STUDIA INFORMATICA 2003
Volume 24 Number 2B (54)

Andrzej BIAŁAS
Instytut Systemów Sterowania w Chorzowie

SPOSÓB FORMALNEGO WYRAŻANIA WŁASNOŚCI BEZPIECZEŃSTWA TELEINFORMATYCZNEGO

Streszczenie. Artykuł dotyczy problemu formalizacji zapisu własności bezpieczeństwa, którego rozwiązanie umożliwia tworzenie modeli, na podstawie których można realizować różnego typu aplikacje wspomagające. Przedstawiono ideę wykorzystania w tym celu generyków, spotykanych już wcześniej w niektórych dokumentach formalnych (zadania lub profile zabezpieczeń), opracowywanych przez konstruktorów zabezpieczeń, a wymaganych podczas ich oceny i certyfikacji. Zbiór generyków ujednolicono pod względem gramatycznym, co umożliwiło ich zastosowanie w systemie projektowania i oceny zabezpieczeń. Zdefiniowano zestaw generyków z podziałem na dziedziny zastosowania i etapy modelowania. Wskazano na możliwość ich wykorzystania do automatyzacji procesów zarządzania bezpieczeństwem teleinformatycznym.

Słowa kluczowe: bezpieczeństwo teleinformatyczne, modelowanie własności bezpieczeństwa, projektowanie i ocena zabezpieczeń.

THE MEANS OF FORMAL ICT SECURITY EXPRESSION

Summary. The paper deals with IT Security modelling using generics concept, introduced by some constructors designing their solutions for evaluation according to CC – Common Criteria (ISO 15408). Common set of generics is proposed, classified horizontally by class of applications and vertically by types of security elements or security designing stages. It allows creating IT security design and evaluation supporting software. Using generics concept also in ICT security management support, seems to be quite realistic.

Keywords: ICT security, modelling, design, evaluation.

1. Wprowadzenie

Bezpieczeństwo teleinformatyczne (*ang. Information and Communication Technology (ICT) security*) rozumiane jest jako zespół procesów zmierzających do zdefiniowania, osiągnięcia i utrzymywania założonego poziomu poufności, integralności, dostępności, rozliczalności, autentyczności i niezawodności w systemach teleinformatycznych, wykorzystywanych przez instytucję do realizacji jej zadań statutowych. Jest niezwykle złożonym zagadnieniem, gdyż:

- oprócz technicznych, wymaga także uwzględnienia aspektów organizacyjnych, ekonomicznych, społecznych, psychologicznych, które z natury są trudne do dokładnego opisu, a przez to obniżają spójność technicznej części systemu bezpieczeństwa;
- występuje ogromna liczba trudnych do zidentyfikowania zależności i sprzężeń zwrotnych między elementami systemu bezpieczeństwa;
- instytucja i jej systemy oraz środowisko zagrożeń ulegają ciągłym przemianom, za którymi musi nadążać organizacja systemu bezpieczeństwa, zachowując przy tym założoną dla niego skuteczność w całym cyklu życia.

Zarządzanie złożonym systemem bezpieczeństwa bez komputerowych środków wspomagających staje się coraz trudniejsze, stąd prowadzone są prace nad automatyzacją wybranych jego elementów, takich jak: zarządzanie incydentami, nadzorowanie urządzeń, zarządzanie zasobami, analiza ryzyka, audyt czy generowanie polityk [5-6]. Osiągnięto wiele sukcesów w tych dziedzinach, jednak prace nad systemami kompleksowymi, integrującymi rozwiązania cząstkowe, znajdują się w początkowym stadium rozwoju. Rozwiązania wymagają problemy modelowania, formalnego opisu zjawisk czy tworzenia protokołów.

Wiele w tym względzie zrobiono przy opracowywaniu standardów, zapewniających gwarantowaną miarę bezpieczeństwa[1], w tym zwłaszcza Wspólnych Kryteriów (PN-ISO/IEC 15408) i dokumentów z nimi związanych [1-4].

Artykuł przedstawia jeden z aspektów budowy modeli – formalnego opisu własności bezpieczeństwa teleinformatycznego z wykorzystaniem nazw rodzajowych zwanych generykami[2]. Termin ten można spotkać w wielu zadaniach/profilach zabezpieczeń [8], tworzonych w procesie oceny i certyfikacji zabezpieczeń, jednak twórcy tych dokumentów stosują je dość swobodnie.

W toku prac nad komputerowym systemem wspomagania projektowania i oceny zabezpieczeń [9] zauważono, że można je stosować jako stały element systemu

[1] Druga grupa standardów, typu „*best practices*"; niczego one nie gwarantują, lecz wskazują na wzorcowe sposoby postępowania.

[2] Od ang. „*generics*" – brak do tej pory odpowiednika w polskiej terminologii.

wspomagającego, pod warunkiem udoskonalenia ich opisu, głównie pod względem spójności, wprowadzenia parametryzacji i opracowania ich klasyfikacji. Na potrzeby niniejszego artykułu przyjmijmy następującą definicję tego pojęcia.

Definicja 1:

Generyk – mnemoniczna nazwa rodzajowa, określająca zbiór wspólnych cech, zachowań lub działań, odnoszących się do różnych elementów systemu bezpieczeństwa, takich jak otoczenie zabezpieczeń, zagrożenie, zasób, podmiot, polityka dostępu, podatność, cel zabezpieczeń, funkcja zabezpieczająca, incydent czy następstwo.

Generyki tworzą pewien zbiór - zestaw nazw, dostępnych dla konstruktorów zabezpieczeń, pozwalających bardziej precyzyjnie i zwięźle formułować własności bezpieczeństwa teleinformatycznego. Ma on charakter otwarty.

2. Potrzeby uściślenia zapisu własności bezpieczeństwa

Proces projektowania zabezpieczeń teleinformatycznych [8], [12] sprowadza się do stopniowego uszczegóławiania opisu (konkretyzacji) - od sformułowań opisowych po stosowanie komponentów - podczas przechodzenia przez kolejne etapy projektowania, takie jak: otoczenie zabezpieczeń, cele zabezpieczeń, wymagania na funkcjonalność i uzasadnienie zaufania oraz określenie funkcji zabezpieczających. Przejście do kolejnego etapu wymaga zawsze procesu dowodowego, który dzięki zastosowaniu generyków staje się efektywniejszy.

Konstruktorzy zabezpieczeń mają do dyspozycji zbiór komponentów funkcjonalnych i uzasadniających zaufanie, zawarty w [2-3], pozostałe zaś pojęcia muszą przedstawiać opisowo w języku naturalnym. Podczas analiz i uzasadnień sformułowania te jako dość rozwlekłe i małoprecyzyjne, a poza tym wielokrotnie powtarzane, nastręczały wielu trudności interpretacyjnych. To z tych potrzeb zrodził się pomysł zwięzłego formułowania pewnych stwierdzeń lub własności dotyczących bezpieczeństwa i zastępowania ich nazwą rodzajową – w ten sposób powstały generyki. Konstruktorzy zaczęli definiować je na potrzeby konstruowanych urządzeń, jednak czynią to z dużą dozą swobody.

Przy budowie systemu wspomagania projektowania zabezpieczeń [9-10] również napotkano na problem zwięzłości zapisu, co w naturalny sposób zrodziło pomysł adaptacji idei generyków do budowy tego systemu. Wymagało to jednak uporządkowania i rewizji wielu pojęć oraz wprowadzenia jednolitej syntaktyki z możliwością parametryzacji generyków (choćby poprzez analogię do komponentów). Powstał w ten sposób jednolity, odpowiednio sklasyfikowany zbiór generyków, stanowiący podstawę tworzenia bibliotek na potrzeby systemu.

3. Przykłady generyków opisujących elementy systemu bezpieczeństwa

Problem projektowania zabezpieczeń sprowadza się do zapewnienia bezpieczeństwa przedmiotowi oceny (*ang. TOE - Target of Evaluation*) w jego środowisku eksploatacyjnym [8], [12]. Prezentowany poniżej zbiór generyków opracowany został w związku z realizacją systemu wspomagania tego procesu projektowania, jak również i procesu oceny zabezpieczeń [9-10]. Zbiór ten ma charakter „otwarty", to znaczy użytkownicy mogą go stale rozszerzać wedle swoich potrzeb, przez analogię do zbioru komponentów [2-3].

Zauważmy, że przedstawiane dalej przykłady generyków zawierają nazwę klasy zastosowań, np. kryptografia, systemy zaporowe, karty elektroniczne, ogólne, choć na tym etapie prac nad systemem wspomagania projektowania i oceny podział ten nie jest jeszcze do końca doprecyzowany. Poniżej przedstawiony zostanie format ogólny generyków i ich wybrane przykłady. W systemie wspomagania dany generyk reprezentowany jest przez co najmniej jedną swoją instancję, z którą związanych jest wiele dodatkowych informacji o charakterze zarządczym.

3.1. Zasoby

Zasoby przedmiotu oceny (TOE) lub jego otoczenia teleinformatycznego, które wymagają ochrony, w tym **dane** (*ang. data objects*) zostaną przedstawione za pomocą rodziny generyków typu **D**, posiadających format: ***D.klasa_zastosowań.rodzaj***, których przykłady przedstawia tabela 1.

Zauważmy, że ***D*** oznacza zasób, zaś jako ***klasa_zastosowań*** wystąpić może np. łańcuch znaków „ECARD", odwołujący się do kart elektronicznych, a ***rodzaj*** przedstawia różne możliwe formy tych zasobów. Własności bezpieczeństwa dotyczące kart procesorowych można więc opisać za pomocą krótkich nazw mnemonicznych. Pozwala to na bardziej zwięzłe wyrażenie różnych relacji zachodzących między elementami modelu bezpieczeństwa, wymienionymi w definicji 1.

Tabela 1 odnosi się do zasobu [7], a więc tylko do jednego z elementów systemu bezpieczeństwa. W kolejnych tabelach zaprezentowano przykłady generyków dotyczących innych elementów systemu bezpieczeństwa.

Zauważmy, że zawsze w generykach występuje „*klasa_zastosowań*", która pozwala na umowną poziomą klasyfikację generyków, przy czym klasyfikacja pionowa dotyczy elementów systemu bezpieczeństwa. Bardziej szczegółowo zagadnienie to przedstawione zostanie w punkcie 4.

Tabela 1

Przykłady generyków opisujących zasoby

Mnemonika	Znaczenie
Klasa zastosowań ENCRYPT (aplikacje kryptograficzne)	
D.ENCRYPT.CERT_STORE	Systemowe magazyny certyfikatów.
D.ENCRYPT.CRYPTO_API	Biblioteka systemowa realizująca operacje kryptograficzne.
D.ENCRYPT.PRIV_KEY	Klucz prywatny do tworzenia podpisu cyfrowego lub odszyfrowywania informacji poufnych.
Klasa zastosowań ECARD (karty procesorowe)	
D.ECARD.RANDOM	Liczba losowa na wyjściu generatora elektronicznej karty procesorowej.
D.ECARD.PLAIN_TEXT	Tekst jawny w dedykowanym rejestrze karty procesorowej.
D.ECARD.CIPHER_EXT	Szyfrogram w dedykowanym rejestrze karty procesorowej.

3.2. Podmioty systemu bezpieczeństwa

Do zasobów dostęp usiłują uzyskać dwa rodzaje **podmiotów** (*ang. subjects*):

- **legalne**, jak uprawnieni użytkownicy, administratorzy czy oprogramowanie,
- **nielegalne**, czyli agenci zagrożeń zwani potocznie intruzami.

Podmiot to kolejny element systemu bezpieczeństwa, możliwy do przedstawienia za pomocą generyków. Format rodziny generyków typu S jest podobny: ***S.klasa_zastosowań.rodzaj***, których przykłady przedstawia tabela 2.

Tabela 2

Przykłady generyków opisujących podmioty

Mnemonika	Znaczenie
Klasa zastosowań ENCRYPT (aplikacje kryptograficzne)	
S.ENCRYPT.USER	Użytkownik systemu operacyjnego i aplikacji kryptograficznej.
S.ENCRYPT.ADMIN	Administrator systemu operacyjnego, który ma prawo do zainstalowania i skonfigurowania aplikacji kryptograficznej i nadania uprawnień dla S. ENCRYPT.USER.
S.ENCRYPT.ATTACKER	Potencjalny napastnik, posiadający wysoki poziom umiejętności, wystarczające środki i głęboką motywację do przeprowadzenia ataku.
Klasa zastosowań ECARD (karty procesorowe)	
S.ECARD.OFF-CARD	Intruz działający poza kartą procesorową.
S.ECARD.ON-CARD	Aplikacja działająca w systemie operacyjnym karty procesorowej.

Zauważmy, że generyki typu D oraz S opisują własności pewnych obiektów, występujących w systemie bezpieczeństwa.

3.3. Założenia

Założenia dotyczące otoczenia zabezpieczeń (*ang. assumption*) precyzują warunki, które powinny być spełnione, aby przedmiot oceny mógł być uznany w nim za bezpieczny.

Metodyka projektowania zabezpieczeń narzuca rozróżnianie sześciu grup AX .. AA założeń o podobnym formacie, których przykłady pokazano w tabeli 3:

AX.klasa_zastosowań.rodzaj - dotyczą realności zagrożeń,
AU.klasa_zastosowań.rodzaj - dotyczą zamierzonego sposobu wykorzystania TOE,
AE.klasa_zastosowań.rodzaj - są realizowane przez środowisko zabezpieczeń,
AC.klasa_zastosowań.rodzaj - dotyczą aspektów połączeniowych,
AP.klasa_zastosowań.rodzaj - dotyczą personelu,
AA.klasa_zastosowań.rodzaj - dotyczą stopnia wymaganego rygoryzmu.

Generyki otoczenia zabezpieczeń wyrażają uwarunkowania lub pewne wzorcowe zachowania.

W tabeli 3 pojawił się pierwszy przykład generyka z parametrem. Zauważmy, że parametryzacja ta wpływa na poprawę zwięzłości opisu i redukcję potrzebnej liczby generyków. Pozwala lepiej wyrazić relacje między zasobami (D), podmiotami (S) oraz własnościami i zachowaniami, opisywanymi przez pozostałe generyki.

Tabela 3

Przykłady generyków założeń

Mnemonika	Znaczenie
Klasa zastosowań ENCRYPT (aplikacje kryptograficzne)	
AE.ENCRYPT.CAPI	Zakłada się, że legalny *[S_parameter]*[3] podczas pracy korzysta z zaufanej biblioteki funkcji kryptograficznych.
AU.ENCRYPT.CGA	Zakłada się istnienie zaufanej aplikacji generującej certyfikaty. Aplikacja ta chroni autentyczności podpisu i danych weryfikujących certyfikatu przez poświadczenie podpisem Centrum Certyfikacji.
Klasa zastosowań GENERAL (ogólna)	
AE.GENERAL.LOCATE	Zakłada się, że przetwarzane zasoby TOE są umieszczone w strefie o kontrolowanym dostępie fizycznym (np. komputer o autoryzowanym dostępie, znajdujący się w chronionym pomieszczeniu).
AC.GENERAL.BY_FIREWALL	Zakłada się, że jedynie możliwym połączeniem sieci wewnętrznej z siecią zewnętrzną jest połączenie przez system zaporowy.

3.4. Zagrożenia

Zagrożenia (*ang. threats*) można przedstawić za pomocą rodziny generyków typu **T**, posiadających format: ***T.klasa_zastosowań.rodzaj***, których przykłady przedstawia tabela 4.

Generyki zagrożeń wyrażają scenariusze zagrożeń, przedstawiając ogólnie, w jaki sposób czynnik wywołujący zagrożenie, czyli tak zwany agent zagrożenia, doprowadza do incydentu i związanych z nim następstw, czyli w jaki sposób wykorzystuje on podatność zasobu i uzyskuje przewagę nad zabezpieczeniami.

---

[3] ***S_parameter*** oznacza parametr, w miejsce którego można podstawić podmiot, np.: S.ENCRYPT.USER, co oznacza, że AE.ENCRYPT.CAPI należy do generyków sparametryzowanych.

Tabela 4

Przykłady generyków opisujących zagrożenia

Mnemonika	Znaczenie
Klasa zastosowań ENCRYPT (aplikacje kryptograficzne)	
T.ENCRYPT.CERTVAL	Certyfikat utracił ważność, został umieszczony na liście certyfikatów odwołanych (CRL), a użytkownik nie uaktualnił CRL.
T.ENCRYPT.ENC	Nielegalny [*S_parameter*] może zdobyć dane użytkownika [*D_parameter*] lub wyznaczyć klucz potrzebny do wyznaczenia [*D_parameter*] z szyfrogramu.
Klasa zastosowań ECARD (karty procesorowe)	
T.ECARD.DPA	Nielegalny [*S_parameter*] może zdobyć klucz [*D_parameter*], analizując pobór energii układu scalonego podczas operacji kryptograficznych (*ang. Differential Power Analysis*), do tego wymagane są specjalistyczna wiedza, odpowiednia metoda i zasoby; jednak bez potrzeby zgłębiania TOE; atak pasywny.
Klasa zastosowań GENERAL (ogólna)	
T.GENERAL.ACCESS	Autoryzowany użytkownik TOE [*S_parameter*] może uzyskać dostęp do zasobu bez zgody jego właściciela lub osoby odpowiedzialnej.
T.GENERAL.COVERT	Autoryzowany użytkownik TOE [*S_parameter*] może rozmyślnie lub przypadkowo przesłać za pośrednictwem ukrytego kanału informacje wrażliwe do użytkowników nieuprawnionych.
T.GENERAL.DENY	Autoryzowany użytkownik TOE [*S_parameter*] jako autor lub odbiorca może uczestniczyć w wymianie informacji, a potem temu zaprzeczyć.

3.5. Polityki bezpieczeństwa

Polityki bezpieczeństwa (*ang. security policies*), ustalające reguły użytkowania TOE wraz z procedurami wspomagającymi, można przedstawić za pomocą rodziny generyków typu **P**, posiadających format: ***P.klasa_zastosowań.rodzaj***, których przykłady znajdują się w tabeli 5.

Tabela 5

Przykłady generyków opisujących polityki

Mnemonika	Znaczenie
Klasa zastosowań ACCESS (dostęp do informacji)	
P.ACCESS.DAC	Prawo dostępu do wybranych obiektów danych [*D_parameter*] wyznaczone jest na podstawie: - prawa własności obiektu, - identyfikacji podmiotu usiłującego uzyskać dostęp do zasobu, - pośrednio bądź bezpośrednio sformułowanych praw dostępu do zasobu przyznanych podmiotowi przez właściciela zasobu.
P.ACCESS.MAC	Prawo dostępu do informacji oznaczonej klauzulą wrażliwości [*D_parameter*] wyznaczone zostaje w następujący sposób: - wgląd do informacji mają tylko podmioty uprawnione, - podmiot nie może obniżyć klauzuli wrażliwości informacji, o ile nie uzyska na to wyraźnej zgody.
Klasa zastosowań GENERAL (ogólna)	
P.GENERAL.ADMIN	Osoby odpowiedzialne za administrowanie systemem (S.ADMIN) zapewnią kontrolę dostępu do systemu operacyjnego (otoczenie TOE).

P.GENERAL.ENVCTRL	Osoby odpowiedzialne za stabilną pracę TOE oraz jego otoczenia zapewnią przegląd stanu technicznego urządzeń wchodzących w skład otoczenia TOE (komputer, UPS itp.), jak również kontrolę zainstalowanego oprogramowania.

Zauważmy, że ta grupa generyków odnosi się do tak zwanej polityki dostępu, wprowadzając relacje między podmiotami a zasobami, definiując zasady autoryzowanego dostępu. Zasady te można przedstawić w sposób bardzo sformalizowany.

3.6. Cele bezpieczeństwa

Cele zabezpieczeń (*ang. objectives*) odnoszą się do koniecznych do zastosowania zabezpieczeń. Metodyka projektowania zabezpieczeń narzuca rozróżnianie czterech ich grup: **OP ..OE** o podobnym formacie, których przykłady pokazano w tabeli 6:

OP.klasa_zastosowań.rodzaj - dotyczą zabezpieczeń prewencyjnych w TOE,
OD.klasa_zastosowań.rodzaj - dotyczą zabezpieczeń detekcyjnych w TOE,
OC.klasa_zastosowań.rodzaj - dotyczą zabezpieczeń korygujących w TOE,
OE.klasa_zastosowań.rodzaj - dotyczą zabezpieczeń umieszczonych w otoczeniu. TOE.

Tabela 6

Przykłady generyków opisujących cele bezpieczeństwa

Mnemonika	Znaczenie
Klasa zastosowań ENCRYPT (aplikacje kryptograficzne)	
OD.ENCRYPT.CERTVAL	TOE zapewni środki kontroli ważności używanych certyfikatów (aktualizacja list CRL).
OP.ENCRYPT.CONFID	TOE zapewni środki do ochrony poufności informacji.
OD.ENCRYPT.INTEGRITY_DATA	TOE zapewni środki do wykrywania utraty integralności informacji.
Klasa zastosowań ECARD (karty procesorowe)	
OP.ECARD.DPA	TOE zapewni poufność klucza [**D_parameter**] podczas operacji kryptograficznych.
OE.ECARD.TAMPER	Otoczenie układu elektronicznego chroni przed bezpośrednią manipulacją – uniemożliwia to ujawnianie danych użytkownika lub kluczy oraz manipulowanie generatorem losowym.
Klasa zastosowań GENERAL (ogólna)	
OP.GENERAL.ANON	TOE zapewni środki umożliwiające podmiotowi korzystanie z zasobów lub usług bez ujawniania jego tożsamości innym podmiotom.
OD.GENERAL.ENTRY	TOE będzie miał możliwość ograniczania dostępu użytkownika do TOE w zależności od czasu i lokalizacji urządzenia.
OP.GENERAL.I&A	TOE będzie w sposób jednoznaczny identyfikował wszystkich użytkowników, a przed przyznaniem użytkownikowi dostępu do TOE będzie sprawdzana jego tożsamość.

3.7. Wymagania na zabezpieczenie otoczenia

Ze względu na fakt, że wymagania dotyczące otoczenia zabezpieczeń (*ang. requirements for the environment*) nie zostały określone w [2] w postaci komponentów, również i one

muszą być wyrażone w postaci generyków. Format generyków typu **RE** (przykłady w tabeli 7) jest następujący: ***RE.klasa_zastosowań.rodzaj.***

Tabela 7

Przykłady generyków opisujących wymagania dotyczące otoczenia zabezpieczeń

Mnemonika	Znaczenie
Klasa zastosowań ECARD (karty procesorowe)	
RE.ECARD.KEY_CALCULATION	Twórca aplikacji działającej na procesorze karty musi zadbać o właściwą implementację operacji kryptograficznych typu Y = F(k,x), k=const, x=var; TOE kontroluje pobór mocy (DPA), wykonując operacje kryptograficzne, z kolei aplikacja zadbać powinna o to samodzielnie.
RE.ECARD.TAMPER_RESIST	Otoczenie TOE (i karty plastykowej) powinno gwarantować integralność fizyczną TOE i wymusić jego użytkowanie w dobrze zdefiniowanych warunkach: rozpoznanie prób manipulacji, odporność konstrukcji czytnika na nie, używanie tylko właściwych czytników.
Klasa zastosowań GENERAL (ogólna)	
RE.GENERAL.LOSSDATA	W przypadku awarii otoczenie TOE powinno umożliwić pewną pracę, bez narażenia na utratę danych (lub z zapewnieniem akceptowalnego poziomu strat).

3.8. Funkcje zabezpieczające

Wymagania funkcjonalne, wyrażone za pomocą skatalogowanych komponentów funkcjonalnych, powinny zostać zaimplementowane (sprzętowo lub programowo) w TOE w postaci wyodrębnionych modułów realizujących funkcje zabezpieczeń F (*ang. security functions*). Przyjęto następujący format dla tych funkcji: ***F.klasa_zastosowań.rodzaj.*** Przykłady zamieszczono w tabeli 8.

Tabela 8

Przykłady generyków opisujących funkcje zabezpieczające

Mnemonika	Znaczenie
Klasa zastosowań ENCRYPT (aplikacje kryptograficzne)	
F.ENCRYPT.DEA	Algorytm DEA (=DES)[4] realizowany jest zgodnie z FCS_COP.1 oraz FIPS PUB46[5] przez koprocesor, z wykorzystaniem klucza 56- lub 112-bitowego[6]; działając na 64-bitowych blokach.
F.ENCRYPT.SIGN_BUFFER	Dane, które mają być kontrolowane, zostają podpisane za pomocą zaimplementowanej funkcji *PodpiszBufor*[7].

Generyki typu F reprezentują więc moduły sprzętowe (urządzenia wolno stojące lub działające na magistrali, scalone układy elektroniczne) lub programowe (funkcje, procedury

[4] DEA=Data Encryption Algorithm występuje jako parametr w komponencie FCS_COP.1 – podstawiono tu DEA:=DES.

[5] Standard dotyczący algorytmu DES.

[6] Rodzaj pracy potrójnego DES (ISO8732).

[7] Należy odnieść się do szczegółowego opisu implementacji.

lub ich zbiory zapisane w języku programowania), w których zaimplementowano konkretne funkcje zabezpieczające zgodne z wyspecyfikowanymi algorytmami, a które wykonano zgodnie z paradygmatem opisanym w [2], wyrażającym wzorcowy model funkcji zabezpieczającej.

4. Możliwość rozwinięcia koncepcji generyków

Ustalenie zbioru docelowego generyków jest sprawą otwartą, podobnie jak ich ostateczna klasyfikacja. Na razie rysują się następujące podziały:

- poziomy - według klas zastosowań: aspekty ogólne bezpieczeństwa (GENERAL), karty elektroniczne (ECARD), aplikacje kryptograficzne (ENCRYPT), środki komunikacji (COMM), kontrola dostępu (ACCESS);
- pionowy – według elementów systemu bezpieczeństwa i etapów jego budowy: zasoby (D), podmioty legalne i nielegalne (S), założenia projektowe (AX .. AA), zagrożenia (T), podatności (V), polityki (P), zabezpieczenia wyrażone w postaci celów (OP .. OE), wymagania otoczenia (RE) oraz funkcje zabezpieczające (F).

Należy przyjąć, że podziały te są dość ogólne. Zapewne zdefiniowanych zostanie więcej klas zastosowań i dodatkowo wydzielone zostaną z nich podklasy. Również podział pionowy, obecnie raczej związany z projektowaniem i oceną zabezpieczeń, zostanie rozwinięty, zwłaszcza przy próbie przeniesienia idei generyków do budowy systemu zarządzania bezpieczeństwem. Należy liczyć się również z postępującym procesem parametryzacji generyków.

5. Zastosowanie generyków w systemie wspomagania projektowania i oceny zabezpieczeń

Na rys. 1 pokazano przykładowe okienko opracowywanego systemu projektowania i oceny zabezpieczeń teleinformatycznych działającego według Wspólnych Kryteriów. Generyki są podstawą budowy tego systemu. Występują we wszystkich fazach projektowania oraz oceny dokumentów profilu zabezpieczeń lub zadania zabezpieczeń.

W lewej części okna przedstawiono drzewko symbolizujące główne fazy projektowania zabezpieczeń, począwszy od otoczenia zabezpieczeń. Założenia, podmioty, zasoby, zagrożenia, polityki, przedstawiające otoczenie wyrażane są właśnie za pomocą generyków, wybieranych z przygotowanych bibliotek, zawierających już kilkaset elementów. Podobnie pokazano zabezpieczenia (cele): prewencyjne, wykrywające, korygujące oraz dotyczące

otoczenia. Poniżej pokazano klasy komponentów funkcjonalnych. Bez generyków niemożliwy byłby kompleksowy opis całego procesu projektowego.

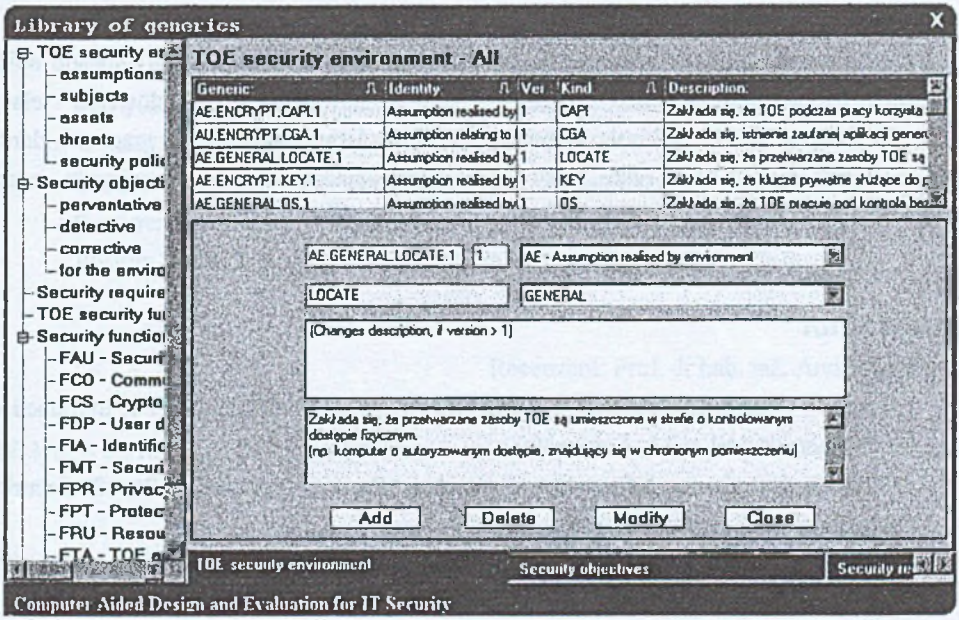
Prawa część okna (rys. 1) przedstawia szczegóły dotyczące generyków założeń otoczenia zabezpieczeń. Ze względu, że system znajduje się jeszcze w fazie rozwojowej i brak jest polskiego tłumaczenia Wspólnych Kryteriów, na rysunku występują dwujęzyczne określenia.

Prace systemem trwają i stanowią poligon doświadczalny przy formułowaniu definicji nowych generyków.

Dzięki wprowadzeniu generyków uzyskano poprawę spójności procesów uzasadniania przejść między etapami projektowania i oceny [9-10]:

- od założeń do celów,
- od celów do poziomu komponentów,
- od komponentów do końcowej specyfikacji funkcji zabezpieczających.

Generyki ułatwiają bowiem tworzenie tabeli lub schematów graficznych, pozwalających formułować osądy na temat spełnienia warunków koniecznych i wystarczających do pokrycia elementów bezpieczeństwa, właściwych dla danego etapu uzasadniania [12].



Rys. 1. Okienko obsługi biblioteki generyków
Fig. 1. Generics library window

Generyki ułatwiają również procesy oceny dokumentów typu zadanie zabezpieczeń lub profil zabezpieczeń, które odbywają się według zasad podanych odpowiednio w klasach ASE i APE Wspólnych Kryteriów [10].

6. Wnioski i uwagi końcowe

Artykuł dotyczy zagadnienia formalizacji opisu własności bezpieczeństwa. Pomysł zastosowania generyków do wypełnienia luki w istniejących sposobach formalizacji opisu (dostępne są tylko komponenty) okazał się bardzo trafny. W znaczący sposób poprawia to spójność sformułowań i wyrażanie relacji zachodzących między elementami systemu bezpieczeństwa, co z kolei ułatwia prowadzenie procesów uzasadniania. Konstruktorzy otrzymują gotowe biblioteki generyków dla różnych obszarów zastosowań i różnych etapów projektowania, co przyspiesza tworzenie i ocenę zabezpieczeń. Opracowanie jednolitego zbioru generyków warunkuje budowę systemu wspomagania projektowania zabezpieczeń. Przyjęty zbiór swą spójnością dorównuje zbiorowi komponentów, choć tej spójności, podobnie jak i one, do końca nie gwarantuje, gdyż dopuszcza się możliwość wprowadzania własnych definicji, jednak przy zastosowaniu ścisłych reguł.

Uważny czytelnik zauważy zapewne analogię między klasami zastosowań generyków a bibliotekami projektowymi systemów wspomagania projektowania układów cyfrowych – w obu przypadkach budowa systemu z gotowych elementów składowych znacznie zwiększa efektywność.

Dotychczasowe analizy wykazują, że generyki stanowią dość uniwersalny sposób opisu własności bezpieczeństwa, stąd mogą też być stosowane do modelowania relacji zachodzących podczas zarządzania systemem bezpieczeństwa, wspieranym przez standardy typu *best practice,* a nie tylko przy ocenie zabezpieczeń, gdzie obowiązuje miara gwarantowana.

LITERATURA

1. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, v.2.1, August 1999.
2. Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, v.2.1, August 1999.
3. Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, v.2.1, August 1999.
4. ISO/IEC PDTR 15446, Information technology – Security techniques – Guide for the production of protection profiles and security targets, v.0.9, January 2000.
5. Project SPARTA: Security Policy Adaptation Reinforced Through Agents - http://www.infosys.tuwien.ac.at/sparta

6. Sipponen M.T.: Policies for Construction of Information Systems' Security Guidelines, Proceedings of 16th IFIP TC11 Annual Working Conference, Beijing, August 2000.
7. Białas A.: Wprowadzenie do modelowania procesów analizy ryzyka w systemach teleinformatycznych. IX Konferencja SIECI KOMPUTEROWE – Zakopane 2002. Studia Informatica vol. 23, Number 2B(49), Silesian University of Technology, Gliwice 2002.
8. Białas A.: Modelowanie i ocena zabezpieczeń teleinformatycznych. IX Konferencja SIECI KOMPUTEROWE – Zakopane 2002, Studia Informatica vol. 23, Number 2B(49), Silesian University of Technology Press, Gliwice 2002.
9. Praca zbiorowa pod red. Białasa A.: Metodyka projektowania zabezpieczeń teleinformatycznych. Projekt KBN: 6.T11.073.2001C/5689 pt. System wspomagania projektowania i oceny zabezpieczeń teleinformatycznych, Instytut Systemów Sterowania, Chorzów 2002.
10. Praca zbiorowa pod red. Białasa A.: Metodyka prowadzenia badań i oceny środków teleinformatycznych. Projekt KBN: 6.T11.073.2001C/5689 pt. System wspomagania projektowania i oceny zabezpieczeń teleinformatycznych, Instytut Systemów Sterowania, Chorzów 2002.
11. Białas A.: Budowa zaufania do zabezpieczeń teleinformatycznych poprzez ich ocenę i certyfikację. Materiały konferencji „Internet w społeczeństwie informacyjnym", Wyższa Szkoła Biznesu, Dąbrowa Górnicza 2003.
12. Białas A.: Projektowanie zabezpieczeń teleinformatycznych. Referaty Międzynarodowej Konferencji „BISK - Bezpieczeństwo informacji w systemach komputerowych", Wyższa Szkoła Informatyki i Zarządzania Biznesu, Bielsko-Biała 2003.

Recenzent: Prof. dr hab. inż. Andrzej Grzywak

Wpłynęło do Redakcji 24 marca 2003 r.

Abstract

The paper deals with IT Security modelling. Generics concept, introduced by some constructors designing their solutions for evaluation according to CC – Common Criteria (ISO 15408) was developed. Set of generics, divided horizontally by application classes and grouped vertically by types or designing stages, corresponding to: assets (table 1), subjects (table 2), environmental assumptions (table 3), threats (table 4), organizational security policies (table 5), security objectives (table 6), environmental requirements (table 7) and

finally, security functions (table 8). On the Fig.1 generics library window is shown. This is one of the IT security design and evaluation application window, build on the presented generics concept.

Adres

Andrzej BIAŁAS: Instytut Systemów Sterowania, ul. Długa 1, 41-506 Chorzów, Polska, abialas@iss.pl .