

# AVISPA PROJEKT

## "PROTOKÓŁ Kerberos V5"

Dominika Atroszczyk, Daria Shevchenko





# Kerberos V5

**Bilet od Serwera Autoryzacyjnego:**  
 $\{U, C, G, K_{cg}, T1start, T1expire\}K_{ag}$

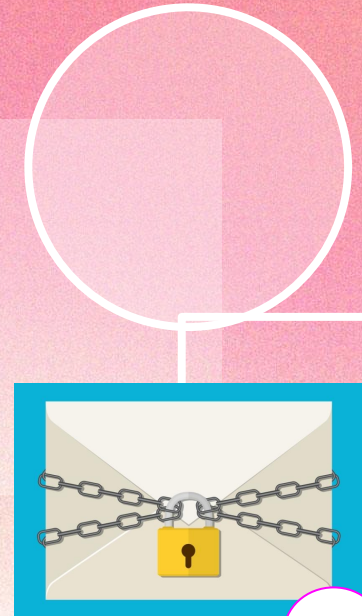
**Autorzy:** B. Clifford Neuman and Theodore Ts'o (1994)

- zaawansowany protokół uwierzytelniania
- wykorzystuje bilety i szyfrowanie symetryczne, wymaga TTP(trusted third party)
- umożliwia bezpieczną i skuteczną weryfikację tożsamości użytkowników oraz serwerów
- działa na porcie UDP 88

## Bilety:

Zawierają klucze sesji oraz inne dane zaszyfrowane -> poufność i integralność danych

Dwa rodzaje biletów: Ticket Granting Ticket, Service Ticket





# Kerberos V5

## **Symbole:**

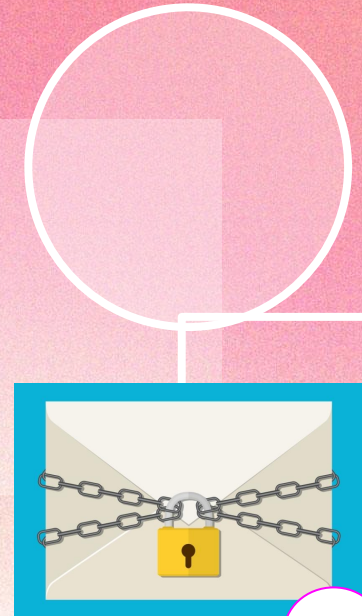
- C – klient
- S – server, z którym C chce się połączyć
- U – użytkownik – osoba w imieniu którego działa klient
- G – serwer biletów (Ticket Granting Server)
- A – serwer autoryzacyjny (Key Distribution Center)

N1, N1: nonce – losowe liczby (świeżość komunikacji)

L1, L2: lifetimes – stałe

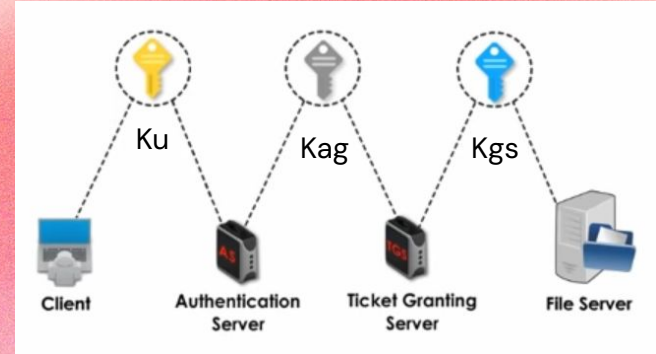
T1start, T1expire: znaczniki czasowe (ważność biletu C a G)

T2start, T2expire: znaczniki czasowe (ważność biletu C a S)



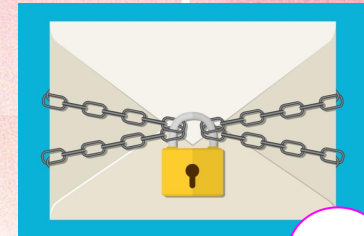


# Kerberos v5



## Symbole kluczy:

- **Kcg**: klucz sesji między klientem (C) a serwerem biletów (G), generowany przez serwer autoryzacyjny (A).
- **Kcs**: klucz sesji generowany przez serwer biletów (G).
- **Kag**: długoterminowy klucz symetryczny, znany tylko przez serwer autoryzacyjny (A) i serwer biletów (G).
- **Kgs**: długoterminowy klucz symetryczny, znany tylko przez serwer biletów (G) i serwer docelowy (S).
- **Ku**: długoterminowy klucz symetryczny użytkownika (U), znany przez użytkownika i serwer autoryzacyjny (A).





# Kerberos V5

## Struktura wiadomości:

- C → A: U, G, L1, N1
- A → C: U, {U, C, G, Kcg, T1start, T1expire}Kag, {G, Kcg, T1start, T1expire}Ku





# KROKI



1. Klient przesyła do Serwera Autoryzacyjnego (A) zapytanie zawierające identyfikator użytkownika, serwera docelowego oraz losowe liczby (nonce).
2. Serwer Autoryzacyjny przesyła Klientowi bilety uwierzytelniające zaszyfrowane kluczem użytkownika oraz serwera.
3. Klient przesyła do Serwera Biletów (G) zapytanie wraz z biletami otrzymanymi od A.
4. Serwer Biletów przesyła Klientowi bilety uwierzytelniające do serwera docelowego.
5. Klient przesyła bilety do Serwera Docelowego (S).
6. Serwer Docelowy potwierdza autentyczność Klienta.



# CEL DZIAŁANIA PROTOKOŁU

**01**

## Uwierzytelnienie

użytkownik i serwer mogą  
wzajemnie zweryfikować swoją  
tożsamość

**02**

## DYSTRYBUCJA KLUCZY SYMetryczNYCH

Używa "biletów" do przesyłania  
kluczy do szyfrowania

**03**

## OCHRONA PRZED ATAKAMI TYPU REPLAY, EAVESDROPPING

Użycie znaczników czasowych i  
losowych liczb chroni przed  
podśluchiowaniem,  
odtworzeniem wiadomości



# WYMOGI BEZPIECZEŃSTWA



Zgodność między klientem ( C ) a serwerem ( S ) co do wartości T2



Zgodność znaczników czasu T1start i T1expire między klientem ( C ) a autoryzatorem ( A )

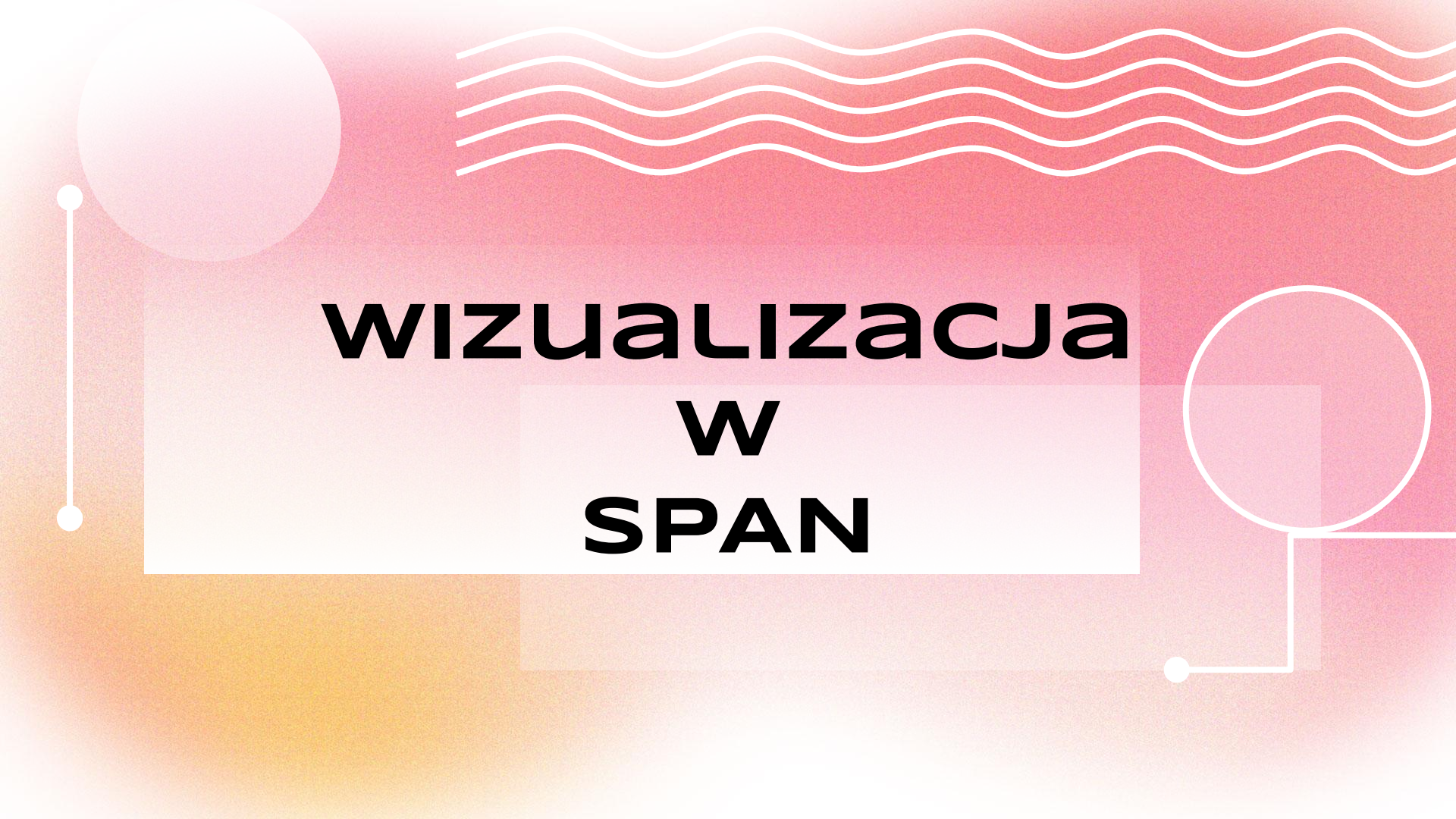


Zgodność znaczników czasu T2start, T2expire i T1 między klientem ( C ) a G



Zapewnienie poufności klucza sesji (Kcs)

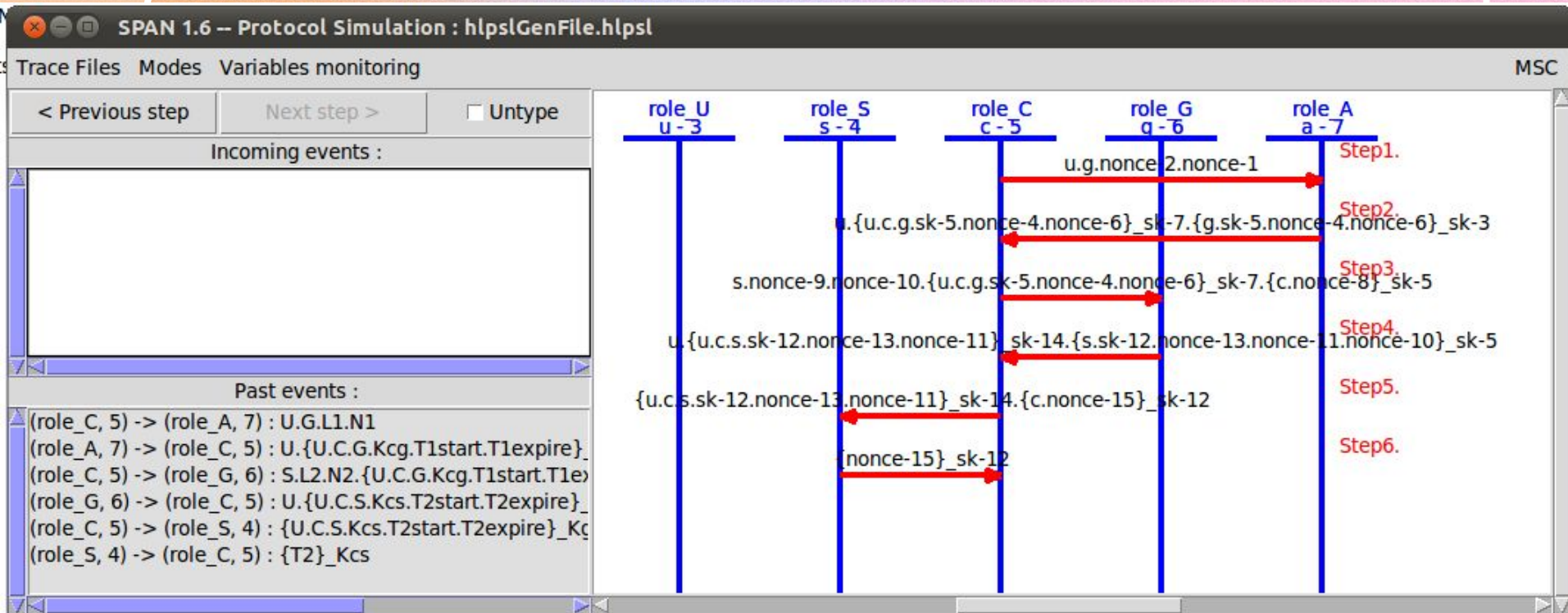




# **WIZUALIZACJA W SPAN**



# symulacja protokołu







# **ZBadanie Bezpieczeństwa**



# Analiza PROTOKOŁU za pomocą OFMC

SPAN 1.6 - Protocol Verification : Kerberos\_V5.cas

File

```
% 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: 0.05s
visitedNodes: 8 nodes
depth: 7 plies
```

Save file View CAS+ View HLPSSL Protocol simulation Intruder simulation Attack simulation

Tools Options

HLPSSL

☐ Session Compilation

HLPSSL2IF

IF

Choose Tool option and press execute

Execute

Depth :

Path :

OFMC ATSE SATMC TA4SP

----- Output error of attack trace generation :

%% Protocol verification result was not "UNSAFE"  
%% See AVISPA output at section "SUMMARY"

%% report2trace terminated abnormally...

Not launching simulation

## symulacja ataku



# Analiza Protokołu za pomocą OFMC

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: 0.02 seconds  
Computation: 0.00 seconds

Save file View CAS+ View HLPSSL Protocol simulation Intruder simulation Attack simulation

Tools Options

HLPSSL  
HLPSSL2IF  
IF

Choose Tool option and press execute  
Execute

OFMC ATSE SATMC TA4SP

Search Algorithm  
Depth first  
Breadth first

----- Output error of attack trace generation :

%% Protocol verification result was not "UNSAFE"  
%% See AVISPA output at section "SUMMARY"

%% report2trace terminated abnormally...

Not launching simulation

**symulacja ataku**



# ANALIZA PROTOKOŁU ZA POMOCĄ OFMC

File

SUMMARY  
INCONCLUSIVE

DETAILS  
ERROR

PROTOCOL  
hpslGenFile.if

BACKEND  
SATMC

Save file View CAS+ View HLPSP Protocol simulation Intruder simulation Attack simulation

Tools Options

HLPSP

HLPSP2IF

IF

OFMC ATSE SATMC TA4SP

Choose Tool option and press execute

Execute

Solver : Chaff  
SIM

Depth :

☐ Abstraction/Refinement

☐ Compound Types

☐ Optimized intruder



# ANALIZA PROTOKOŁU ZA POMOCĄ OFMC

SUMMARY  
INCONCLUSIVE

DETAILS:  
NOT\_SUPPORTED

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

GOAL:  
SECREC

BACKEND:  
TA4SP

COMMENTS:  
The protocol specified could be non executable

STATISTICS:  
Translation: 0.00 seconds

Save file

View CAS+

View HLP

Protocol simulation

Intruder simulation

Attack simulation

Tools

Options

HLPSL

HLPSL2IF

IF

OFMC

ATSE

SATMC

TA4SP

Choose Tool option and press execute

Execute

Verification Model

☐ Two Agent Only

Intruder Knowledge

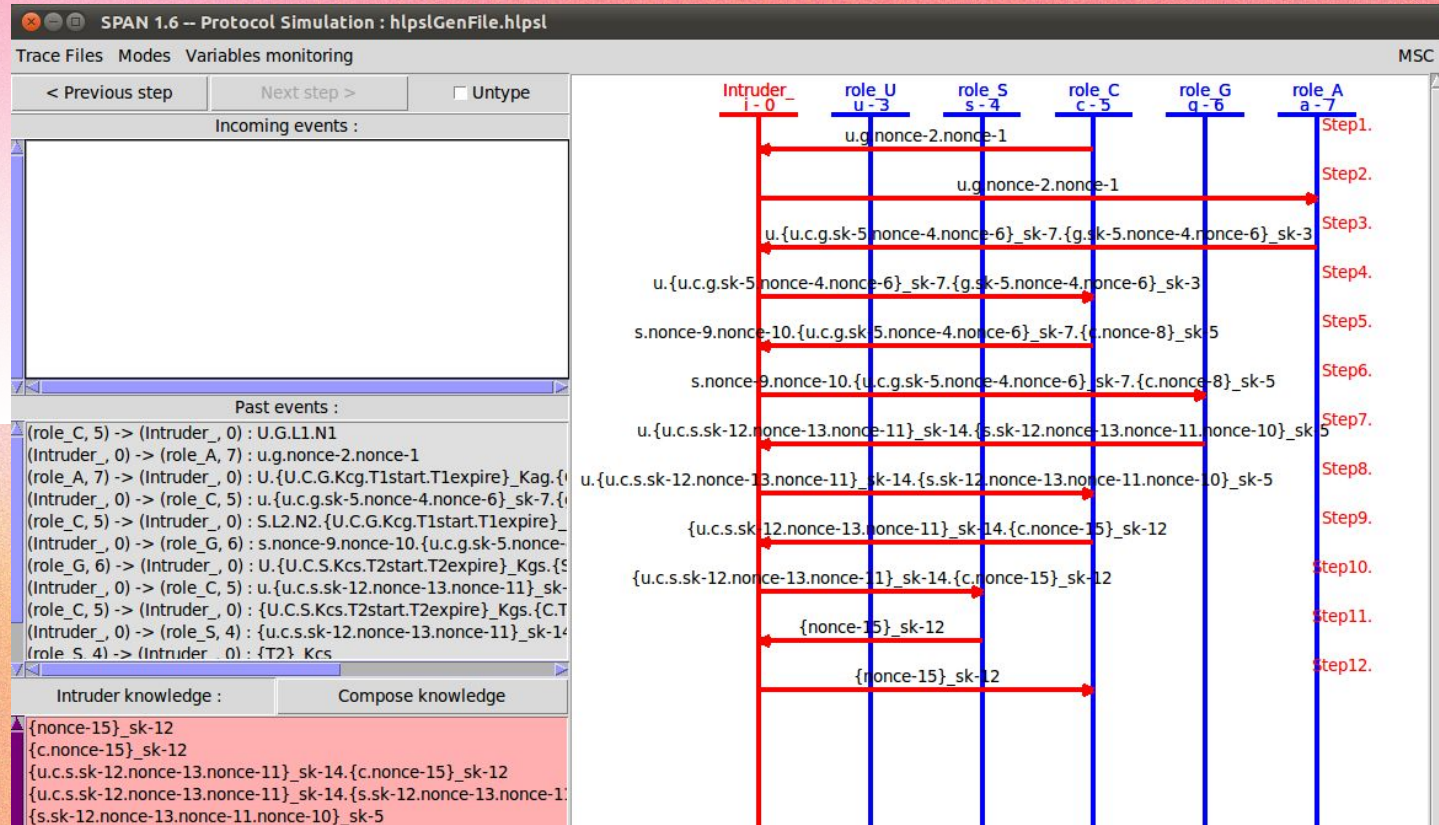
☒ Over-Approximation

☐ Under-Approximation

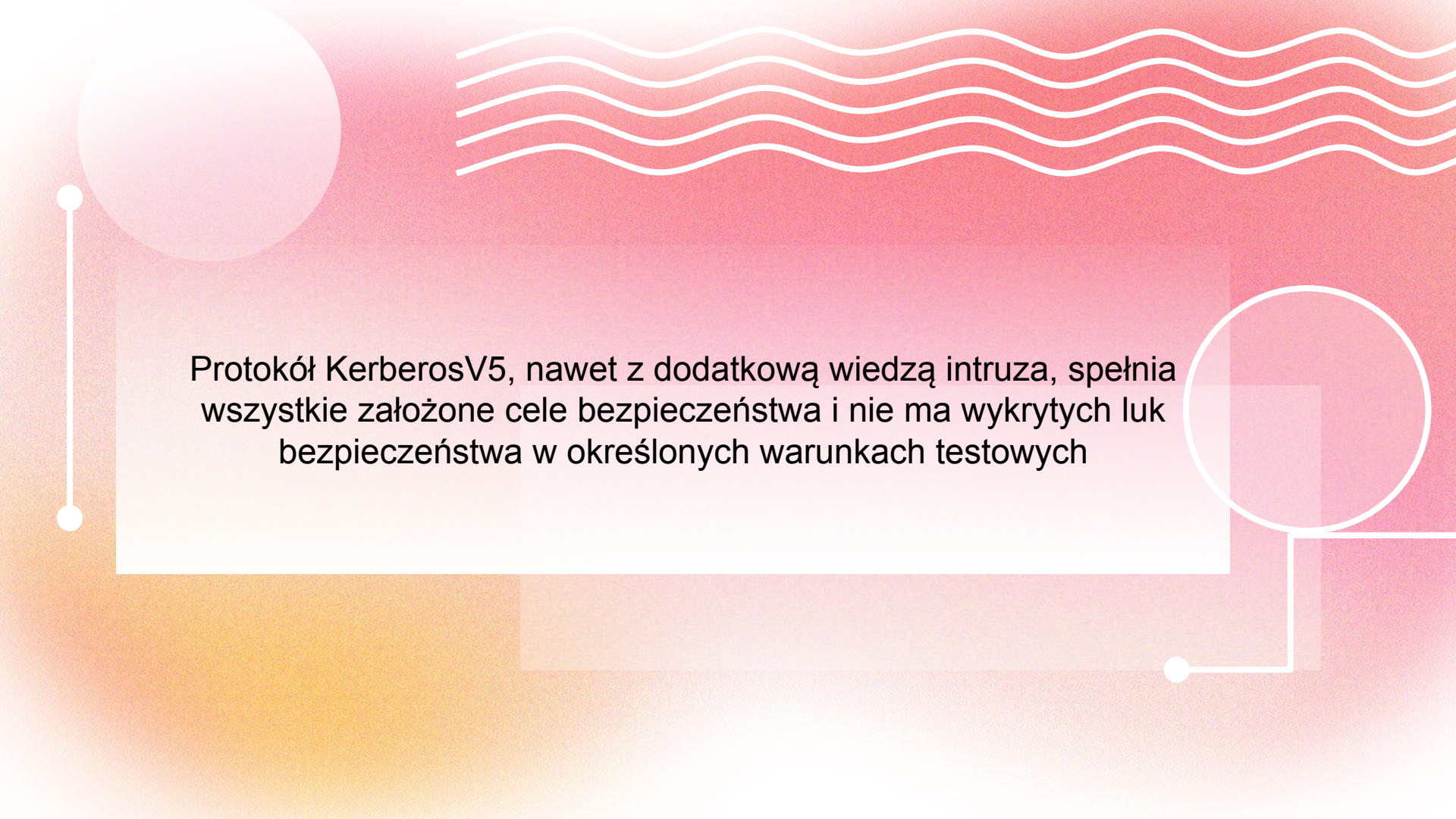
Level :



# symulacja intruza







Protokół KerberosV5, nawet z dodatkową wiedzą intruza, spełnia wszystkie założone cele bezpieczeństwa i nie ma wykrytych luk bezpieczeństwa w określonych warunkach testowych





# **AVISPA PROJEKT**

## **"PROTOKÓŁ Kerberos V5"**

Dominika Atroszczyk, Daria Shevchenko

