Bezpieczeństwo w zarządzaniu siecią – SNMP

Patryk Czarnik

Wydział Matematyki, Informatyki i Mechaniki
Uniwersytet Warszawski

Bezpieczeństwo sieci komputerowych – MSUI 2010/11

Simple Network Management Protocol

Cel

- monitorowanie urządzeń i aplikacji
- konfiguracja urządzeń

Status

- standard IETF
- wersja 1 – 1988, RFC: 1065–1067,
  zastąpione przez RFC: 1155, 1213, 1157,
- wersja 2 – 1993, RFC: 1441–1452
  - SNMPv2c (*community-based*), RFC: 1901–1908
  - SNMPv2u (*user-based*), RFC: 1909–1910
- wersja 3 – 2004, RFC: 3411–3418

Idea SNMP

Elementy architektury zarządzania siecią

- stacja zarządzająca (NMS),
- zarządzane urządzenie,
- agent,
- zarządzany obiekt,
- baza informacji (MIB),
- protokół zarządzania siecią.

Modele komunikacji

- NMS $\overset{\rightarrow}{\leftarrow}$ urządzenie
- urządzenie $\rightarrow$ NMS (trap)
- NMS $\rightarrow$ NMS (inform)

Idea SNMP

Elementy architektury zarządzania siecią

- stacja zarządzająca (NMS),
- zarządzane urządzenie,
- agent,
- zarządzany obiekt,
- baza informacji (MIB),
- protokół zarządzania siecią.

Modele komunikacji

- NMS $\overset{\rightarrow}{\underset{\leftarrow}{}}$ urządzenie
- urządzenie $\rightarrow$ NMS (trap)
- NMS $\rightarrow$ NMS (inform)

Stacja zarządzająca – wymagania

- Zestaw aplikacji służących do analizy informacji, naprawiania błędów itp.
- Interfejs służacy administratorowi do obserwacji i kontroli sieci.
- Możliwość przekładania wymagań administratora sieci na faktyczną możliwość obserwacji i kontroli elementów sieci.
- Baza danych zawierająca informacje z baz informacji administracyjnych (MIB) wszystkich jednostek w administrowanej sieci.

Polecenia SNMP

- **GetRequest** – dla każdego obiektu wymienionego w poleceniu zwróć wartość tego obiektu
- **GetNextRequest** – dla każdego obiektu wymienionego w poleceniu zwróć wartość następnego obiektu (w porządku leksykograficznym danego MIBa)
- **GetBulk (SNMPv2)** – dla każdego obiektu wymienionego w poleceniu zwróć wartość następnych *N* obiektów
- **SetRequest** – dla każdego obiektu wymienionego w poleceniu ustaw wartość na wymienioną w poleceniu
- **Trap** – prześlij informację o zaistniałym zdarzeniu (agent do menedżera)
- **Inform (SNMPv2)** – prześlij informację o zaistniałym zdarzeniu (menedżer do menedżera)
- **GetResponse** – odpowiedz na żądanie menedżera

Elementy bezpieczeństwa w SNMP

- **Kontrola dostępu** – ograniczenie dostępu menedżera do konkretnego fragmentu MIBa oraz określonego zbioru poleceń.
- **Uwierzytelnianie (SNMPv2)** – procedura umożliwiająca stronie odbierającej sprawdzenie, że komunikat pochodzi z danego źródła i ma właściwy czas. Realizuje się ją przez dołączenie do komunikatu dodatkowej informacji.
- **Prywatność (SNMPv2)** – ochrona danych przed odczytaniem przez nieupoważnionych odbiorców. Realizuje się ją przez szyfrowanie danych.
- **(SNMPv3)** – złożony model kontroli dostępu

Społeczności w SNMPv1

- Namiastka uwierzytelnienia w SNMPv1 (i SNMPv2c).
- Identyfikowana napisem unikalnym dla agenta (często dla całej sieci).
- W zamyśle grupa menedżerów mająca określone uprawnienia do określonych obiektów.
- Stacja zarządzająca dołącza do polecenia nazwę społeczności (jawnym tekstem!).
- Agent może obsługiwać wiele społeczności, menedżer może należeć do wielu społeczności.

Polityka ograniczeń dostępu w SNMPv1

Każdej społeczności SNMP odpowiada profil społeczności określający politykę dostępu do obiektów MIB. Profil taki ma dwa aspekty:

- **widok MIB** – to zbiór obiektów MIB do których dostęp ma dana społeczność
- **tryb dostępu** – określa polecenia które możliwe są do wykonania na danym obiekcie. Tryb dostępu w SNMPv1 to jeden z: {*READ-ONLY, READ-WRITE*}

Bezpieczeństwo w SNMPv2

Zagrożenia występujące w SNMPv1, przed którymi chronią środki zapewniania bezpieczeństwa w SNMPv2:

- **ujawanianie** – przeciwnik może śledzić informacje wymieniane przez menedżera i agenta i w ten sposób poznać wartość zarządzanych obiektów oraz uzyskać informacje o wydarzeniach,
- **maskarada** – przeciwnik może starać się podszyć pod członka społeczności w celu wykonania niedozwolonej dla siebie operacji,
- **modyfikacja treści komunikatu** – przeciwnik może zmienić wygenerowany przez członka społeczności komunikat w trakcie przesyłania w taki sposób aby doprowadzić do wykonania niedozwolonej operacji zarządzania,
- **modyfikacja kolejności i czasu komunikatów** – w celu doprowadzenia do wykonania niedozwolonych operacji przeciwnik może zmieniać kolejność, opóźniać lub powtarzać komunikaty.

(Nie)Bezpieczeństwo w SNMPv2

SNMPv2 nie chroni natomiast przed następującymi zagrożeniami:

- **uniemożliwienie działania** – przeciwnik może zablokować wymianę informacji między agentem a menedżerem,
- **analiza ruchu** – przeciwnik może śledzić schemat ruchu pomiędzy menedżerem i agentami.

Strony w SNMPv2

Strona

- Abstrakcja użytkownika/urządzenia i roli w jakiej występuje w danym kontekście.
- Każdy agent/menedżer może posiadać wiele stron.
- Większa elastyczność w nadawaniu uprawnień i kontroli dostępu.

Baza danych jednostki o znanych stronach

- **Strony lokalne** – zbiór stron na których działania wykonuje lokalna jednostka SNMPv2 czyli zbiór ról tej jednostki,
- **Strony reprezentowane** – zbiór stron jednostek reprezentowanych przez daną jednostkę SNMPv2,
- **Strony odległe** – zbiór stron, których działania realizują inne jednostki SNMPv2 z którymi dana jednostka może wchodzić w interakcje.

Strony w SNMPv2

Strona

- Abstrakcja użytkownika/urządzenia i roli w jakiej występuje w danym kontekście.
- Każdy agent/menedżer może posiadać wiele stron.
- Większa elastyczność w nadawaniu uprawnień i kontroli dostępu.

Baza danych jednostki o znanych stronach

- **Strony lokalne** – zbiór stron na których działania wykonuje lokalna jednostka SNMPv2 czyli zbiór ról tej jednostki,
- **Strony reprezentowane** – zbiór stron jednostek reprezentowanych przez daną jednostkę SNMPv2,
- **Strony odległe** – zbiór stron, których działania realizują inne jednostki SNMPv2 z którymi dana jednostka może wchodzić w interakcje.

Pola bazy danych (o stronach)

Dla każdej znanej strony:

- identyfikator,
- domena, adres,
- zegar(!),
- max. czas życia komunikatu,
- uwierzytelnienie:
  - algorytm,
  - publiczne dane uwierzytelniające,
    np. klucz publiczny w algorytmie asymetrycznym,
  - prywatne dane uwierzytelniające,
    np. klucz prywatny w algorytmie asymetrycznym,
- szyfrowanie:
  - algorytm,
  - dane publiczne,
  - dane prywatne (jak wyżej).

Format komunikatu SNMPv2u

Postać ogólna

`version`	INTEGER
`model`	INTEGER
`qoS`	8 bitów
`agentID`	12 oktetów
`agentBoots`	32 bity
`agentTime`	32 bity
`maxSize`	16 bitów
`userLen`	1 oktet
`userName`	1..16 oktetów
`authLen`	1 oktet
`authDigest`	0..255 oktetów
`contextSelector`	0..40 oktetów
`PDU, PDU, ...`	*Protocol Data Unit* – właściwa treść SNMP

Format komunikatu SNMPv2u

Brak zabezpieczeń

`version`	= 2
`model`	= 1
`qoS`	= 00
`agentID`	
`agentBoots`	
`agentTime`	
`maxSize`	
`userLen`	
`userName`	
`authLen`	= 0
`authDigest`	puste
`contextSelector`	
`PDU, PDU, ...`	

Format komunikatu SNMPv2u

Uwierzytelnienie bez szyfrowania

`version`	= 2
`model`	= 1
`qoS`	= 01
`agentID`	
`agentBoots`	
`agentTime`	
`maxSize`	
`userLen`	
`userName`	
`authLen`	> 0
`authDigest`	= hash(wiadomość · klucz)
`contextSelector`	
`PDU, PDU, ...`	

Format komunikatu SNMPv2u

Szyfrowanie i uwierzytelnienie

`version`	= 2
`model`	= 1
`qoS`	= 11
`agentID`	
`agentBoots`	
`agentTime`	
`maxSize`	
`userLen`	
`userName`	
`authLen`	> 0
`authDigest`	= hash(wiadomość · klucz)
`contextSelector`	
`PDU, PDU, ...`	*szyfrowanie* (tylko tu)

Prywatność

- W oryginalnym SNMPv2:
  - szyfrowanie z użyciem algorytmu DES,
  - wymaga aby obie strony dzieliły wspólny klucz szyfrujący.
- Struktura bazy danych umożliwia jednak zastosowanie innych algorytmów szyfrujących (symetrycznych bądź asymetrycznych).

Uwierzytelnianie

1. Sprawdzenie, czy strona znana.
2. Sprawdzenie czy znane nam zegary stron zgadzają się z podanymi we wiadomości z dokładnością do czasu życia pakietu (granularność: 1 sekunda).
3. Weryfikacja podpisu wiadomości.

Kontrola dostępu

Na politykę kontroli dostępu składają się cztery elementy:

- **strona przeznaczenia** – strona SNMP wykonująca operację zarządzania na żądanie strony źródłowej
- **strona źródłowa** – strona SNMP żądająca wykonania operacji na żądanie stron przeznaczenia
- **zasoby** – informacje zarządzania, na których można przeprowadzać żądane operacje zarządzania w postaci lokalnego widoku MIB lub relacji pełnomocnictwa, nazywane także kontekstem
- **przywileje** – operacje dozwolone, zdefiniowane jako dozwolone PDU przynależące do danego kontekstu i do których wykonania w imieniu podmiotu jest uprawniony odbiorca

Kontrola dostępu cd.

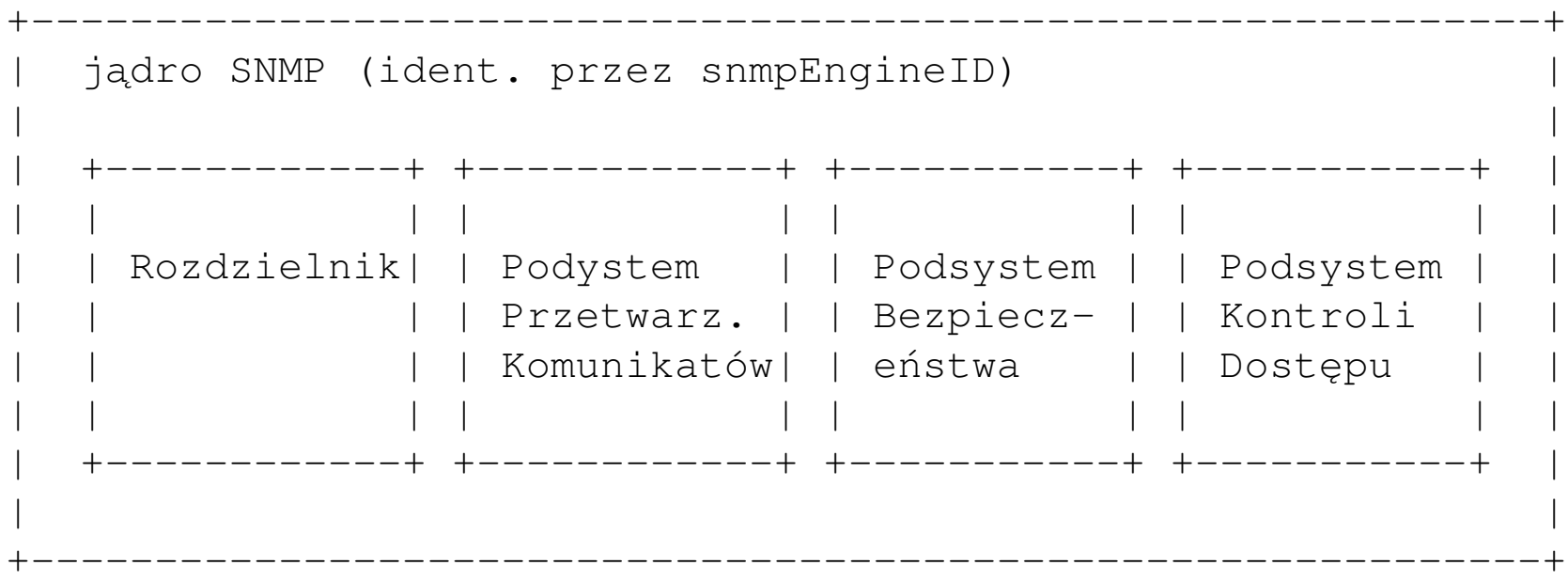
Kontrolę dostępu określają informacje zawarte w MIB stron. Baza ta składa się z czterech tablic:

- **tablicy stron** – zawiera po jednej pozycji na każdą stronę znaną lokalnemu agentowi. Każda pozycja zawiera parametry uwierzytelniania i prywatności. Raz na sekundę lokalny menedżer musi zwiększyć wartość zegara dla każdej pozycji tablicy
- **tablica kontekstów** – może zawierać pozycje związane z infromacjami lokalnymi oraz relacjami pełnomocnictwa
- **tablica kontroli dostępu** – jest indeksowana stroną źródłową, stroną przeznaczenia i kontekstem.
  Każda pozycja zawiera zbiór PDU akceptowanych przez odbiorcę
- **tablica widoków MIB** – składa się ze zbioru widoków

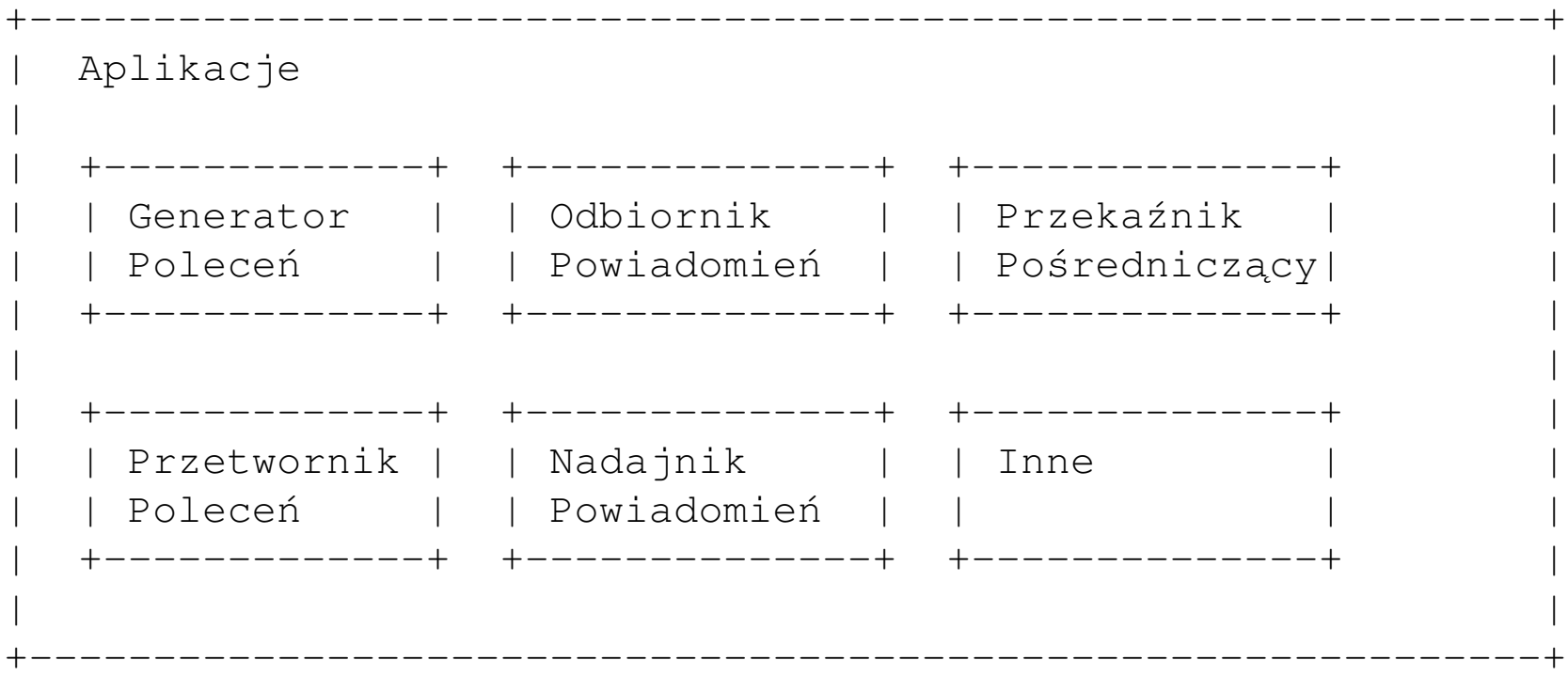
Architektura jednostki SNMPv3

- Koegzystencja starego i nowego.
- Elementy
  - Jądro SNMP
    - dokładnie jedno dla każdej jednostki,
    - identyfikowane przez snmpEngineID.
  - Aplikacje.

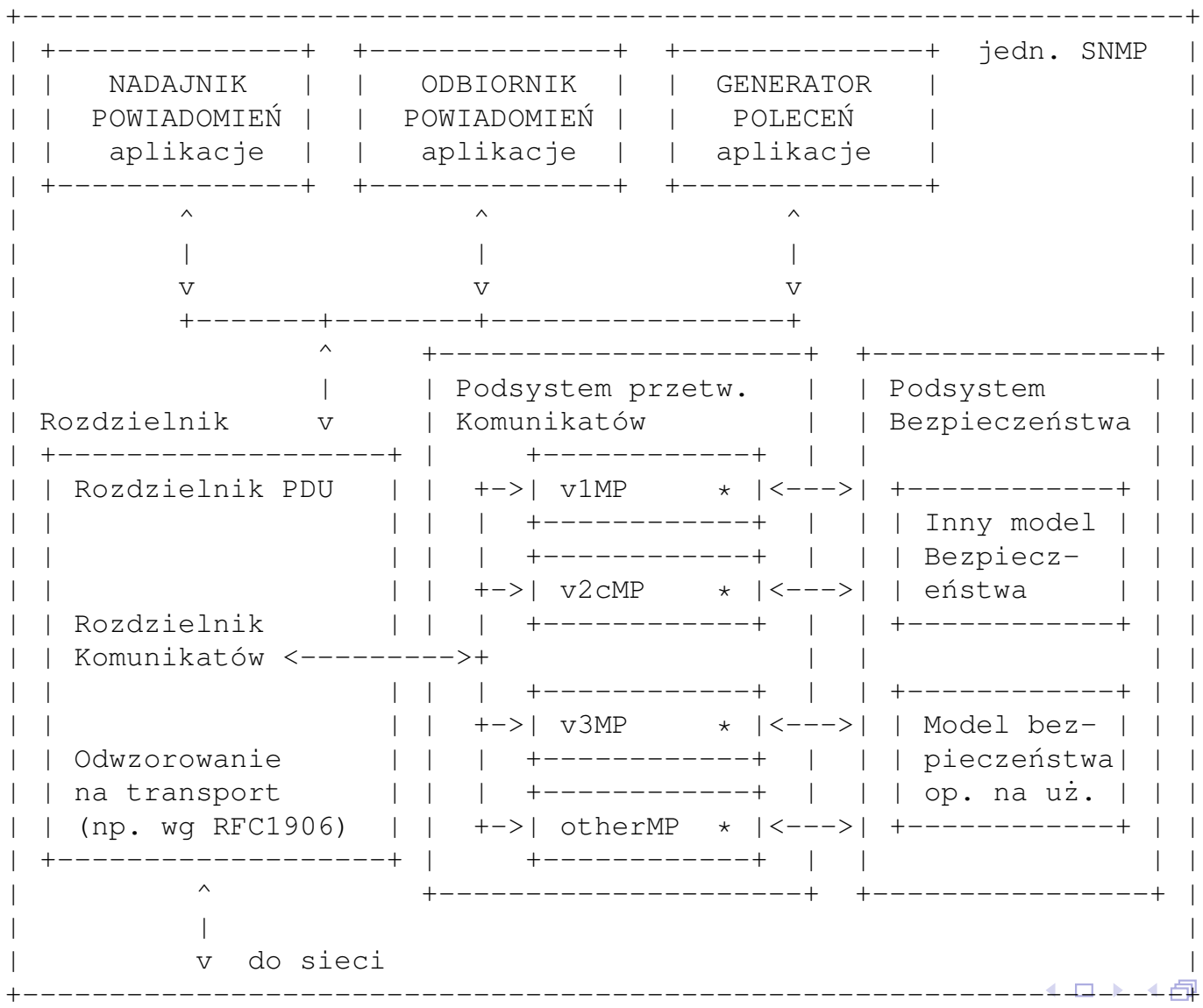
Architektura jednostki SNMP – jądro



Architektura jednostki SNMP – aplikacje



Schemat działania jednostki SNMP



Wysokopoziomowe parametry bezpieczeństwa

- securityModel – zastosowany model bezpieczeństwa:
  - oparty na społecznościach,
  - oparty na użytkownikach.
- securityName – nazwa osoby, organizacji itp. wykonującej czynności zarządzania,
- securityLevel – wymagany poziom bezpieczeństwa.
  - bez autentyfikacji i poufności (noAuthNoPriv),
  - z autentyfikacją, ale bez poufności (authNoPriv),
  - z autentyfikacją i poufnością (authPriv).

Podział na moduły

- Moduł uwierzytelnienia
  - integralność danych,
  - uwierzytelnienie pochodzenia danych.
- Moduł czasowy
  - ochrona przed powtórzeniami,
  - ochrona przed opóźnieniami.
- Moduł ochrony prywatności
  - zapewnienie poufności danych.

Stosowane mechanizmy bezpieczeństwa

- HMAC-MD5-96,
- HMAC-SHA-96,
- CBC-DES,
- czas sprawdzany tylko przy sprawdzaniu integralności danych:
  - autentyfikacja synchronizacji czasu,
  - snmpEngineBoots – liczba uruchomień agenta,
  - snmpEngineTime – czas na maszynie agenta.

Atrybuty użytkownika

- userName – nazwa,
- securityName – nazwa niezależna od modelu bezpieczeństwa,
- authProtocol – czy komunikaty mają być uwierzytelniane i jaki protokół ma być używany,
- authKey – klucz (prywatny) do powyższego uwierzytelniania (różny dla różnych jąder SNMP),
- authKeyChange i authOwnKeyChange – sposób zmiany klucza uwierzytelnienia,
- privProtocol – czy komunikaty mają być szyfrowane i jaki protokół obsługi szyfrowania ma być użyty,
- privKey – klucz (prywatny) do powyższego szyfrowania (różny dla różnych jąder SNMP),
- privKeyChange i privOwnKeyChange – sposób zmiany klucza szyfrowania.

Klucze

- Lokalizacja
  - Hasło jest konwertowane na klucz K_u za pomocą MD5 lub SHA,
  - Z wartości $K_u \cdot \text{snmpEngineID} \cdot K_u$ za pomocą przypisanej użytkownikowi metody generowania hasza generowany jest wyciąg – to jest klucz lokalny.
- Renegocjacja
  - specjalne komunikaty,
  - oparta na tajności starego klucza i losowości.

Model kontroli dostępu oparty na perspektywach (VACM)

- Pamięć lokalnej konfiguracji (Local Configuration Datastore – LCD) zawiera informacje o prawach dostępu.
- Zdefiniowane jest pojęcie grupy (zbiór par securityModel, securityName).
- Prawa są definiowane z uwzględnieniem securityLevel.

Perspektywy

- Dla każdego kontekstu (adresu w MIB) może być ustalona perspektywa: określa się typy (i opcjonalnie instancje typów), do których jest dostęp.
- Perspektywy są definiowane przez
  - poddrzewa perspektywy,
  - rodziny drzew perspektywy (maski bitowe).
- Każda grupa ma perspektywy
  - odczytu,
  - zapisu,
  - powiadamiania.