



Verifying the Independence of Security Protocols

eng. Genge Bela¹, prof. dr. eng. Iosif Ignat²

¹ PhD student at the Technical University of Cluj-Napoca and a junior lecturer at the “Petru Maior” University of Targu Mures

² Professor at the Technical University of Cluj-Napoca

Contact: ¹bgenge@upm.ro, ²Iosif.Ignat@cs.utcluj.ro



Introduction

- ◆ Security protocols?
 - Communication protocols + cryptography
 - Example message specification: $\{A, B, Na, K\}K_{ab}$
- ◆ Multi-protocol attacks?
 - Protocols running in the same environment
 - The attacker uses messages from other protocols (replay, type-flaw)
- ◆ Verifying the independence?
 - Verifying that protocols are not open to multi-protocol attacks



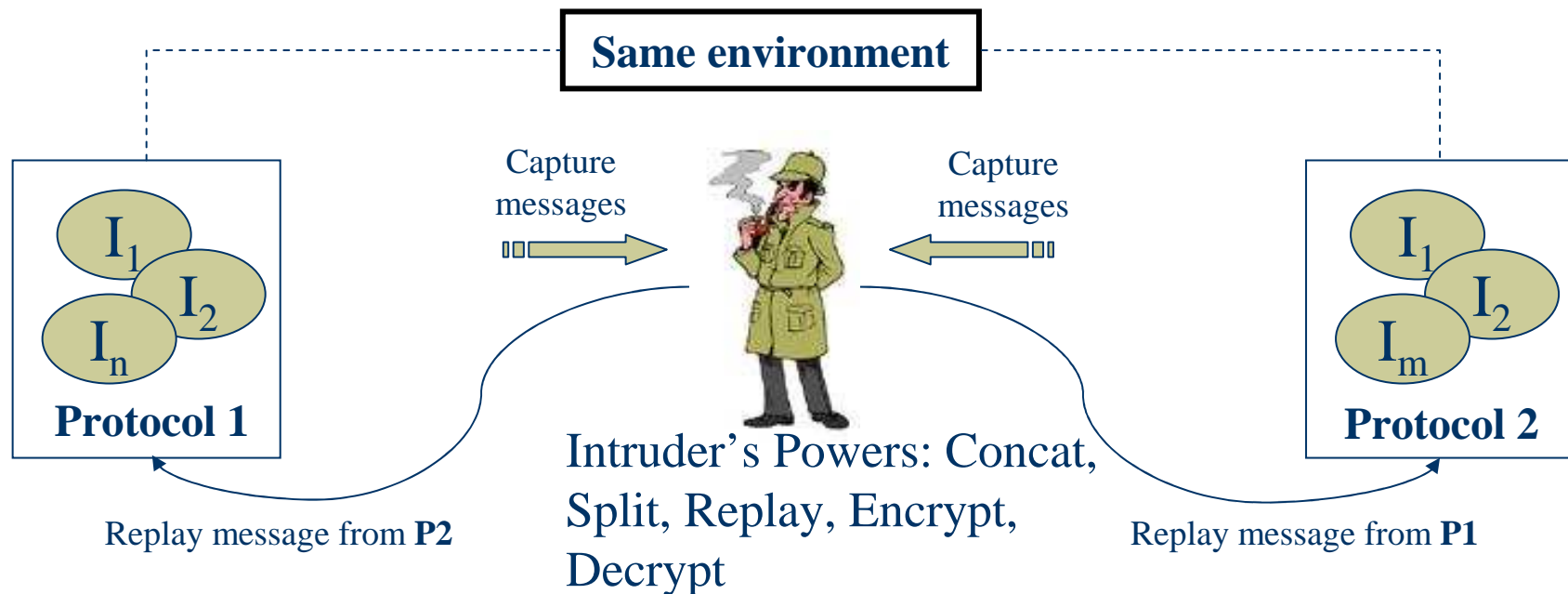
Overview of the presentation



- ◆ The analysis problem
- ◆ Syntactical analysis
- ◆ Analyzing single protocols
- ◆ Protocol independence requirements
- ◆ Analyzing the independence of two protocols
- ◆ Provide a tagging scheme
- ◆ Summary

The analysis problem

- ◆ Multiple protocol instances
- ◆ The intruder has complete control over the network
 - Dolev-Yao intruder model



Syntactical analysis

- ◆ Offers:
 - Message specification-based analysis
 - Eliminating the state-space explosion problem
- ◆ Proposed solution:
 - Use message patterns (i.e. term types):
 - $Na, Nb, \dots \rightarrow n$
 - $A, B, \dots \rightarrow r$
 - $Kab, Kas, \dots \rightarrow k_i$
 - Example: $n, r, \{n, n, r\}k, \{n, k\}h$
 - Use participant knowledge in the specification:
 - If $t \notin \kappa \rightarrow u$, else *use message patterns*, where t is a message term

Analyzing individual protocols against replay attacks

- ◆ Lowe's modified Wide Mouthed Frog protocol:

$A \rightarrow S: A, \{Ta, B, Kab\}Kas$
 $S \rightarrow B: \{Ts, A, Kab\}Kbs$
 $B \rightarrow A: \{Nb\}Kab$
 $A \rightarrow B: \{Nb+1\}Kab$

where

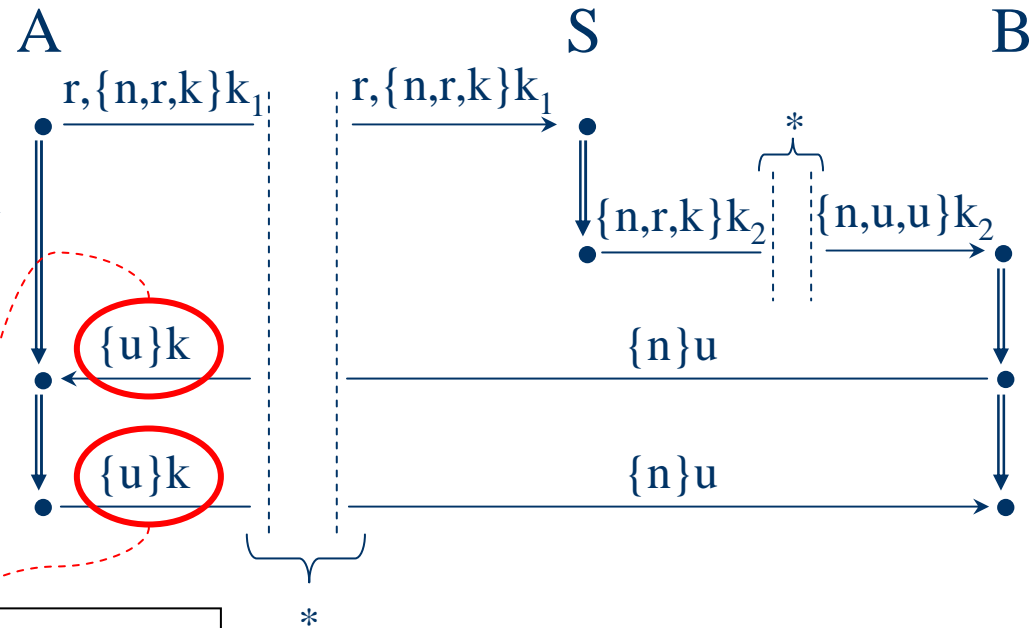
A, B, S – participant names

Ta, Ts – timestamps

Kas, Kbs – long-term keys

Kab – session key

Nb – nonce



Attacker can replay message $\{Nb+1\}Kab$: $\{Nb+1\}Kab$ is accepted as valid by A

* Transformation layers based on role knowledge

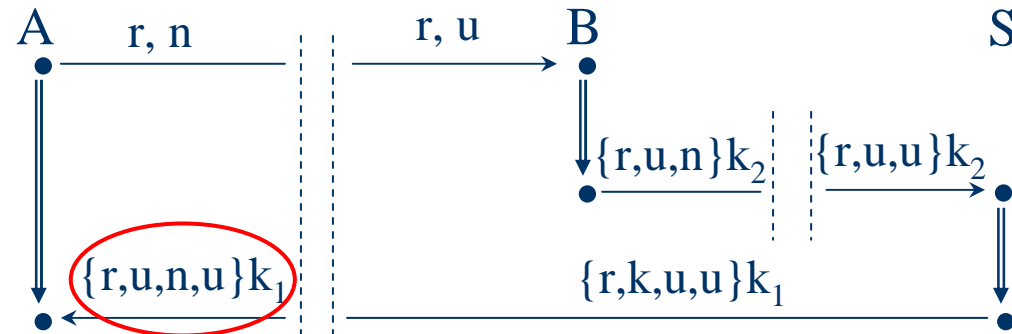
Protocol independence requirements

- ◆ Intruder's Powers: Encrypt, Decrypt, Concat, Split, Replay
- ◆ ¹Key secrecy independence of P_1 from P_2
 - Secrecy independence: secret terms from P_1 are not sent out unencrypted in P_2
 - Safe keys from P_1 are also safe in P_2
- ◆ ²Message independence of P_1 from P_2
 - Structural differentiation of encrypted terms
- ◆ Consequences
 - ¹The intruder can not inject valid re-constructed terms in P_1 based on captured terms from P_2
 - ²The intruder can not replay valid messages captured from P_2

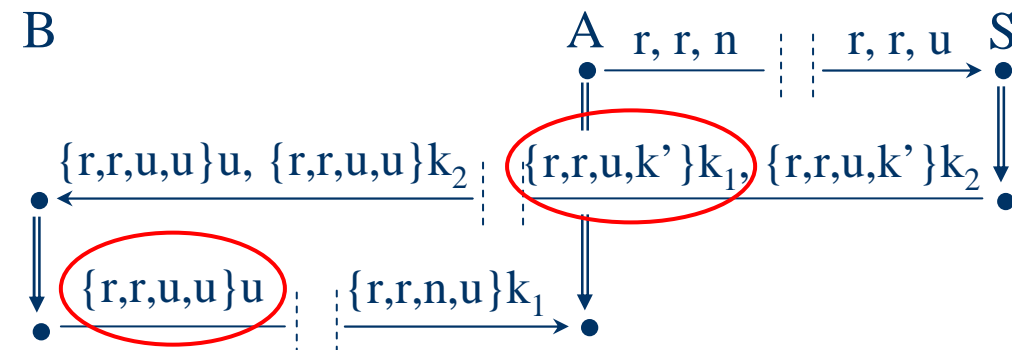
Analyzing the independence of two protocols

- ◆ Key exchange parts from the Yahalom-Lowe (Y-L) and Kao-Chow (K-C) protocols

(Y-L)
 $A \rightarrow B: A, Na$
 $B \rightarrow S: \{A, Na, Nb\}K_{bs}$
 $S \rightarrow A: \{B, Kab, Na, Nb\}K_{as}$



(K-C)
 $A \rightarrow S: A, B, N'a$
 $S \rightarrow B: \{A, B, N'a, K'ab\}K_{as},$
 $\{A, B, N'a, K'ab\}K_{bs}$
 $B \rightarrow A: \{A, B, N'a, K'ab\}K_{as}$



Message analysis

- ◆ Message sent in K-C:
 - $\{r,r,u,k'\}_{k_1}$ which is in fact $\{A,B,N'a,K'ab\}_{Kas}$
- ◆ Message expected in Y-L:
 - $\{r,u,n,u\}_{k_1}$ which is in fact $\{B,Kab,Na,Nb\}_{Kas}$
- ◆ Discovered attack:
 1. $A(Y-L) \rightarrow I: A, Na$
 2. $I \rightarrow S(K-C): B, A, Na$
 3. $S(K-C) \rightarrow I: \{B, A, Na, Kab\}_{Kas}$
 4. $I \rightarrow A(Y-L): \{B, A, Na, Kab\}_{Kas}$

User A now thinks the session key is 'A'
- *type flaw* attack -

Correcting the problem

- ◆ Adding more known information to the Y-L message:
 - $\{B, K_{ab}, N_a, N_b\}_{K_{as}} \rightarrow \{A, B, K_{ab}, N_a, N_b\}_{K_{as}}$
- ◆ The problem:
 - Other protocols can still be used to construct attacks
- ◆ More complex solutions (applied to all messages):
 - Using tagging schemes to prevent type-flaw attacks:
 - $\{B, K_{ab}, N_a, N_b\}_{K_{as}} \rightarrow \{B, K_{ab}, N_a, N_b, (n, k, n, n)\}_{K_{as}}$
 - Adding protocol information to prevent replay attacks:
 - $\{B, K_{ab}, N_a, N_b\}_{K_{as}} \rightarrow \{B, K_{ab}, N_a, N_b, (P1, V, M_x, n, k, n, n)\}_{K_{as}}$



Existing problems and future development

- ◆ The procedure can not show how the attack is constructed
- ◆ The procedure allows only a strong independence:
 - Message structure must be different
- ◆ The construction of the model and the analysis process require:
 - Professional knowledge of the involved protocols
- ◆ Future work:
 - Creating an automated tool for analyzing security protocols
 - Analyzing real life protocols using the developed tool



Summary

- ◆ We have developed:
 - A canonical model for capturing the structure of security protocol messages
 - A set of requirements that protocols must meet to achieve independence
- ◆ We have (re)discovered attacks:
 - Inside Lowe's Wide Mouth Frog protocol
 - Between the Yahalom-Lowe and Kao-Chow protocols
- ◆ We have provided a tagging scheme to avoid type-flaw and replay attacks



Questions?

Thank you for your attention!

Presented by: Genge Bela

Email: bgenge@upm.ro