez uprawnione osoby na podstawie dobrze określonych reguł i jest kontrolowane.

3. Model Clarka-Wilsona

Artykuł [4], opisujący model nazywany od nazwisk autorów artykułu modelem Clarka-Wilsona, został opublikowany w 1987 roku, w 13 lat po ukazaniu się artykułu D.E. Bella i L.J. La Paduli [1] oraz 4 lata po

[2] Co można zauważyć podejmując większe kwoty w banku – kasjerka przed wypłaceniem pieniędzy woła inną osobę, która autoryzuje transakcję.

opublikowaniu przez Departament Obrony USA w tzw. „Pomarańczowej Książce" (*Orange Book* [7]) kryteriów oceny „zaufanych" systemów komputerowych. Artykuł ten systematyzował, na podstawie wieloletnich doświadczeń, ówczesne poglądy na możliwości stosowania, głównie w praktyce biznesowej firm i organizacji finansowych, reguł przetwarzania informacji opracowanych dla specyficznych w tym zakresie potrzeb wojska i administracji rządowej. W tamtych latach wiedziano już, że w praktyce biznesowej stosowanie modelu Bella-La Paduli jest nieopłacalne, ale nie było modelu konkurencyjnego, przystosowanego do „komercyjnej" praktyki przetwarzania informacji. W [4] Clark i Wilson zaproponowali taki model, porównując go jednocześnie z modelem Bella-La Paduli (por. także uwagi w [2]).

Podstawowe elementy, z których składa się model zaproponowany w [4], to:

I. Dwa typy obiektów (danych):
   - dane przetwarzane zgodnie z ustalonymi regułami (CDI, ang. *Constrained Data Items*[3]),
   - dane, które nie podlegają ustalonym dla CDI regułom przetwarzania[4] (UDI, ang. *Unconstrained Data Items*). Przykładem takich danych są dane wprowadzane do systemu przez użytkownika za pomocą klawiatury.

II. Dwie procedury działań na danych typu CDI:
   - procedura weryfikacji integralności (IVP, ang. *Integrity Verification Procedure*). Zadaniem IVP jest potwierdzenie, że w chwili działania tej procedury wszystkie dane typu CDI są integralne,
   - procedura transformacji (TP, ang. *Transformation Procedure*). Procedury tego typu są implementacją zasady „dobrze opisanych reguł przetwarzania" – w ich wyniku zbiór danych typu CDI jest przekształcany z jednego poprawnego stanu w inny poprawny, w sensie konkretnego zbioru reguł, stan.

   Poprawność działania konkretnej procedury TP lub IVP jest ustalana poprzez certyfikację zgodności ich działania z konkretną polityką zapewniania integralności. Zapewnianie integralności jest zatem procesem dwuczęściowym: najpierw certyfikacja zgodności procedur z przyjętą

[3] System musi zapewnić, że te dane są przetwarzane wyłącznie przez procedurę typu TP. Jest to specyficzne „ograniczenie", wyjaśniające angielską nazwę tego typu danych.

[4] Należy mieć na uwadze, że chodzi tu o reguły określone w modelu Clarka-Wilsona omawiane w niniejszym opracowaniu. Nie oznacza to jednak, że proces przetwarzania UDI nie podlega żadnym regułom – mogą to być reguły wynikające z konkretnej polityki ochrony informacji.

w danej firmie polityką zapewniania integralności, wykonywana przez osoby odpowiedzialne za bezpieczeństwo informacji, następnie wdrożenie tych procedur w komputerowym systemie przetwarzania informacji.

III. Dziewięć reguł:

III.1. Pięć reguł „certyfikacyjnych" (ang. *certification rules*):

C1: Procedura weryfikacyjna (IVP) musi potwierdzić, że w chwili działania tej procedury wszystkie dane typu CDI są integralne.

C2: Wszystkie procedury transakcyjne (TP) muszą mieć potwierdzoną w procesie certyfikacji poprawność działania, tzn. zbiór integralnych danych musi być transformowany zawsze w integralny zbiór danych. W praktyce oznacza to, że dla każdej procedury TP_i i dla każdego zbioru danych CDI_j, na którym TP_i może działać (ma „dopuszczenie" do działania), musi być określona, np. przez osobę odpowiedzialną za bezpieczeństwo informacji, relacja (TP_i, (CDI_1, CDI_2, CDI_3, …)) gdzie lista CDI_j definiuje określony zbiór danych, dla których TP_i uzyskała certyfikację.

C3: Relacje z reguły E2 (patrz dalej punkt III.2) muszą zapewniać spełnienie zasady SoD.

C4: Wszystkie procedury transakcyjne (TP) muszą zapisywać informacje niezbędne do kontroli przeprowadzonych transformacji (transakcji) w „dopisywalnym" (ang. *append-only*) dzienniku zdarzeń (logu, jest to także obiekt typu CDI). Operacja dopisywania różni się od operacji pisania tym, że uniemożliwia zmianę istniejących danych, do których są dopisywane tą operacją nowe dane.

C5: Każda procedura transakcyjna (TP), jeżeli otrzyma na wejściu dane typu UDI, musi je przekształcić na dane typu CDI lub usunąć.

III.2. Cztery reguły „wykonawcze" (ang. *enforcement rules*):

E1: System musi utrzymywać listę relacji

$$(TP_i, (CDI_1, CDI_2, CDI_3, \ldots))$$

i musi zapewniać, że dla każdego CDI_j transformacje są wykonywane wyłącznie przez TP_i określoną w relacji.

E2: System musi utrzymywać listę relacji (UserID, TP_i, (CDI_1, CDI_2, CDI_3, …)) łączących konkretnego użytkownika (identyfikowanego przez UserID) z konkretnym zbiorem przypisanych mu, zgodnie z regułą certyfikacyjną C3, procedur

TP i związanych z tymi procedurami zbiorem danych CDI oraz musi zapewniać, że dla każdego CDI_j transformacje są wykonywane wyłącznie przez TP_i określoną w relacji.

E3: System musi zapewnić poprawne uwierzytelnianie i autoryzację każdego użytkownika.

E4: Jedynie podmiot[5] mający uprawnienia do certyfikacji może modyfikować przyporządkowania użytkowników i CDI do procedur typu TP. Jednocześnie podmiot taki nie może mieć uprawnień do działania na CDI i TP, które certyfikuje lub modyfikuje.

Można zauważyć, że wymagania na „komercyjne" przetwarzanie informacji, w kontekście zachowania jej integralności, można podzielić na dwie grupy:

- wymagania na *integralność wewnętrzną*, zapewnianą przez system komputerowy,
- wymagania na *integralność zewnętrzną*, zapewnianą przez odpowiednie rozwiązania organizacyjne (poza systemem komputerowym), dotyczące np. audytu, przydziału obowiązków itp. W ogólności, zapewnienie integralności zewnętrznej sprowadza się do sformułowania, wdrożenia i nadzoru *polityki* ochrony informacji.

Zatem podstawowe kryteria, pozwalające ocenić, czy system komputerowy, w którym są przetwarzane informacje, spełnia „komercyjne" wymagania ochrony, są następujące:

1. System musi zapewniać oddzielne uwierzytelnianie i autoryzację dla każdego użytkownika.
2. System musi zapewniać, że określone dane są przetwarzane wyłącznie przez dopuszczony do użytku zbiór sprawdzonych (zaufanych) programów, które spełniają zasadę „dobrze opisanych reguł przetwarzania danych".
3. System musi zapewnić przydzielanie użytkownikom programów (które mogą uruchomić na konkretnych danych) zgodnie z regułą SoD.
4. System musi zapewnić możliwość odnotowania w dziennikach zdarzeń (logach systemowych) wszystkich uruchamianych programów wraz z nazwą (lub identyfikatorem) użytkownika, który je uruchomił.

[5] Termin „podmiot" oznacza tutaj osobę lub zespół wyznaczony, na podstawie obowiązujących w konkretnej firmie/organizacji zasad i przepisów, do wykonania wymienionych działań (certyfikacji i modyfikacji).

5. System musi zawierać mechanizm zapewniający spełnienie wymagań 1-4.
6. Mechanizm, o którym mowa w punkcie 5, musi być odporny na manipulacje i nieuprawnione zmiany.

4. Podsumowanie

Mechanizmy zapewniające „bezpieczne" przetwarzanie informacji na bazie modelu Clarka-Wilsona różnią się istotnie od mechanizmów stosowanych w modelu Bella-La Paduli. Po pierwsze, integralność przetwarzanych danych jest zapewniana przez określenie zbioru programów przetwarzających, a nie przez przypisanie do określonego poziomu tajności. Po drugie, użytkownikowi nie wyznacza się uprawnień do czytania lub zapisywania określonych danych, tylko do wykonywania określonego zbioru programów na określonych danych.

Literatura

1. BELL D.E., LA PADULA L.J., *Secure Computer System: Unified Exposition and Multics Interpretation*, ESD-TR-75-306, Bedford 1974 MA: ESD/AFSC, Hanscom AFB, Available at: http://csrc.nist.gov/publications/history/bell76.pdf.
2. BELL D.E., *Looking Back at the Bell-La Padula Model*, Reston VA, 20191, Dec. 7. 2005.
3. BREWER D., NASH M., *The Chinese Wall Security Policy*, Proc. IEEE Computer Society Symposium on Research in Security and Privacy, pp. 215-228, 1989.
4. CLARK D., WILSON D.R., *A Comparison of Commercial and Military Computer Security Policies*, Proc. IEEE Symposium on Research in Security and Privacy, pp. 184-194, 1987.
5. LIDERMAN K., *O organizacji i implementacji mechanizmów dostępu do informacji wrażliwych przetwarzanych w systemach teleinformatycznych*, Biuletyn WAT, Vol. LVII, Nr 4, 2008.
6. LIDERMAN K., *O ochronie informacji przed niepożądanym przepływem i gromadzeniem*, [w:] Kosiński J. (red): Przestępczość teleinformatyczna, str. 95-101, WSPOL, Szczytno, 2009.
7. Trusted Computer System Evaluation Criteria. DoD, 15 August 1983, CSC-STD-001-83.

Information integrity assurance in commercial computer systems – the Clark-Wilson model

ABSRACT: The paper concerns the protection of information integrity in commercial computer systems. The basis is an example of the Clark-Wilson model. This paper is a supplement to the content of papers [5] and [6].

KEY WORDS: security, integrity, the Bell-La Padula model, the Clark-Wilson model, the Brewer-Nash model

Praca wpłynęła do redakcji: 12.02.2010.