Marek R. OGIELA, Urszula OGIELA
AKADEMIA GÓRNICZO-HUTNICZA W KRAKOWIE
Al. Mickiewicza 30, 30-059 Kraków

Lingwistyczne schematy progowe w inteligentnym zarządzaniu sekretnymi danymi

Prof. dr hab. Marek R. OGIELA

Jest profesorem zwyczajnym na Akademii Górniczo – Hutniczej w Krakowie. Prowadzi badania nad kognitywnymi systemami informacyjnymi nowej generacji, a także kryptografią i podziałem sekretów. Jest członkiem wielu renomowanych towarzystw naukowych, a także autorem ponad 190 publikacji o zasięgu międzynarodowym.

e-mail: mogiela@agh.edu.pl

Mgr inż. Urszula OGIELA

Pracownik AGH w Krakowie, autorka kilkunastu prac o zasięgu międzynarodowym z zakresu zarządzania informacją, ekonomii oraz inteligentnego podziału strategicznych informacji w przedsiębiorstwach.

e-mail: ogiela@agh.edu.pl

Streszczenie

W niniejszej pracy zostanie zaprezentowane nowe podejście do tworzenia schematów progowych współdzielenia informacji, wykorzystujące techniki lingwistyki matematycznej. Schematy takie zostały zaproponowane przez autorów do realizacji bezpiecznych protokołów podziału sekretnych danych w różnych strukturach zarządzania informacją, a w szczególności hierarchicznych. Zaproponowane techniki bazujące na językach formalnych definiują nową klasę algorytmów określonych mianem lingwistycznych schematów progowych.

Słowa kluczowe: Podział sekretu, schematy progowe, zarządzanie informacją, lingwistyka matematyczna.

Linguistic threshold schemes in intelligent secret data management

Abstract

Secure information splitting is used in many tasks of the intelligent sharing of secrets and key data in business organisations. The significance of information splitting depends on its nature, while the significance of information sharing may depend on its importance and the meaning it has for the organisation or institution concerned. This paper presents models for multi-level information splitting and information management with use of the linguistic approach and formal grammars. Such methods constitute a secure enhancement of traditional secret splitting algorithms and introduce an additional stage at which information is coded using the appropriately defined regular or context-free grammar. The many possible applications of such methods include their use for the intelligent management of important or confidential information in government institutions or businesses. Algorithms of multi-level information splitting allow information which is not available to all employees of a given organisation or its environment to be securely split or shared.

Keywords: secret sharing, threshold schemes, information management, mathematical linguistic.

1. Wstęp

Jednym z najszybciej rozwijających się zagadnień związanych z wprowadzaniem nowoczesnych technologii informatycznych do zadań inteligentnego zarządzania informacją w instytucjach rządowych czy organizacjach gospodarczych są zagadnienia związane z pozyskiwaniem, przepływem, kontrolą i analizą zagrożeń poufności oraz integralności takich danych. Prowadzone w tym zakresie badania naukowe mają charakter interdyscyplinarny, a duży stopień upowszechnienia się tej problematyki pozwolił wręcz wyodrębnić nowy nurt badań określany mianem bezpieczeństwa informacji (*Information security*). W nurt badań naukowych związanych z takimi zagadnieniami zaczęło wpisywać się nowe zagadnienie związane z możliwościami inteligentnego podziału ważnych danych strategicznych oraz technik zarządzania nimi w różnych strukturach przepływu danych. Problematyka utajniania i ochrony informacji czerpie swoje korzenie z zagadnień kryptograficznych opartych przede wszystkim na algorytmach zapewniania poufności danych oraz technikach podziału informacji, a także na zagadnieniach związanych z metodami ich odtwarzania.

W niniejszej pracy zostanie podjęta także próba pokazania w jaki sposób schematy takie mogą zostać zaaplikowane do tworzenia nowych modeli zarządzania informacjami współdzielonymi np. w różnych strukturach organizacyjnych. Szczególny nacisk zostanie także położony na algorytmy podziału wielopoziomowego. Podział taki charakteryzuje się tym, iż możliwe jest odtworzenie informacji ze zbiorów zawierających różne liczby składowych dzielonego sekretu. Tematyka taka nie została jeszcze w pełni rozwinięta w prowadzonych badaniach naukowych i wydaje się niezwykle istotna z punktu widzenia przyszłościowego rozwoju nowoczesnych systemów utajniania lub zarządzania informacją.

Propozycja nowych rozwiązań opartych na zaproponowanych przez autorów lingwistycznych schematach progowych pozwoli odejść od czysto matematycznych modeli podziału informacji lub ich wykorzystania wyłącznie w dedykowanych, specjalistycznych zadaniach kryptograficznego współdzielenia informacji, na rzecz szerszego wykorzystania takich technik do zadań zarządzania informacją przeznaczoną dla szerszych grup użytkowników. Informacje takie mogą praktycznie być wykorzystywane w dowolnych organizacjach gospodarczych lub instytucjach państwowych, a ich znaczenie może być wykorzystywane tylko w przypadku uprawnionego dostępu przez wyznaczone grupy osób uczestniczących w podziale sekretu. Dlatego też zostanie podjęta próba zdefiniowania modelowej struktury przepływu oraz przydzielania składowych informacyjnych dla poszczególnych grup zainteresowanych osób (niezależnie od ich liczebności). Zaproponowany model mógłby zostać następnie wdrożony do praktycznych zastosowań w dowolnej organizacji gospodarczej lub w instytucji w oparciu o istniejące tam systemy informacyjne.

2. Rodzaje technik podziału i współdzielenia informacji

Algorytmy inteligentnego podziału lub współdzielenia tajemnicy stanowią stosunkowo młodą, aczkolwiek coraz istotniejszą w dzisiejszym świecie dziedzinę informatyki i zarządzania wiedzą [7]. Pojawia się w nich problem podziału ważnych informacji w sposób umożliwiający odtworzenie oryginalnej wiadomości pewnej grupie n uprawnionych osób (uczestników protokołu podziału sekretu), współdziałającej w celu rozszyfrowania sekretu. Jednocześnie, żadne ze zgrupowań uczestników o liczności mniejszej niż n nie powinno być w stanie odszyfrować (odtworzyć) takiej wiadomości.

Algorytmy podziału i współdzielenia informacji umożliwiają podział jej na części zwane udziałami (ang. soares) lub cieniami (ang. shadows), które następnie zostają rozdzielone pomiędzy

uczestników protokołu tak, że złożone udziały pewnych podzbiorów użytkowników są w stanie zrekonstruować oryginalną tajemnicę.

Istnieją dwie grupy algorytmów dzielenia informacji:

- rozdzielanie wiadomości (*secret splitting*),
- współdzielenie wiadomości (*secret sharing*).

W pierwszej wiadomość jest rozdzielana wśród uczestników protokołu i w celu jej rekonstrukcji wszyscy uczestnicy muszą złożyć swoje części. Bardziej uniwersalną metodą dzielenia tajemnicy są jednak techniki współdzielenia, gdzie wiadomość również jest rozdzielana wśród uczestników protokołu, ale do jej odtworzenia wystarczy jedynie pewna, określona przy tworzeniu schematu, liczba udziałów. Obie z wymienionych metod mają zastosowanie w rzeczywistych zadaniach bezpiecznego zarządzania informacjami. Przykładem takiego zastosowania może być podpis elektroniczny, umożliwiający pewnej grupie uprawnionych osób, po złożeniu swoich udziałów na podpisanie dokumentu elektronicznego.

Pierwsza z wymienionych technik tj. *rozdzielanie wiadomości* polega na takim podzieleniu jej na części, które nie mają osobno żadnego znaczenia, natomiast po ich złożeniu w jedną całość otrzymujemy oryginalną wiadomość [9]. W ten sposób można rozdzielić informację pomiędzy n dowolnych osób. Wszyscy razem mogą odtworzyć tajemnicę po złożeniu części informacji, które otrzymali. Z drugiej strony żadna z rozdzielonych części nie pozwala na odtworzenie oryginalnej wiadomości bez połączenia z pozostałymi częściami.

Drugi rodzaj technik tzn. metody *współdzielenia informacji,* są bardziej skomplikowanymi metodami rozdzielania informacji. Algorytmy współdzielenia tajemnicy zwane są często schematami progowymi (*threshold schemes*). Przy użyciu takiego schematu, można pobrać dowolną informację i podzielić ją na n dowolnych części, zwanych cieniami (*shadows*), w ten sposób, że dowolne m ($m < n$) spośród nich, może być użyte do odtworzenia wiadomości. Jest to tzw. schemat (m, n)-progowy. Schemat progowy współdzielenia wiadomości został opracowany niezależnie przez A. Shamira [12] i G. Blakleya [2], był także intensywnie badany przez G. Simmonsa [13].

Jednym z celów niniejszej pracy będzie próba zdefiniowania nowych rodzajów schematu podziału tajemnic tzn. lingwistycznych schematów progowych, których bezpieczeństwo będzie również oparte na wykorzystaniu lingwistycznych formalizmów do tworzenia nowych reprezentacji współdzielonych danych.

3. Hierarchiczny podział i zarządzanie informacją

Podział informacji występuje w organizacjach gospodarczych niezależnie od rodzaju dzielonej informacji, sposobu jej przetwarzania czy też celu w jakim jest ona gromadzona w danej organizacji. Istotność podziału informacji zależeć może od sposobu jej podziału, celu w jakim jest ona dzielona, a także od rodzaju informacji. Istotność współdzielenia informacji może natomiast zależeć od jej ważności oraz znaczenia jakie niesie ona w sobie dla danej organizacji. Jeżeli bowiem informacja jest informacją ważną o dużym znaczeniu dla danej organizacji lub np. dla organizacji zewnętrznych, to celowym jest wówczas podjęcie próby współdzielenia informacji w celu jej ochrony i zabezpieczenia przed ujawnieniem osobom (czy też organizacjom) postronnym. W przypadku określenia rodzaju informacji, która zostanie poddana procesowi podziału lub współdzielenia należy rozważyć jej „charakter" utożsamiany z jej poufnością, istotnością oraz ważnością bowiem tylko informacja ważna stanowi w tym przypadku o sposobie jej podziału oraz o celowości takiego przedsięwzięcia.

W niniejszym rozdziale zostaną przedstawione i scharakteryzowane modele wielopoziomowego podziału informacji oraz zarządzania informacjami zaproponowane na użytek organizacji gospodarczych. Istotność tego rodzaju modeli polegać będzie na właściwym wyborze technik służących do wielopoziomowego podziału i współdzielenia informacji stosownie dobranych do zaproponowanej organizacji gospodarczej. W zależności od rodzaju struktury wskazany zostanie właściwy dobór metod podziału tajemnicy przynależny odpowiedniemu rodzajowi struktury organizacyjnej.

Algorytmy wielopoziomowego podziału informacji opisywane są w zależności od rodzaju zastosowanego podziału. Może to być podział hierarchiczny lub podział warstwowy. Zasadnicza różnica pomiędzy prezentowanymi rodzajami podziałów występuje w odniesieniu do sposobu wprowadzania samego podziału. Jeśli mówimy o podziałach w obrębie jednorodnych, jednolitych grup lub warstw to wówczas mamy do czynienia z podziałem warstwowym, jeśli natomiast podział dokonywany jest niezależnie od jednorodności grupy lub warstwy, a w odniesieniu do kilku grup uszeregowanych w sposób hierarchiczny, to mamy do czynienia z podziałem hierarchicznym.

Podział warstwowy zatem jest podziałem przebiegającym względem danej warstwy, podział hierarchiczny uwzględnia natomiast hierarchiczność (zależność) danej struktury lub większej liczby struktur względem siebie.

Podział informacji może następować zarówno w całej strukturze, w której jest określona jakaś zależność hierarchiczna, lub też w ramach danej grupy, a także w obrębie dowolnej jednorodnej warstwy. Dlatego też w zależności od rodzaju podziału informacji zasadnym jest wskazanie odpowiednio dobranych algorytmów podziału informacji.

Podział informacji pomiędzy uczestników danej grupy, w której każdy posiada jednakowe przywileje jest tożsamy z podziałem warstwowym. Warto zwrócić uwagę na fakt, iż podział warstwowy może dotyczyć następujących rodzajów podziału:

- **Różnych tajemnic dzielonych w różnych warstwach w podobny sposób** – sytuacja taka oznacza jednakowy (w sensie metody) podział tajemnicy niezależny od warstwy, której ta tajemnica dotyczy. Zmianie podlega tylko informacja stanowiąca tajemnicę, która podlega podziałowi w danej warstwie.
- **Tej samej tajemnicy dzielonej w różny sposób w zależności od warstwy** – w tym przypadku jednakowa informacje jest rozdzielana w różny sposób w zależności od warstwy i liczby uczestników protokołu na poszczególnych warstwach.

Podział hierarchiczny charakteryzuje się możliwością przeprowadzenia dowolnego podziału sekretnej informacji w sposób zdeterminowany przez uprawnienia dostępu na poszczególnych poziomach struktury hierarchicznej. W najbardziej ogólnym przypadku może to być podział różnych tajemnic w obrębie różnych warstw.

4. Idea lingwistycznych schematów progowych

W niniejszym rozdziale pracy zaprezentowane zostaną nowe rozwiązania w dziedzinie współdzielenia sekretnych danych oparte na koncepcji lingwistyki matematycznej. Istotą prezentowanego podejścia jest wykorzystanie formalizmów lingwistycznych wywodzących się z teorii języków formalnych.

Zaproponowany algorytm pozwoli na funkcjonalne rozszerzenie klasycznych schematów podziału i współdzielenia informacji, poprzez generację dodatkowej składowej informacyjnej w postaci lingwistycznej. Składowa taka będzie niezbędna do odtworzenia całości tajemnicy. Ogólna metodologia wykorzystania podejścia opartego na językach formalnych do rozszerzenia klasycznych schematów progowych jest następująca:

1. wybór podstawowego schematu podziału sekretów spośród znanych technik podziału informacji,
2. konwersja współdzielonych danych (tekstowych lub obrazowych) do reprezentacji bitowej,
3. zdefiniowanie gramatyki formalnej kodującej bloki bitowe o różnej długości,
4. konwersja lingwistyczna ciągu bitowego do nowej reprezentacji w postaci ciągu numerów produkcji gramatyki,

5. podział nowej reprezentacji sekretu za pomocą wcześniej wybranego schematu progowego,
6. dystrybucja cieni pomiędzy poszczególnymi uczestnikami protokołu,

Takie etapy definiują podstawowe czynności niezbędne do wygenerowania składowych współdzielonych informacji, które mogą zostać przekazane wszystkim uczestnikom całego postępowania przydziału sekretnych części współdzielonych danych.

Warto jednak zwrócić uwagę na fakt, że w zależności od tego, jak będą generowane i przydzielane sekretne składowe oraz informacja o wykorzystanej gramatyce można wyróżnić jeszcze dwa warianty dalszego postępowania . Warianty te są następujące:

1. jeśli reguły gramatyki będą znane tylko instancji generującej i rozdzielającej cienie to wówczas określiliśmy protokół rozjemczy, w którym do odtworzenia tajemnicy musi również zostać włączony zaufany arbiter lub instancja,
2. jeśli natomiast reguły zdefiniowanej gramatyki zostaną ujawnione to w praktyce mamy do czynienia z realizacją czystego schematu progowego, w którym dodatkowym cieniem jest właśnie zbiór reguł wyprowadzających gramatyki.

W dalszej części zostanie zaprezentowana uogólniona gramatyka pozwalająca realizować konwersję bitowej reprezentacji wejściowego sekretu na bloki *n*-bitowe i dalszą ich transformację do nowej reprezentacji w postaci ciągu numerów produkcji zdefiniowanej gramatyki. Gramatyka taka może zostać zdefiniowana w następujący sposób:

$$G_{n\text{-}bit} = (N, T, P, STS)$$

gdzie: N = {SECRET, BB, 1B, 2B, 3B, 4B, 5B, 6B, …, NB} – zbiór symboli nieterminalnych, T = {1b, 2b, 3b, 4b, 5b, 6b, …, nb, λ} – zbiór symboli terminalnych, w którym zostały zdefiniowane możliwe bloki *n*-bitowe, {λ} –symbol pusty, *STS* = SECRET – symbol startowy gramatyki, P – zbiór produkcji zdefiniowany w następujący sposób:

1. SECRET → BB BB
2. BB → 1B | 2B | 3B | 4B | 5B | 6B, … | NB
   {RÓŻNEJ DŁUGOŚCI BLOKI N-BITOWE}
3. BB → λ
4. 1B → 1b {0, 1}
5. 2B → 2b {00, 01, 10, 11}
6. 3B → 3b {000, 001, 010, 011, 100, 101, 110, 111}
7. 4B → …
8. 5B → 5b
9. 6B → …
10. ……
11. NB → nb
12. b → {0, 1}

Tak wprowadzona uogólniona gramatyka pozwala na szybsze i zwięzłe przekodowanie wejściowej reprezentacji tajemnicy, która następnie zostanie podzielona pomiędzy uczestników protokołu. Korzyścią płynącą z grupowania bitów w większe bloki jest to, że w trakcie realizacji dalszych kroków protokołu współdzielenia tajemnicy uzyskujemy krótsze reprezentacje dla dzielonych, a później odtwarzanych danych. Jest to szczególnie widoczne przy realizacji procedur korzystających z nadmiarowych reprezentacji bitowych tzn. przy zapisach i interpretacji wartości jedno lub kilkubitowych za pomocą kodów w reprezentacjach 8 lub 16 bitowych.

5. Wykorzystanie schematów progowych w strukturach hierarchicznych

Procesy podziału i współdzielenia informacji w instytucjach czy organizacjach gospodarczych powinny uwzględniać znaczenie informacji rozumiane jako stopień ważności i istotności danej informacji, jej stopień dostępności a tym samym stopień poufności, rodzaj organizacji, w której dochodzi do procesu utajniania informacji, strukturę organizacji, w obrębie której dokonany zostanie podział danych, a także sposób podziału danych tj. hierarchiczność lub warstwowość.

Metody współdzielenia informacji w organizacjach gospodarczych mogą być różnorodne, a ich rodzaj zależny jest przede wszystkim od sposobu podziału informacji, tj. od wyboru algorytmu podziału i współdzielenia danych. Dla każdego rodzaju organizacji gospodarczej istnieje optymalny algorytm podziału informacji, niemniej jednak można wskazać także i takie sposoby podziału i współdzielenia danych, które są uniwersalne. Tego rodzaju modele zostaną zaprezentowane w dalszej części pracy dla nowoczesnych struktur zarządzania informacją na przykładzie struktur wirtualnych (zespołów wirtualnych) oraz zostanie przedstawiony podział uniwersalny.

5.1. Podział informacji w strukturach wirtualnych

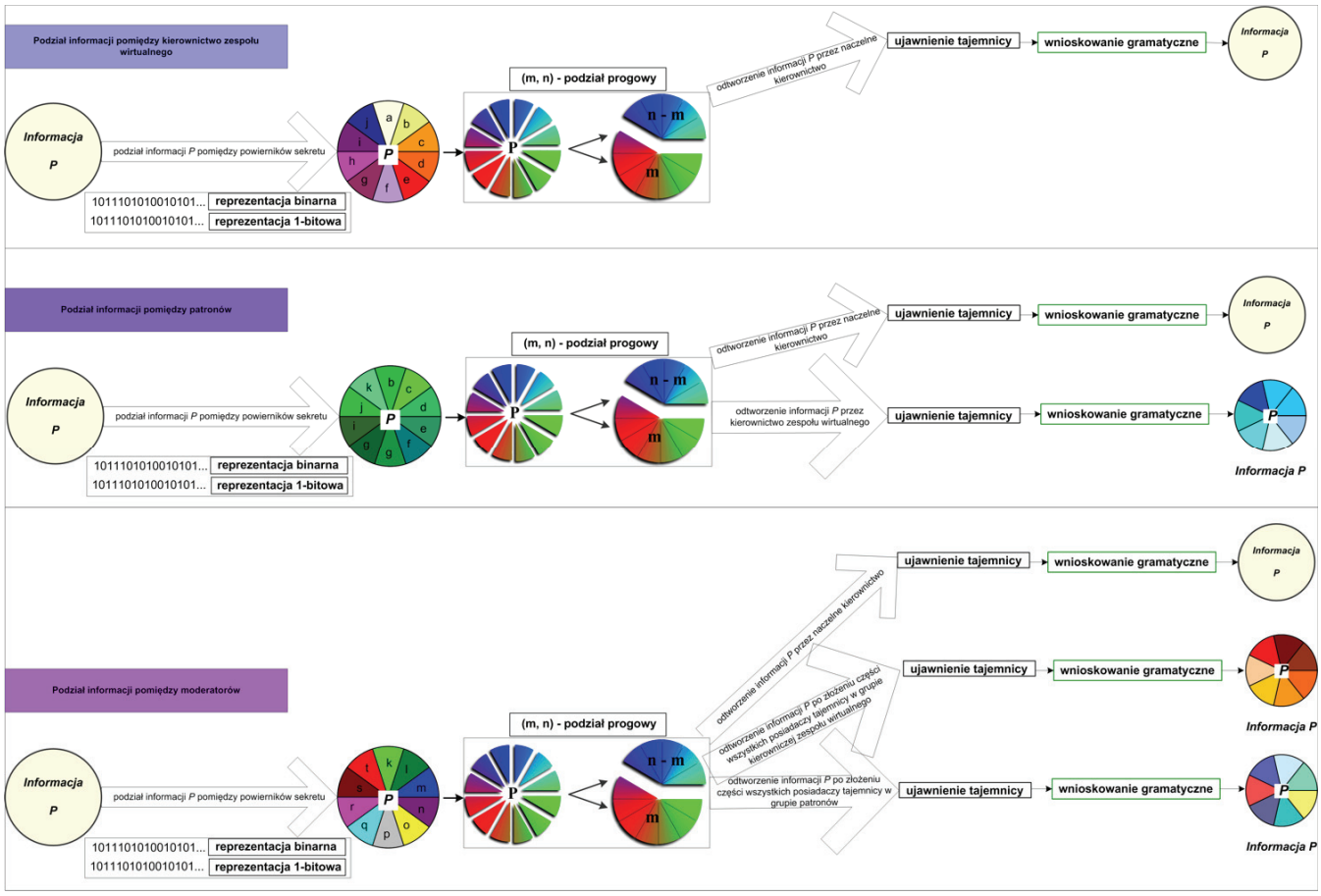
Struktura wirtualna stanowi niezwykle specyficzny i nowoczesny rodzaj struktury z uwagi na to, iż jej zespoły zadaniowe nie zawsze muszą być stałymi elementami danej struktury, niemniej funkcjonuje ona także w oparciu o podział warstwowy i podział hierarchiczny. Podział hierarchiczny odnosi się do zależności pomiędzy zespołami wirtualnymi, patronami, moderatorami oraz kierownictwem organizacji (rys. 1), podział warstwowy natomiast dotyczy przedstawicieli zespołów wirtualnych, patronów, a także moderatorów w danych zespołach.

Zaprezentowany podział informacji w strukturach wirtualnych bazuje na podejściu obrazującym zależności podwładności występujące w tego rodzaju strukturach. Informacja zatem może zostać podzielona na podstawie podziału (*m*, *n*)-progowego pomiędzy:

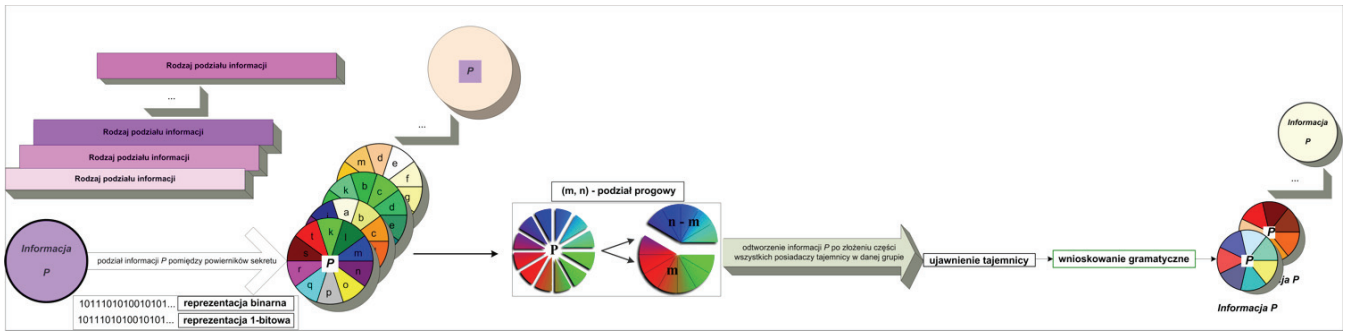
- moderatorami (podział warstwowy),
- patronami (podział warstwowy),
- kierownictwem zespołów wirtualnych (podział warstwowy),
- moderatorami a patronami (podział hierarchiczny),
- moderatorami a kierownictwem zespołów wirtualnych (podział hierarchiczny),
- moderatorami a kierownictwem naczelnym (podział hierarchiczny),
- patronami a kierownictwem zespołów wirtualnych (podział hierarchiczny),
- patronami a kierownictwem naczelnym (podział hierarchiczny),
- kierownictwem zespołów wirtualnych a kierownictwem naczelnym (podział hierarchiczny),
- moderatorami, patronami a kierownictwem zespołów wirtualnych (podział hierarchiczny),
- moderatorami, kierownictwem zespołów wirtualnych a kierownictwem naczelnym (podział hierarchiczny),
- patronami, kierownictwem zespołów wirtualnych a kierownictwem naczelnym (podział hierarchiczny),
- moderatorami, patronami, kierownictwem zespołów wirtualnych i kierownictwem naczelnym (podział hierarchiczny).

5.2. Uniwersalne i specyficzne modele systemów współdzielenia informacji

Modele podziału informacji mogą być tworzone dla struktur organizacyjnych w zależności od rodzaju struktury, ale zaproponowane metody podziału i współdzielenia informacji pozwalają skonstruować modele uniwersalne dla poszczególnych rodzajów grup uczestników podziału informacji. Specyfika prezentowanego w niniejszej pracy podejścia sprawia, że określenie uniwersalności opisywanych metod jest niezwykle zasadne z uwagi na zastosowane w algorytmach podziału informacji formalizmy lingwistycznej analizy danych. Formalizmy te umożliwiają prawidłowy podział informacji bez konieczności każdorazowo wprowadzania nowych rozwiązań zależnych od rodzaju analizowanej struktury organizacyjnej. Uniwersalność metod podziału informacji jest możliwa dzięki zastosowaniu do budowy algorytmów semantycznych modułów wnioskowania (rys. 2).



Rys. 1. Hierarchiczny podział informacji w strukturach wirtualnych
Fig. 1. Hierarchical information splitting in virtual structures



Rys. 2. Uniwersalny podział informacji w strukturach organizacyjnych
Fig. 2. Universal information splitting for organizational structures

Istotą uniwersalności prezentowanej metody jest to, że w zależności od rodzaju struktury instytucji lub organizacji, w obrębie której dokonywany jest podział informacji, wybierane są rodzaje podziału informacji, do których zaliczyć można podział dokonywany pomiędzy:

- stanowiska wykonawcze,
- stanowiska doradcze w tym kierownictwo naczelne,
- stanowiska kierownicze,
- komórki doradcze,
- zespoły kierownicze,
- zespoły zadaniowe,
- zespoły wirtualne,
- patronów,
- moderatorów.

W zależności od wyboru sposobu podziału informacji system dokonuje zdefiniowanych algorytmów podziału w oparciu o zapis reprezentacji bitowej danych podziału zilustrowanego na rysunku 2 jako różnych możliwości podziału na części naszej informacji/danych. Następnie wykonywany jest (m, n)-progowy podział przy użyciu wybranego (ze zbioru zdefiniowanych w systemie) rodzaju podziału, mający na celu wyłączenie cieni, które stanowić będą podstawę odtworzenia informacji. Etap odtworzenia informacji będzie możliwy dzięki złożeniu części posiadaczy tajemnicy w danej grupie, pomiędzy których został podzielony sekret/informacja. Kolejny etap to etap ujawnienia tajemnicy polegający na tym, iż posiadacze jej części mogą dokonać ich połączenia, na podstawie którego po etapie wnioskowania gramatycznego może dojść do złożenia i odtajnienia informacji stanowiącej sekret.

6. Podsumowanie

Metody podziału informacji i techniki ich lingwistycznego współdzielenia stają się obecnie nowymi rozwiązaniami mogącymi mieć swój udział w procesach utajniania informacji/danych niedostępnych dla szerokiego gremium. Dlatego też wszelkiego

rodzaju informacje poufne lub tajne skutecznie mogą zostać zaszyfrowane, podzielone pomiędzy powierników sekretu, i przy udziale właściwych algorytmów i reguł gramatycznych zdefiniowanych podczas procesu definiowania gramatyk formalnych, mogą zostać odtworzone przez powierników sekretu lub przez wybraną ich grupę.

W niniejszej pracy przedstawiona została metodologia wykorzystania technik progowych współdzielenia informacji do wielopoziomowego zarządzania danymi w postaci cyfrowej. Zaprezentowano ogólny model współdzielenia ważnych informacji z wykorzystaniem znanych formalizmów matematycznych wraz z protokołami ich odtwarzania, a także zdefiniowano autorską metodę lingwistycznego współdzielenia informacji, mogącą pełnić użyteczne funkcje w modelach zarządzania współdzielonymi informacjami.

Zaproponowane w niniejszej pracy lingwistyczne schematy progowe posiadają następujące właściwości:

- Pozwalają współdzielić dowolne dane cyfrowe (tekstowych lub obrazowych), dla których istnieje potrzeba inteligentnego podziału pomiędzy uprawnione osoby, a następnie możliwości jej sekretnego odtworzenia,
- Wykorzystują w działaniu klasyczne techniki kryptograficznego podziału informacji tj. schematy (*m*, *n*)-progowe,
- Wprowadzają dodatkowe zabezpieczenia przed nieuprawnionym odtworzeniem informacji i dają możliwość realizacji w dwóch niezależnych wariantach protokołów przydziału utworzonych cieni dla poszczególnych uczestników protokołu – wariant z udziałem zaufanego arbitra jako strony pośredniczącej w przydziale i odtwarzaniu informacji oraz wariant bez arbitra (zaufanej dodatkowej strony) tylko z przydziałem wprowadzonej gramatyki jako dodatkowej części sekretu,
- uzyskiwany poziom zabezpieczeń jest niezależny od długości bloków poddawanych konwersji za pomocą reguł wprowadzonej gramatyki,
- złożoność obliczeniowa zaproponowanych schematów jest złożonością wielomianową.

Wymienione cechy charakterystyczne proponowanych algorytmów lingwistycznego podziału informacji stanowią ich zaletę i pokazują jak uniwersalnymi metodami są zaproponowane metody podziału i współdzielenia sekretnych lub strategicznych informacji.

7. Literatura

[1] Asmuth C., Bloom J.: A Modular Approach to Key Safeguarding, IEEE Transactions on Information Theory, marzec 1983, s. 208–210.

[2] Blakley G.R.: Safeguarding Cryptographic Keys, Proceedings of the National Computer Conference, 1979, s. 313–317.

[3] Blakley G.R.: One-time pads are key safeguarding schemes, not cryptosystems: fast key safeguarding schemes (threshold schemes) exist, in: "Proceedings of the 1980 Symposium on Security and Privacy", IEEE Press, 1980, pp. 108-113.

[4] Chomsky N.: Syntactic Structures, London Mouton, 1957.

[5] ElGamal T.: A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE Transactions on Information Theory, 1985, s. 469–472.

[6] Mackenzie Owen J. (eds.): Information Science and Knowledge Management, Springer-Verlag, Berlin, 2006.

[7] Menezes A., van Oorschot P., Vanstone S.: Handbook of Applied Cryptography, CRC Press, Waterloo, 2001.

[8] Ogiela M.R., Ogiela U.: Security of Linguistic Threshold Schemes in Multimedia Systems, in: Ernesto Damiani, Jechang Jeong, Robert J.Howlett and Lakhmi C. Jain (Eds.), "New Directions in Intelligent Interactive Multimedia Systems and Services – 2", Studies in Computational Intelligence (SCI) vol. 226, pp. 13–20, Springer – Verlag Berlin Heidelberg 2009, pp. 13-20.

[9] Ogiela M.R., Ogiela U.: Secure Information Splitting Using Grammar Schemes, in: Ngoc Thanh Nguyen, Radosław Katarzyniak, Adam Janiak (Eds.), "New Challenges in Computational Collective Intellignence", Studies in Computational Intellignece, vol 244, Springer-Verlag, Berlin-Heidelberg, 2009, pp. 327-336.

[10] Ogiela M.R., Ogiela U.: Shadow Generation Protocol in Linguistic Threshold Schemes, in: Dominik Ślęzak, Tai-hoon Kim, Wai-Chi Fang, Kirk P. Arnett (Eds.) "Security Technology", CCIS – Communication in Computer and Information Science, vol. 58, Springer-Verlag, Berlin, Heidelberg 2009, pp. 35-42.

[11] Seberry J., Pieprzyk J.: Cryptography: An Introduction to Computer Security, Englewood Cliffs, NJ, Prentice-Hall, 1989.

[12] Shamir A.: How to Share a Secret, Communications of the ACM, 1979, s. 612–613.

[13] Simmons G.J.: An Introduction to Shared Secret and/or Shared Control Schemes and Their Application, w Contemporary Cryptology: The Science of Information Integrity, IEEE Press, 1992, s. 441–497.

[14] Tang S.: Simple Secret Sharing and Threshold RSA Signature Schemes, Journal of Information and Computational Science 1, 2004, s. 259–262.

[15] Wang S.J., Tsai Y.R., Chen P.Y.: Proactive (k, n) Threshold Secret Sharing Scheme with variant k and n, Proceedings of the IPC 2007 - The 2007 International Conference on Intelligent Pervasive Computing, October 11th -13th, 2007, Jeju Island, Korea, pp. 117-120, IEEE Computer Society.

otrzymano / received: 06.11.2010
przyjęto do druku / accepted: 02.02.2011 *artykuł recenzowany*

INFORMACJE

Informacja redakcji dotycząca artykułów współautorskich

W miesięczniku PAK od numeru 06/2010 w nagłówkach artykułów współautorskich wskazywany jest autor korespondujący (Corresponding Author), tj. ten z którym redakcja prowadzi wszelkie uzgodnienia na etapie przygotowania artykułu do publikacji. Jego nazwisko jest wyróżnione drukiem pogrubionym. Takie oznaczenie nie odnosi się do faktycznego udziału współautora w opracowaniu artykułu. Ponadto w nagłówku artykułu podawane są adresy korespondencyjne wszystkich współautorów.

Wprowadzona procedura wynika z międzynarodowych standardów wydawniczych.

Redakcja