WYDAWNICTWO POLITECHNIKI ŚLĄSKIEJ W GLIWICACH

ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 2018
Seria: ORGANIZACJA I ZARZĄDZANIE z. 130

IDENTYFIKACJA ZMIAN ATRYBUTU INTEGRALNOŚCI PLIKÓW KOMPUTEROWYCH, JAKO ELEMENT ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

Artur SZLESZYŃSKI

Akademia Wojsk Lądowych im. gen. Tadeusza Kościuszki, Wrocław; artur.szleszynski@awl.edu.pl

Streszczenie: W pracy przedstawiono koncepcję wykorzystania funkcji skrótu do badania zmian atrybutu integralności wiadomości. Zaprezentowano wyniki badań czasu potrzebnego do binarnego porównania plików oraz czasu potrzebnego do wygenerowania funkcji skrótu. Przedstawiono proces postępowania z wiadomością w momencie stwierdzenia naruszenia atrybutu integralności.

Słowa kluczowe: atrybut integralności zasobu informacyjnego, funkcja skrótu wiadomości.

IDENTIFICATION CHANGES OF INTEGRITY ATTRIBUTE OF COMPUTER FILES AS A COMPONENT OF INFORMATION SECURITY MANAGEMENT

Abstract: Paper presents the concept of the hash function use in order to examine changes in file integration attribute. The results of time necessary to binary comparison of files and time needed to hash function generation were presented. Then, the process of the file handling that its integrity attribute is violated, was shown.

Keywords: information assets attribute of integrity, message hash function.

1. Wprowadzanie

W grupie zasobów informacyjnych organizacji pliki komputerowe stanowią sposób na gromadzenie i przechowywanie użytecznych informacji. Elektroniczna postać informacji pozwala na szybką wymianę informacji pomiędzy lokalizacjami organizacji przy wykorzystaniu infrastruktury telekomunikacyjnej. To zaś decyduje o przebiegu procesów

decyzyjnych wewnątrz i na zewnątrz organizacji. Jeżeli przyjąć, że system informacyjny[1] wspomagany podsystemami informatycznymi służy efektywnemu działaniu organizacji to zachowanie bezpieczeństwa zasobów informacyjnych nabiera kluczowego znaczenia. Norma PN ISO/IEC 27000 stwierdza, że informacja jest ważnym aktywem organizacji (ISO 27000, 2015). Zatem dbałość o bezpieczeństwo zasobów informacyjnych jest jednym z kluczowych zadań Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) tworzonego wewnątrz organizacji.

Norma stwierdza, że bezpieczeństwo informacji definiowane jest przez zachowanie jej: poufności, integralności oraz dostępności (ISO 27000, 2015). Inne ujęcie definicji pojęcia „bezpieczeństwa informacji" zostało przedstawione w pracy K. Lidermana. Według autora pojęcie bezpieczeństwo informacji oznacza *"... stopień uzasadnionego (np. analizą ryzyka i przyjętymi metodami z ryzykiem) zaufania, że nie zostaną poniesione straty wynikające z niepożądanego (świadomego lub przypadkowego): ujawnienia, modyfikacji, zniszczenia lub uniemożliwienia przetwarzania informacji przechowywanej, przetwarzanej i przesyłanej w określonym systemie obiegu informacji"* (Liderman, 2008). Wymienione w normie elementy są atrybutami[2] bezpieczeństwa zasobu informacyjnego. Atrybut integralności definiuje się, jako *„właściwość polegającą na zapewnieniu dokładności i kompletności"* (ISO 27000, 2015). Bardziej szczegółowo pojęcie integralności definiowane jest w pracy K. Lidermana, gdzie *„integralność informuje, czy dane i informacje są poprawne, nienaruszone i nie zostały poddane manipulacji"* (Liderman, 2012).

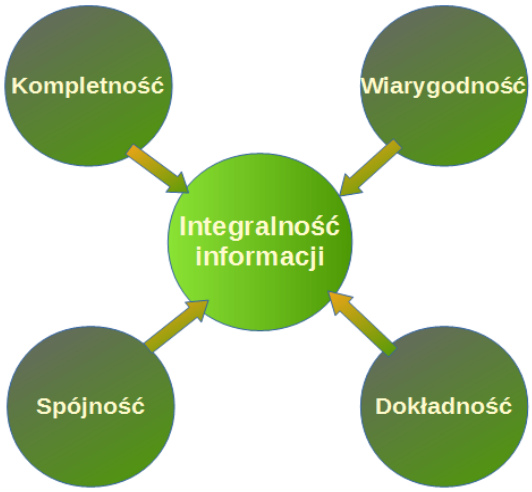
Inne ujęcie terminu integralności przedstawiono w pracy S. Kaczmarka, gdzie stwierdza się, że: *„integralność danych polega na zapewnieniu im: kompletności, wiarygodności, spójności i dokładności"* (Kaczmarek, 2018). Jeżeli dane są szczególnym przypadkiem informacji (informacja zapisana jest w postaci cyfrowej) to można zauważyć, że atrybut integralności definiowany jest przez cztery kolejne atrybuty wymienione w definicji rys. 1.

Podejście prezentowane w definicji jest interesujące, ale i trudne do wyrażenia wartościami liczbowymi. Jak zdefiniować miarę kompletności informacji, tak by zachować powtarzalność pomiaru? Warunek powtarzalności konieczny jest do weryfikacji uzyskanych wyników przez stronę trzecią[3], którą może być audytor bezpieczeństwa informacji. Zatem w pracy integralność informacji rozumiana będzie zgodnie z definicją przedstawioną przez K. Lidermana. Przyjęcie, że integralność informacji związana jest z brakiem zmian w zawartości pliku umożliwia np. binarne (bajt po bajcie) porównanie.

[1] Przez system informacyjny rozumie się wszystkie postaci informacji analogowe i cyfrowe znajdujące się poza urządzeniami komputerowymi. Jest to inne podejście niż zawarte w definicji zamieszczonej w normie PN - ISO/IEC 27000, gdzie system informacyjny utożsamiany jest informacją znajdującą się w urządzeniach komputerowych wykorzystywanych w organizacji oraz jej otoczeniu.

[2] Pojęcie atrybutu norma odnosi do właściwości obiektu (w tym przypadku zasobu informacyjnego), który może mieć wymiar ilościowy lub jakościowy. Ponadto atrybut może być rozróżniany (ISO 27000, 2015).

[3] Przez stronę trzecią rozumie się np. audytora bezpieczeństwa informacyjnego.



Rysunek 1. Atrybuty definiujące integralność zasobu informacyjnego. Kaczmarek, 2018.

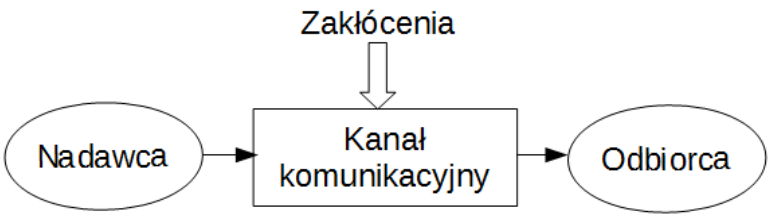
Zatem atrybut integralność odnosi się, do jakości informacji używanej w procesie decyzyjnym. Jeżeli nie doszło do żadnego z wymienionych zdarzeń to informację można uznać za godną zaufania. Co więcej zmiana wartości atrybutu integralności informacji może sugerować naruszenie atrybutu poufności. Jednakże stwierdzenie tego faktu wymaga dodatkowego badania, bazującego na wnioskowaniu rozmytym. Posłużenie się logiką rozmytą wynika z faktu istnienia wiedzy niepewnej. Tym, co posiada decydent jest przypuszczenie wystąpienia zdarzenia naruszenia atrybutu poufności. Przykład oceny bazującej na logice rozmytej przedstawia praca H. Hosmer, gdzie posługiwanie się aparatem logiki rozmytej w odniesieniu do oceny wnioskowania na podstawie danych zapisanych w systemie bazy danych (Hosmer, 1993). Wracając do zagadnień bezpieczeństwa systemów komputerowych, jeśli chcieć opisać ich bezpieczeństwo przy pomocy logiki klasycznej należy się posłużyć precyzyjnym aparatem pojęciowym. Jednakże precyzja aparatu pojęciowego i złożoność systemu wzajemnie się wykluczają (Hosmer, 1993). Próba wykazania pełnego bezpieczeństwa wymaga posłużenia się prostym obiektem a nie systemem. Pojawia się pytanie – jak zatem ocenić system składający się z wielu obiektów, gdzie każdy posiada niezerową liczbę cech indywidualnych? Proponowanym rozwiązaniem jest posłużenie się logiką rozmytą do oceny nieścisłości i niedokładności badanego systemu (Hosmer, 1993).

Zatem stwierdzenie, czy doszło do naruszenia atrybutu integralności zasobu informacyjnego oraz co było przyczyną opisanego zdarzenia stanowi ważne zadanie w procesie zarządzania bezpieczeństwem informacji w organizacji. Zadania tworzące proces weryfikacji naruszenia atrybutu integralności zasobu informacyjnego muszą dawać wiarygodne i powtarzalne wyniki oraz powinny być efektywne czasowo. Zadania odpowiedzialne za sprawdzenie nie mogą angażować zasobów sprzętu powyżej przyjętego kryterium. Takimi kryteriami oceny efektywności metod mogą być: procentowe wykorzystanie procesora oraz rozmiar pamięci operacyjnej przydzielonej do wykonania zadania.

2. Geneza problemu

Literatura przedmiotu dzieli komunikację na dwie kategorie: rozgłoszeniową oraz punkt – punkt[4]. Oba rodzaje komunikacji posiadają wady i zalety, które nie będą opisywane w pracy. W praktyce biznesowej wykorzystywane są obie wymienione kategorie komunikacji.

Chcąc porównać zmiany wprowadzone w treści wiadomości najprościej jest porównać jej zawartość w miejscu odebrania z treścią znajdującą się u nadawcy. Zatem w systemie powinny się pojawić dwie wiadomości: wzorzec (wiadomość w miejscu wprowadzenia jej do kanału komunikacyjnego) i wiadomość do porównania. Wiadomość od nadawcy do odbiorcy należy wysłać co najmniej dwa razy. Przyjęta metoda oceny, porównanie wzorca z odebraną wiadomością, powiązana jest z definicją systemu komunikacyjnego, w którym występują elementy takie jak: nadawca (nazwany też źródłem), kanał komunikacyjny oraz odbiorca, co pokazano na rys. 2 (Haykin, 2001).



Rysunek 2. System komunikacyjny. Na podstawie Haykin, 2001.

Na kanał komunikacyjny oddziałują zakłócenia, które mogą powodować zniekształcenia przekazywanej wiadomości. W przypadku informacji analogowej odfiltrowanie zakłóceń jest trudne. Prostszym zadaniem jest filtrowanie zakłóceń dla wiadomości w postaci binarnej, gdyż możliwe jest dołączenie informacji np. o liczbie wartości 1 w wiadomości lub dołączenie kodu korekcyjnego. Występowanie zakłóceń, naturalnych lub sztucznie generowanych, będzie wpływać na wzorzec i wiadomość odebraną. Zatem pojawia się kolejny problem do rozwiązania, który można sformułować następująco – jak przesłać wzorzec systemie komunikacyjnym tak by jego zawartość pozostała nie zmieniona pomimo istnienia zakłóceń w kanale komunikacyjnym? Jeżeli udałoby się rozwiązać wymieniony problem to przesyłanie wzorca staje się bezzasadne, gdyż wiadomość odebrana przez odbiorcę będzie identyczna z wzorcem. Skoro, co stwierdzono wcześniej, w kanale komunikacyjnym pojawia się zakłócenie to wzorzec również ulegnie zniekształceniu. Czy w opisanych warunkach przesyłanie wzorca do odbiorcy jest zasadne? Co może upewnić odbiorcę, że wzorzec, z którym porównuje wiadomość nie został zmieniony, czyli został

[4] Komunikacja rozgłoszeniowa – oznacza wykorzystanie jednego nadawcy (źródła wiadomości), która dostarczana jest do wszystkich odbiorców jednocześnie np. radiofonia lub telewizja. Ten rodzaj komunikacji jest typowy dla analogowych sieci radiowych. Komunikacja punkt – punkt oznacza utworzenie połączenia pomiędzy nadawcą a odbiorcą. Komunikacja ta jest dwukierunkowa tzn. nadawca i odbiorca mogą zamieniać się funkcjami (Haykin, 2001).

zachowany atrybut integralności odebranej wiadomości? W przypadku wiadomości w postaci analogowej stwierdzenie nie naruszenia atrybutu integralności może być trudne. Trudność polega na tym, że zakłócenie zmieniające treść przekazu może być trudne do odfiltrowania. W przypadku cyfrowej postaci informacji możliwe jest wyznaczenie funkcji skrótu wiadomości według zależności pokazanej w równaniu (1).

$$h_1 = H(m_1) \tag{1}$$

gdzie:

h_1 – wartość funkcji skrótu,

H – funkcja wyznaczająca skrót wiadomości,

m_1 – przesyłana wiadomość.

Zaletą stosowania wartości funkcji skrótu wiadomości jest jej niewielki rozmiar od 16 do 32[5] bajtów. Inaczej niż w przypadku szyfrowania wartość funkcji skrótu nie pozwala na uzyskanie postaci źródłowej wiadomości ale pozwala zweryfikować czy nie została ona zmodyfikowana. To umożliwia zdefiniowanie problemów, które zamierza się rozwiązać w pracy.

3. Definicja problemów badawczych

- Jaki jest potrzebny czas do porównania zawartości dwóch plików o różnych rozszerzeniach i rożnych rozmiarach?
- Jaka minimalna zmiana w treści pliku zostanie odwzorowana w wartości funkcji skrótu?
- Kiedy zostanie stwierdzone naruszenie integralności zasobu informacyjnego, jak należy postąpić z takim plikiem?

Chcąc udzielić odpowiedzi na postawione pytania problemowe posłużono się grupą plików o różnym rozmiarze i przeznaczeniu (różne formaty plików). Do badania wykorzystano funkcję skrótu MD – 5. Funkcja ta wykorzystywana jest w procesie tworzenia kluczy sesji w standardzie bezpiecznej transmisji, w sieci Internet[6]. Funkcja skrótu MD – 5 podsiada podatność, którą jest możliwość wystąpienia kolizji, co opisuje zależność (2).

$$\exists(m_1 \neq m_2) \wedge \exists\{h_1 = H(m_1), h_2 = H(m_2)\} \Rightarrow h_1 = h_2 \tag{2}$$

gdzie:

h_1 – wartość funkcji skrótu wiadomości m_1,

h_2 – wartość funkcji skrótu wiadomości m_2,

H – funkcja wyznaczająca skrót wiadomości,

m_1 – wiadomość pierwsza,

m_2 – wiadomość druga.

[5] 16B dla funkcji skrótu MD - 5, 32B dla funkcji skrótu SHA - 256.

[6] Protokół wymiany kluczy Diffie'go – Hellman'a.

Możliwość wystąpienia kolizji sprawiła, że organizacja ITEF[7] w dokumencie RFC – 6151 wydała zalecenie zastąpienia funkcji skrótu MD – 5 inną funkcją, która jest bardziej odporna na możliwość wystąpienia kolizji np. SHA – 256 lub AES (RFC6151, 2011).

4. Propozycja rozwiązania

Jeżeli sprawdzenie integralności dwóch plików wykonać na zasadzie binarnego porównania ich zawartości to czas potrzebny do wykonania takiej czynności przedstawiono w tabeli 1.

Jednakże, co opisano wcześniej, wymaga on istnienia kanału komunikacyjnego pozbawionego zakłóceń. Warunek ten nie jest możliwy do spełnienia, gdyż nie istnieje kanał komunikacyjny, w którym nie byłby obecny szum. Zatem przesłanie wiadomości wzorcowej obarczone jest możliwością zmiany jej treści, co może zmienić wynik porównania. Dodatkowo metoda wymaga posiadania odrębnego kanału komunikacyjnego, co w pewnych warunkach może być nieosiągalne np. kanały radiowe wykorzystywane w komunikacji pomiędzy abonentami w sieci.

Tabela 1.
Czas potrzebny do binarnego porównania zawartości dwóch plików

Lp.	Rozmiar pliku [kB]	Czas porównania [s]
1	97	1,1
2	97 / 152	0,83
3	310	0,69
4	619	5,76
5	1273	1,1

W celu porównania czasu potrzebnego do wyznaczenia funkcji skrótu dla pliku testowego posłużono się plikiem o rozmiarze 518 kB[8], dla którego wyznaczana była wartość funkcji skrótu. Wartość statystyki opisowej czasu potrzebnego do wyznaczenia wartości funkcji skrótu MD5 dla pliku testowego pokazano w tabeli 2. Do oszacowania czasu potrzebnego obliczenia funkcji skrótu posłużono się narzędziem MD5 Checksum Tool.

[7] Internet Engineering Task Force – zespół zadaniowy ds. inżynierii internetowej.
[8] Plik jest większy o 38 B od wartości średniej rozmiaru plików w próbie testowej.

Tabela 2.
Parametry rozkładu statystyki czasu potrzebnego do wyznaczenia wartości funkcji skrótu dla pliku testowego

Parametr rozkładu	Wartość
Średni czas [s]	0,11
Maksymalny czas [s]	0,25
Minimalny czas [s]	0,01
Odchylenie standardowe	0,076

Na podstawie danych zaprezentowanych w tabeli 2 wynika, że obliczenie wartości funkcji skrótu nie jest działaniem wymagającym długiego czasu. Dla pliku testowego o rozmiarze 518 kB maksymalny czas potrzebny do wyznaczenia wartości funkcji skrótu wyniósł 0,25s, gdy binarne porównanie dwóch plików o rozmiarze 619 kB wymagało 5,76 s. Co więcej maksymalny czas potrzebny do wyznaczenia funkcji skrótu był 0,44 s krótszy od czasu potrzebnego do binarnego porównania dwóch plików o rozmiarze mniejszym od pliku testowego. Można przyjąć, że jest to wartość akceptowalna przyjmując, jako kryterium oceny rozmiar pliku. Jeżeli przyjąć, że liczba plików o podobnym rozmiarze wyniesie np. 100 wówczas czas potrzebny do wyznaczenia wartości funkcji skrótów dla wszystkich plików będzie się zawierał w przedziale od 1 do 25 s., z wartością średnią 11 s. Podane wartości można zaakceptować, jeśli uwzględni się wydajność obliczeniową współczesnych systemów komputerowych.

Kolejną kwestią, którą zamierzano sprawdzić jest zdolność funkcji skrótu do wykrywania małych zmian w treści pliku. Parametr ten można nazwać czułością funkcji skrótu. Przez małą zmianę rozumie się wartość zmian poniżej 10% zawartości pliku. Modyfikacje wprowadzono przy wykorzystaniu edytora heksadecymalnego. Przy pomocy narzędzia zmodyfikowano bajty wewnątrz plików należących do grupy testowej, po czym wyznaczono wartości funkcji skrótów dla zmodyfikowanych plików. Obliczone wartości funkcji skrótu dla podanej próby testowej plików oraz ich modyfikacji pokazano w tabeli 3.

Zmiany, jakie wprowadzono do plików są małe zatem zaleca się traktować je, jako celowe czyli takie które przynoszą korzyść atakującemu[9]. Innym rodzajem zmian są zmiany duże, czyli takie w których liczba zmienionych bajtów przekracza wartość 40%. Taka zmiana może być podyktowana szyfrowaniem zawartości pliku (Szleszyński, 2015). Opisany incydent typowy jest dla działania oprogramowania złośliwego nazywanego ransomeware.

Do wyznaczenia procentowego poziomu zmian, które wystąpiły w otrzymanym pliku konieczne jest użycie pliku wzorcowego.

[9] Przykładem takiej jest zmiany jest podmiana numeru konta bankowego potrzebnego do wykonania przelewu. Rozmiar takiej zmiany nie przekracza 10% rozmiaru pliku, mierzonego liczbą bajtów. Jako przykład ataku można podać malware o nazwie ZeuS (ZeuS, 2018).

Tabela 3.
Przykład zmian w wartości funkcji skrótu powstałych w wyniku modyfikacji zawartości plików źródłowych

Plik wzorcowy	Wartość funkcji MD - 5 plik wzorcowy	Plik zmodyfikowany	Wartość funkcji MD - 5 plik zmodyfikowany
plik1.doc	30E1DF1B05AC757537159C3CEFBA0094	plik1m.doc	8BDCB6B2FD55E41D60B9D07C48C65FB6
plik2.pdf	664AB1BCD90CA429752643DC3E0A6CB6	plik2m.pdf	CC690EB99939022E6EA933AE8E510B3A
plik3. mpp	65F5B187D8BDCD7B30A98391EFDD231A	plik3m. mpp	2190246F6E44C800BF02E099C90CE4C1
plik4. pcapng	594CDE5672FC3A49903F9BE346C2C79F	plik4m. pcapng	CA9DBC8EC4F7857EC357A6AF5443E437

Wartość zmiany może zostać oszacowana po przesłaniu pliku, którego treść została zmodyfikowana do źródła wiadomości, czyli do nadawcy. Procentową modyfikację zawartości plików należących do próby testowej przedstawiono w tabeli 4.

Pytaniem, na które należy udzielić odpowiedzi jest sposób postępowania z zasobem informacyjnym (plikiem) w momencie stwierdzenia naruszenia jego atrybutu integralności. Pierwszą czynnością, jaką zaleca się wykonać, jest zweryfikowanie istotności oraz rozmiaru zmian. Czasami zmiana zawartości pliku nie stanowi problemu dla poprawnego zinterpretowania jego treści[10]. W systemach telekomunikacji cyfrowej istnieją mechanizmy ochrony treści wiadomości przed przypadkową lub celową zmianą jej treści. Należą do nich techniki badające poprawność przesłanych danych, do których zaliczają się kody korekcyjne lub sumy kontrolne (Casad, 2018),(Lammle, 2007).

W przypadku komunikacji z wykorzystaniem protokołów TCP/IP w przypadku różnic pomiędzy obliczoną sumą kontrolną a umieszczoną sumą kontrolną w nagłówku protokołu TCP, następuje żądanie powtórzenia transmisji pakietów lub datagramów (Lammle, 2007). Czynność ta odbywa się bez udziału nadawcy i odbiorcy[11] wiadomości (pakietu danych), gdyż wynika ze standardu, w jaki odbywa się komunikacja pomiędzy dwoma punktami docelowymi. Problem pojawia się w momencie, kiedy nie ma możliwości powtórzenia transmisji danych ze względu na niską przepustowość łącza lub częste przerwania połączenia. Jest to sytuacja typowa dla łączności radiowej, gdzie kanał transmisyjny poddawany jest oddziaływaniu zakłóceń o naturalnym lub sztucznym pochodzeniu. Opisana sytuacja występuje w przypadku, gdy odbiorca i/lub nadawca przemieszczają się, co powoduje, że zmienia się odległość pomiędzy punktami docelowymi w sieci radiowej oraz warunki propagacyjne.

[10] Przez to pojęcie należy rozumieć możliwość odtworzenia pierwotnej treści lub przesłania wiadomości przez jej odbiorcę, a następnie zachowanie się zgodne z intencją nadawcy wyrażoną w odebranej wiadomości.
[11] Przez nadawcę i odbiorcę rozumie się osoby lub programy wysyłające i odbierające dane.

Przedstawione zdarzenia sprawiają, że komunikacja pomiędzy uczestnikami będzie charakteryzować się niską niezawodnością i jakością. W przypadku wystąpienia opisanej wcześniej sytuacji należy przygotować procedury postępowania z odebranymi wiadomościami, których atrybut integralności został zmieniony. Rozważania zostaną ograniczone do wiadomości przesyłanych w cyfrowych systemach telekomunikacyjnych, tak więc można przedstawić ich reprezentację fizyczną jako plik. Przykładowy proces postępowania z wiadomością otrzymaną od nadawcy przedstawiono na rysunku 3.

Tabela 4.
Liczba zmienionych bajtów w pliku zmodyfikowanym w porównaniu do pliku wzorcowego

Plik	Liczba zmienionych bajtów	Procentowa wartość zmiany [%]
plik1.doc / plik1m.doc	10	0,0101
plik2.pdf / plik2m.doc	11	0,0034
plik3.mpp / plik3.mpp	5	0,00078
plik4.pcapng / plik4m.pcapng	11	0,00084

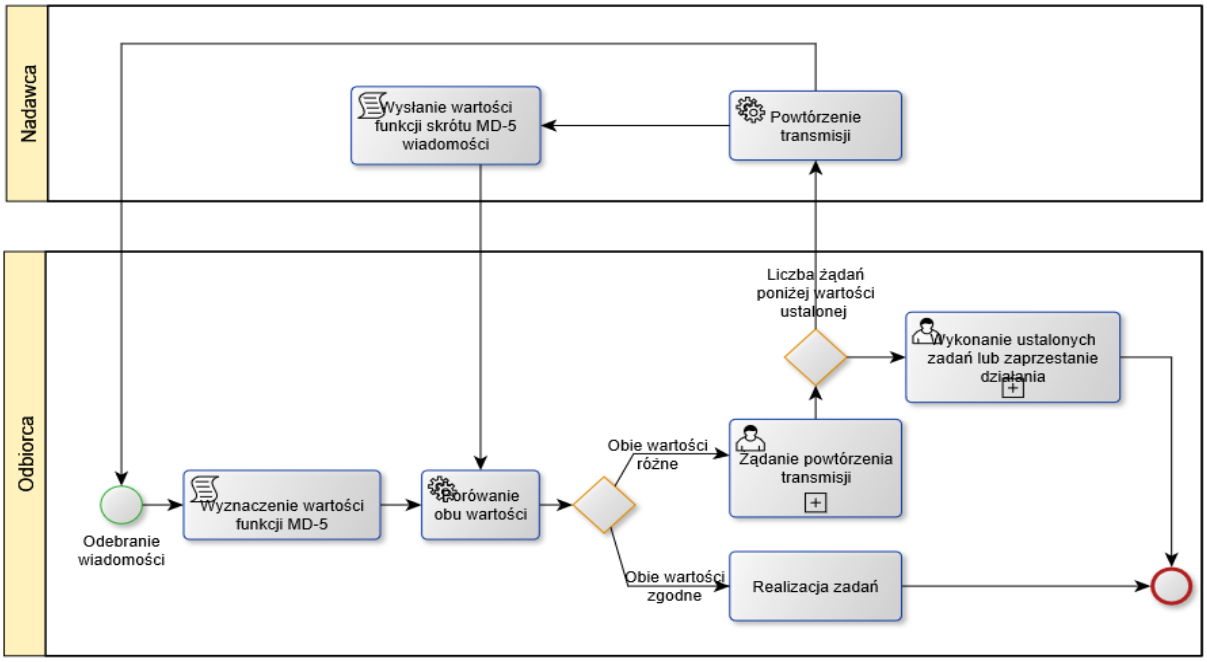
W przypadku gdy występują różnice w wartościach funkcji skrótów jednakże wiadomość została odebrana a jej treść jest niezrozumiała dla odbiorcy należy wygenerować żądanie powtórzenia transmisji (rys. 3). Liczbę żądań powtórzenia transmisji wiadomości należy ograniczyć, gdyż może wystąpić zjawisko wypełnienia pasma transmisji wewnątrz kanału telekomunikacyjnego. Jest ono wynikiem kolejnych retransmisji wiadomości od nadawcy do odbiorcy oraz niskiej przepustowości kanału telekomunikacyjnego[12]. Na niską przepustowość kanału mają wpływ zakłócenia obecne w nim (Haykin, 2001).

Brak jednoznacznego przekazu zawartego w wiadomości może skutkować różnymi decyzjami w zależności od sytuacji. Może on oznaczać kontynuację działania podmiotu według wcześniej ustalonych procedur (np. reagowanie na zjawiska kryzysowe na podstawie ustalonych procedur działania). Może on oznaczać zatrzymanie działania lub nie podejmowanie działania – przez odbiorcę – w przypadku działalności biznesowej, jeżeli w strategii nie przewidziano takiej sytuacji.

Procesy decyzyjne dotyczące postępowania w sytuacjach szczególnych (naruszenie atrybutu integralności oraz brak możliwości powtórzenia transmisji) można symulować z użyciem narzędzi wykorzystywanych w teorii gier. Przyjmując różne warunki występujące w środowisku działania oraz powiązane z nimi warianty decyzyjne można oszacować możliwe straty lub korzyści. To zaś umożliwia przygotowanie procedur działania w zależności od zdarzeń występujących w systemie informacyjnym. Metodą, która umożliwia

[12] Jest to istotne w przypadku systemów radiokomunikacyjnych wykorzystywanych w zarządzaniu kryzysowym. Systemy te pozwalają na uniezależnienie się od infrastruktury operatorów komercyjnych, która może być zniszczona w wyniku oddziaływania czynnika kryzysowego np. powodzi lub pożaru.

zbadanie funkcjonowania złożonego systemu, jakim jest system informacyjny, jest symulacja komputerowa. Symulacja komputerowa pozwala na generowanie zdarzeń w środowisku działania oraz obserwację skutków działania elementów decyzyjnych i wykonawczych.



Rysunek 3. Przykład procesu postępowania z wiadomością otrzymaną od nadawcy.

5. Podsumowanie

System decyzyjny pełni ważną funkcję wewnątrz organizacji sterując jej działaniem. Informacja odpowiedzialna jest za funkcje sterujące wewnątrz organizacji. Zatem bezpieczeństwo informacji przekazywanej w podsystemie teleinformatycznym organizacji jest kluczowe dla efektywnego działania organizacji. Wymiana dużej liczby informacji pomiędzy różnymi lokalizacjami przestrzennymi powoduje, że próba ręcznego weryfikowania niezmienionej wartości atrybutu integralności jest czasochłonna. Brak zaufania do treści odebranego komunikatu może skutkować niewykonaniem ważnych zadań w kluczowych procesach organizacji. Przedstawiona metoda oceny zmian atrybutu integralności zasobu informacyjnego pozwala na stwierdzenie czy zawartość zasobu informacyjnego została zmieniona. Obliczenie wartości funkcji skrótu nie wymaga długiego czasu, co przedstawiono w tabeli 2. Również zdolność do identyfikowania niewielkich zmian w zawartości pliku jest zachowana (tab. 3 i tab. 4).

Wiedząc, że zawartość pliku uległa zmianie można sprawdzić, jak istotna[13] była modyfikacja. Znając istotność zmiany możliwa jest ocena naruszenia atrybutu poufności zasobu informacyjnego a następnie należy użyć procedur postępowania z informacją (plikiem), którego atrybut poufności został naruszony.

Bibliografia

1. Casad, J. (2018). *TCP/IP w 24 godziny*. Gliwice: Helion.
2. Haykin, S. (1993). *Communication systems*. New York: John Wiley & Sons Inc.
3. Hosmer, H.H. (1993). *Security is fuzzy! Applying the fuzzy logic paradigm to the multipolicy paradigm,* NSPW.
4. Jak działa ZeuS? (01.05.2018). Available online: https://niebezpiecznik.pl/post/jak-dziala-zeus/
5. Kaczmarek, S. (01.05.2018). *Integralność danych imperatyw kategoryczny bezpieczeństwa IT*. Retrived from: http://it-filolog.pl/integralnosc-danych-czyli-imperatyw-kategoryczny-bezpieczenstwa-it/
6. Lammle, T. (2007). *Cisco Certified Network Associate. Study Guide*. Indianapolis: Wiley Publishing.
7. Liderman, K. (2008). *Analiza ryzyka i ochrona informacji w systemach komputerowych*. Warszawa: Wydawnictwo Naukowe PWN.
8. Liderman, K. (2012). *Bezpieczeństwo informacyjne*. Warszawa: Wydawnictwo Naukowe PWN.
9. Polska Norma PN-ISO/IEC 27000 (2014). *Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji*. Przegląd i terminologia. Warszawa: Polski Komitet Normalizacyjny.
10. Szleszyński, A. (2015). Zarządzanie poufnością zasobów informacyjnych w systemach teleinformatycznych. *Zeszyty Naukowe Organizacja i Zarządzanie.* Gliwice: Wydawnictwo Politechniki Śląskiej, z. 86, s. 537-548.
11. Turner, S., Chen, L. (2011). *Internet Engineering Task Force* (IETF). Request for Comments: 6151, Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms, Retrived from https://tools.ietf.org/pdf/rfc6151.pdf.

[13] Przez istotność zmiany należy rozumieć maksymalizację oczekiwanych, przez atakującego, korzyści wynikających z wprowadzonej zmiany lub zmian.