Bezpieczeństwo danych - Projekt AVISPA

Juliusz Kuzyka, Rafał Dadura

Czerwiec 2023

Spis treści

1 Omówienie działania protokołu

1.1 Cel działania prtokołu

Protokół Kerberos V5 jest protokołem uwierzytelniania sieciowego, który został opracowany w celu zapewnienia bezpiecznego uwierzytelniania i kontrolowania dostępu do zasobów w środowiskach sieciowych. Jego głównym celem jest zapewnienie poufności, integralności i autentyczności komunikacji między klientem a serwerem w sieciach, które mogą obejmować wiele hostów i usług.

1.2 Kroki

Najpierw dochodzi do procesu uwierzytelniania klienta na serwerze, nazywanym centrum dystrybucji kluczy (KDC), który przesyła nazwę użytkownika.

KDC generuje unikatowy identyfikator, zwany ticket-granting ticket (TGT), szyfruje go za pomocą tajnego klucza TGS i przekazuje zaszyfrowaną wartość klientowi.

Proces logowania klienta:

1. Użytkownik wprowadza login i hasło na swoim urządzeniu klienta.
2. Mechanizmy logowania, takie jak pkinit, umożliwiające użycie kluczy publicznych zamiast hasła, również mogą być wykorzystane.
3. Klient konwertuje hasło na klucz symetryczny, korzystając z wbudowanego klucza lub jednokierunkowej funkcji haszującej, zależnie od użytych narzędzi kryptograficznych.

Proces uwierzytelniania:

1. Klient wysyła swoje ID w postaci jawnej wiadomości do serwera uwierzytelniającego (AS).
2. AS generuje tajny klucz, konwertując hasło użytkownika znajdujące się w bazie danych.
3. AS sprawdza, czy klient istnieje w bazie danych. Jeśli tak, AS wysyła dwie wiadomości zwrotne:
   - Wiadomość A: Klucz sesji klienta, zaszyfrowany tajnym kluczem klienta.
   - Wiadomość B: Ticket-granting ticket (TGT) - zawiera ID klienta, adres jego sieci i zaszyfrowany klucz sesji klienta tajnym kluczem TGS.
4. Po otrzymaniu wiadomości A i B, klient rozpoczyna proces odszyfrowywania wiadomości A za pomocą tajnego klucza wygenerowanego z hasła użytkownika. Jeśli wprowadzone przez użytkownika hasło nie odpowiada hasłu w bazie danych AS, tajny klucz klienta będzie inny i klient nie będzie w stanie odszyfrować wiadomości A. Jeśli klucz jest prawidłowy, klient odszyfrowuje wiadomość A. Klucz sesji z tej wiadomości będzie używany do dalszej komunikacji. Klient nie jest w stanie odszyfrować wiadomości B, ponieważ jest ona zaszyfrowana tajnym kluczem TGS.

Proces autoryzacji:

1. Wysyłając zapytanie o wykonanie usługi, klient przesyła do TGS następujące wiadomości:
   - Wiadomość C: Zawiera TGT z wiadomości B oraz ID oczekiwanej usługi.
   - Wiadomość D: Uwierzytelnienie (zawierające ID klienta i znacznik czasu), zaszyfrowane za pomocą klucza sesji klienta/TGS.
2. TGS "tworzy"wiadomość B na podstawie wiadomości C. Następnie odszyfrowuje wiadomość B za pomocą tajnego klucza TGS, tworząc klucz sesji klienta/TGS. Wykorzystując ten klucz, TGS odszyfrowuje wiadomość D (uwierzytelnienie) i wysyła dwie następujące wiadomości do klienta:
   - Wiadomość E: Zawiera ID klienta, adres sieciowy, okres ważności i klucz sesji klienta/serwera. Całość jest zaszyfrowana tajnym kluczem usługi.
   - Wiadomość F: Klucz sesji klienta/serwera, zaszyfrowany kluczem sesji klienta/TGS.

Zapytanie klienta:

1. Po otrzymaniu wiadomości E i F od TGS, klient posiada wystarczającą ilość danych, aby zostać uwierzytelnionym na serwerze usług (SS). Klient nawiązuje połączenie z SS i wysyła następujące wiadomości:
   - Wiadomość E z poprzedniego kroku.
   - Wiadomość G: Narzędzie uwierzytelnienia zawierające ID klienta i znacznik czasu. Zaszyfrowane kluczem sesji klienta/serwera.
2. SS odszyfrowuje dane przy użyciu własnego tajnego klucza, aby uzyskać klucz sesji klienta/serwera. Następnie SS odszyfrowuje wiadomość G przy użyciu tego klucza sesji i wysyła klientowi następującą wiadomość w celu potwierdzenia tożsamości klienta i zgody na wykonanie usługi:
   - Wiadomość H: Znacznik czasu z wiadomości uwierzytelniającej klienta, zaszyfrowany kluczem sesji klienta/serwera.
3. Klient odszyfrowuje wiadomość H za pomocą klucza sesji klienta/serwera. Dodatkowo sprawdza, czy znacznik czasu jest prawidłowy. Jeśli jest, klient może uznać serwer za wiarygodny i rozpoczyna wysyłanie zapytań o usługi na tym serwerze.
4. Serwer rozpoczyna wykonywanie żądanych usług na prośbę klienta.

1.3 Wymogi bezpieczeństwa

Protokół Kerberos V5 wprowadza szereg wymogów bezpieczeństwa w celu zapewnienia skutecznego uwierzytelniania i ochrony danych. Oto niektóre z tych wymogów:

- Poufność danych: Protokół Kerberos V5 zapewnia poufność danych poprzez szyfrowanie komunikacji między klientem a serwerem. Wykorzystywane są algorytmy kryptograficzne, takie jak DES (Data Encryption Standard) lub AES (Advanced Encryption Standard), aby zabezpieczyć przesyłane informacje przed nieautoryzowanym dostępem.
- Integralność danych: Protokół Kerberos V5 chroni integralność danych, zapewniając, że informacje nie zostały zmienione w trakcie transmisji. Wykorzystywane są funkcje skrótu (hash), takie jak SHA-1 (Secure Hash Algorithm 1) lub SHA-2, które są używane do weryfikacji integralności danych w różnych etapach uwierzytelniania.
- Ochrona poufności hasła: Protokół Kerberos V5 zapewnia ochronę poufności hasła użytkownika. Hasła są przechowywane w postaci zaszyfrowanej (zazwyczaj jako funkcje skrótu), co minimalizuje ryzyko kompromitacji w przypadku wycieku bazy danych uwierzytelniania.
- Uwierzytelnienie dwustronne: Protokół Kerberos V5 umożliwia uwierzytelnienie dwustronne, co oznacza, że zarówno klient, jak i serwer uwierzytelniają się nawzajem. Działa to na zasadzie wzajemnego wymagania biletów uwierzytelniających, co zapewnia większe bezpieczeństwo w porównaniu do jednostronnego uwierzytelnienia.
- Limit czasu ważności biletów: Bilety uwierzytelniające w protokole Kerberos V5 mają określony czas ważności. Ograniczenie to minimalizuje ryzyko wykorzystania biletu przez niepowołane osoby po określonym czasie. Po upływie ważności biletu, użytkownik musi ponownie przejść proces uwierzytelniania.
- Zabezpieczenie przed atakami powtarzającymi: Protokół Kerberos V5 zawiera mechanizmy, które zapobiegają atakom opartym na powtarzaniu wcześniej przechwyconych komunikatów. Są to między innymi unikalne identyfikatory transakcji (nonce), które uniemożliwiają wykorzystanie wcześniej przechwyconych komunikatów uwierzytelniających.
- Odporność na ataki brute force: Protokół Kerberos V5 wprowadza mechanizmy opóźnienia i blokady po wielu nieudanych próbach uwierzytelnienia, aby utrudnić ataki typu brute force, które polegają na próbie odgadnięcia hasła przez wypróbowanie wielu kombinacji.

Wymienione powyżej wymogi bezpieczeństwa przyczyniają się do zapewnienia silnego uwierzytelniania i ochrony danych w protokole Kerberos V5.

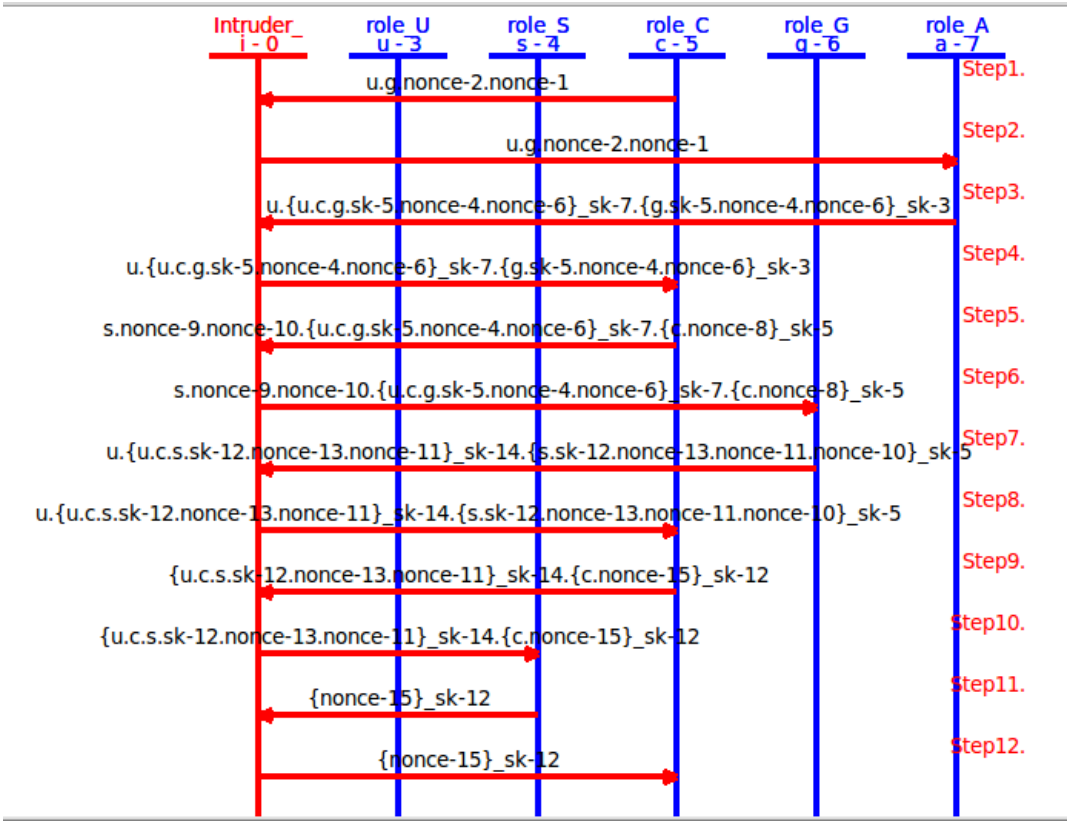
2 Specyfikacja protokołu w CAS

```
protocol KerberosV5;
identifiers
A, G, C, S, U          : user;
N1, N2                 : number;
L1, L2                 : number;
T1start, T1expire,T1 : number;
T2start, T2expire,T2  : number;
Kcg, Kcs, Kag, Ku, Kgs  : symmetric_key;

messages
1. C -> A  : U, G, L1, N1
2. A -> C  : U, {U, C, G, Kcg, T1start, T1expire}Kag,{G, Kcg, T1start, T1expire}Ku
3. C -> G  : S, L2, N2, {U, C, G, Kcg, T1start, T1expire}Kag,{C, T1}Kcg
4. G -> C  : U, {U, C, S, Kcs, T2start, T2expire}Kgs,{S, Kcs, T2start, T2expire, N2}Kcg
5. C -> S  : {U, C, S, Kcs, T2start, T2expire}Kgs,{C, T2}Kcs
6. S -> C  : {T2}Kcs

knowledge
A          : A,G,C,S,U;
G          : A,G,C,S,U;
S          : A,G,C,S,U;
C          : A,G,C,S,U;
U          : A,G,C,S,U;

session_instances
 [A:a,G:g,C:c,S:s,U:u];

goal
 S authenticates C on T2;
```

Rysunek 1: Specyfikacja protokołu w CAS

3 Specyfikacja ataków

Przeprowadziliśmy atak man in the middle po tym, jak zwiększyliśmy wiedzę napastnika o A, G, C, S i U.



Rysunek 2: Specyfikacja protokołu w CAS

4 Wyniki 4 testów

4.1 OFMC

Test OFMC wskazał, że Kerberos V jest bezpieczny.

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /home/span/span/testsuite/results/hlpslGenFile.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 0.01s
  visitedNodes: 8 nodes
  depth: 7 plies
```

Rysunek 3: Atak OFMC

4.2 ATSE

Test ATSE również wykazał bezpieczeństwo badanego protokołu.

```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL

PROTOCOL
  /home/span/span/testsuite/results/hlpslGenFile.if

GOAL
  As Specified

BACKEND
  CL-AtSe

STATISTICS

  Analysed   : 13 states
  Reachable  : 5 states
  Translation: 0.00 seconds
  Computation: 0.00 seconds
```

Rysunek 4: Atak ATSE

4.3 SATMC

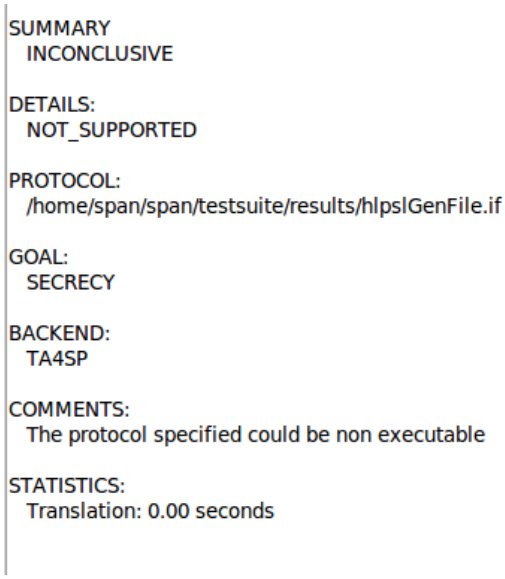
Test SATMC nie jest dostępny dla protokołu Korbaros V.

```
SUMMARY
  INCONCLUSIVE

DETAILS
  ERROR

PROTOCOL
  hlpslGenFile.if

BACKEND
  SATMC
```

Rysunek 5: Atak SATMC

4.4 TA4SP

Test TA4SP nie jest obsługiwany, dlatego nie jesteśmy w stanie sprawdzić rzetelności testu.



Rysunek 6: Atak TA4SP

Literatura

[1] M. R. Arcos. Kerberos: a secure network authentication system. *Network Protocols Handbook*, 2:587–604, 1997.

[2] C. Ellison and B. Frantz. *Kerberos: The Definitive Guide*. O'Reilly Media, 2005.

[3] S. Kent and R. Atkinson. Security architecture for the internet protocol. Technical report, RFC 2401, 1998.

[4] J. Kohl and C. Neuman. The kerberos network authentication service (v5). https://web.mit.edu/kerberos/krb5-1.12/doc/krb5-user/Intro-to-Kerberos-V5.html, 1993.

[5] A. Medvinsky, M. Hur, and M. Peinado. Integrating kerberos authentication into the windows operating system. https://www.microsoft.com/en-us/research/publication/integrating-kerberos-authentication-into-the-windows-operating-system/, 2001.

[6] MIT Kerberos Consortium. *The Kerberos Network Authentication Service (V5) - Tutorial*, 2008.

[7] C. Neuman, T. Yu, and S. Hartman. The kerberos network authentication service (v5). Technical report, RFC 1510, 1994.

[8] A. Radding. *Kerberos: A Network Authentication System*. Addison-Wesley Professional, 2003.

[9] L. Seitz and J. Schwenk. Kerberos: An authentication service for computer networks. *Communications of the ACM*, 46(5):110–113, 2003.

[10] R. Wright and R. Thompson. Kerberos: A network authentication system. *IEEE Communications Magazine*, 37(9):54–59, 1999.