Sequence Diagram Crypto Analyzer

A CARiSMA Plugin

Fakultät für Informatik LS 14 - Software Engineering
Technische Universität Dortmund

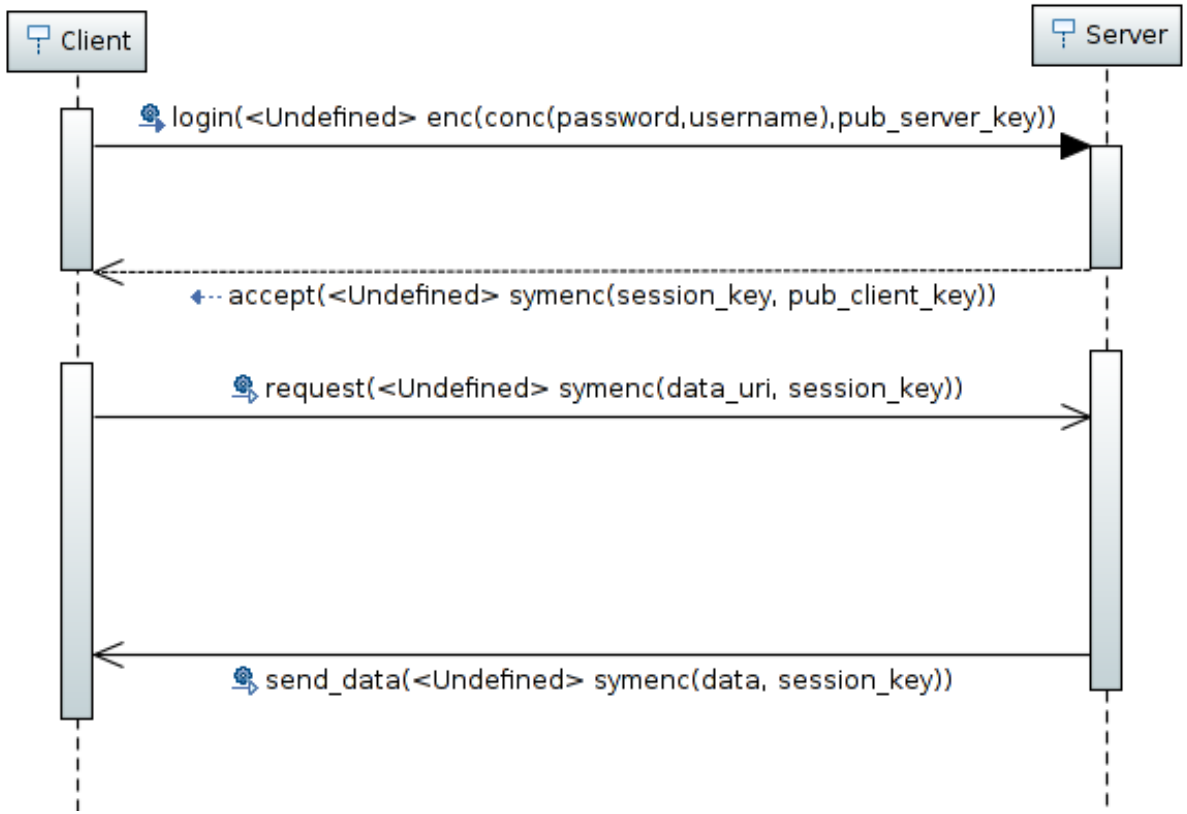
12. Mai 2015

Szenario

Ein **Client** möchte von einem **Server** Daten erhalten. Hierzu muss der Client sich zunächst **autorisieren**. Erfolgreich autorisiert erhält der Client ein **Session-Schlüssel** mit dem die darauf folgende Kommunikation verschlüsselt werden soll. Die vollständige Übertragung soll so ablaufen, dass ein MITMA **weder** in der Lage sein soll, zu erfahren wie das Passwort, der Benutzername des Clients lauten **noch** soll der MITMA in der Lage sein die Daten mitzulesen. Server und Client kennen hierzu, genau so wie der MITMA, mindestens die öffentlichen Schlüssel von Server und Client.

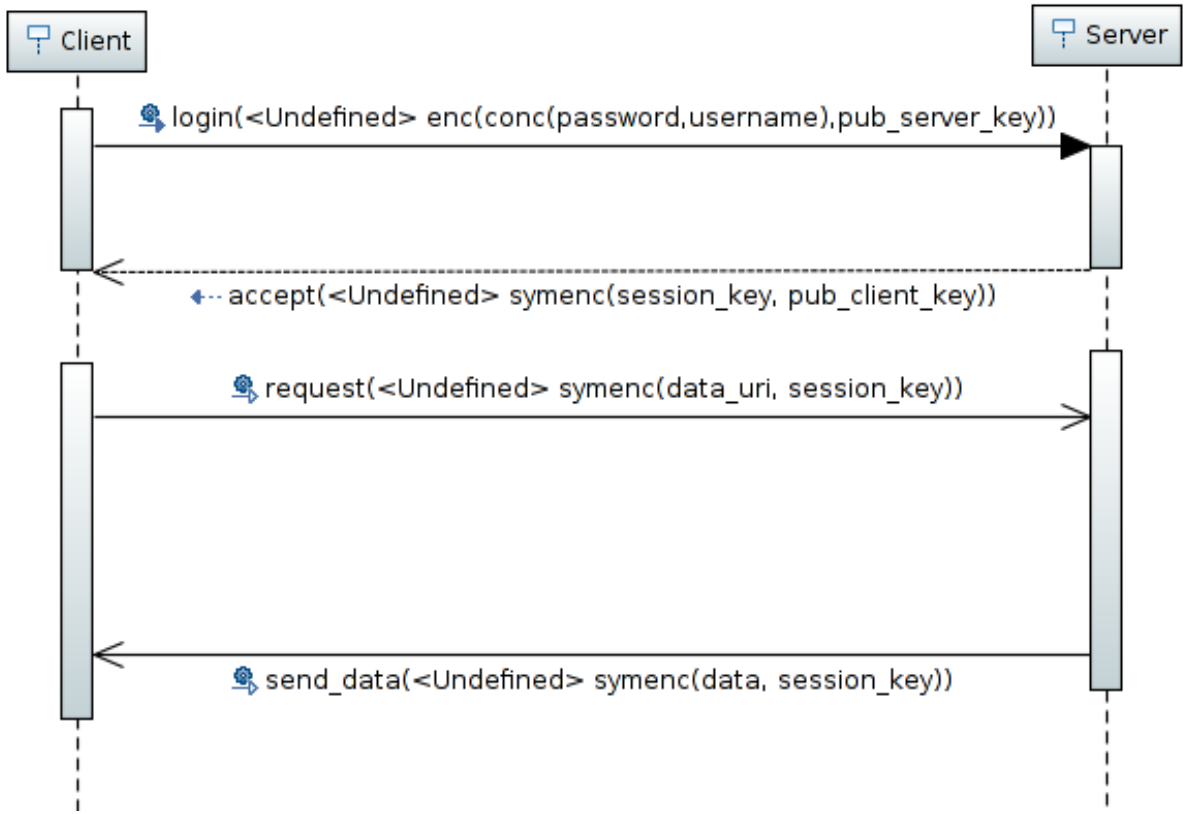
Mögliche Realisierung

Sequenz-Diagramm



Dieses mittels Papyrus erstellte UML Sequenz-Diagramm könnte das besagte Szenario realisieren. **Frage:** Ist diese Realisierung sicher?

Sequenz-Diagramm

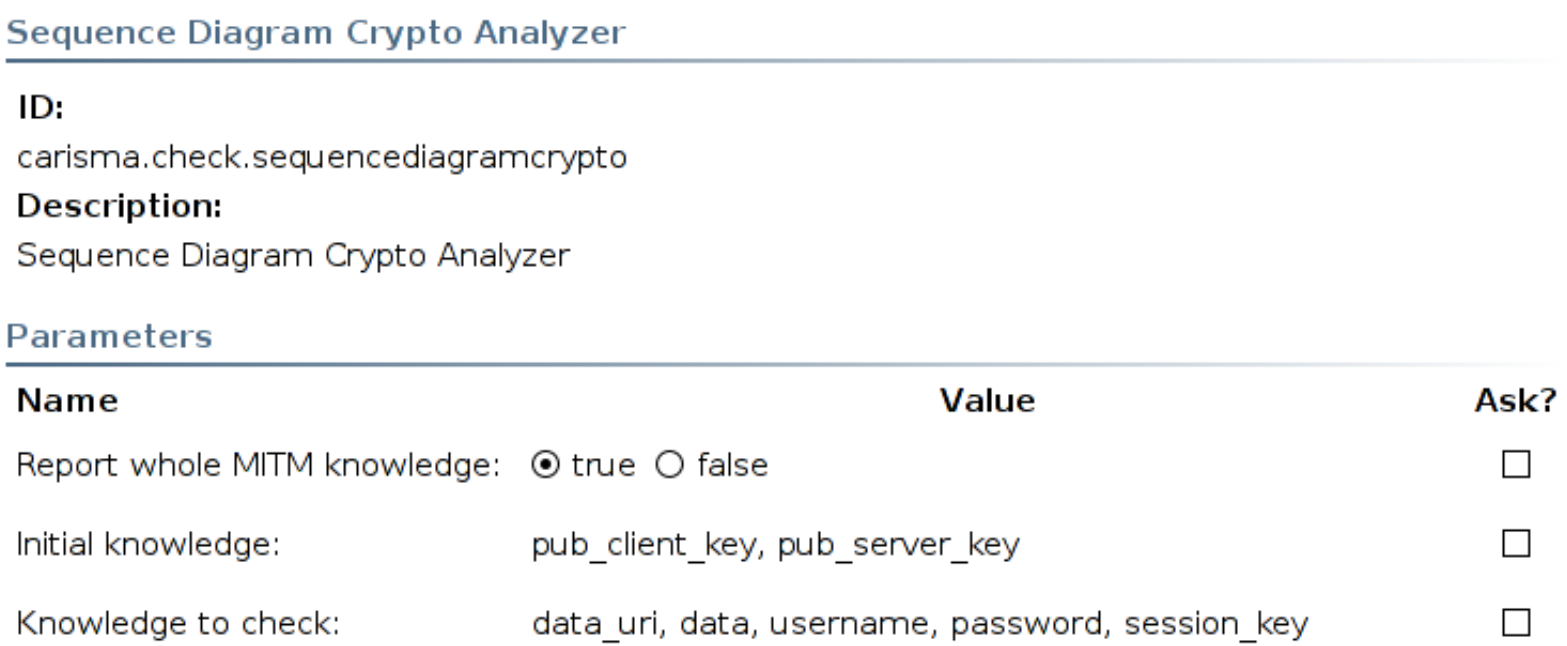


Dieses mittels Papyrus erstellte UML Sequenz-Diagramm könnte das besagte Szenario realisieren. **Frage:** Ist diese Realisierung sicher?

Um dies zu überprüfen konfigurieren wir im folgenden das Plugin, lassen es das Diagramm analysieren und beleuchten die dabei entstandene Analyse.

Plugin Konfiguration

technische universität dortmund



Parameter

Das Plugin besitzt 3 Parameter: **Report whole MITM knowledge**, **Initial knowledge** und **Knowledge to check**.

Plugin Konfiguration

technische universität dortmund

Sequence Diagram Crypto Analyzer

ID:
carisma.check.sequencediagramcrypto
Description:
Sequence Diagram Crypto Analyzer

Parameters

Name	Value	Ask?
Report whole MITM knowledge:	◉ true ○ false	☐
Initial knowledge:	pub_client_key, pub_server_key	☐
Knowledge to check:	data_uri, data, username, password, session_key	☐

Report whole MITM knowledge

Diese Einstellung ermöglicht es, das vollständige zur Überprüfung notwendige MITM Wissen ausgeben zu lassen; Also das Wissen welches der potenzielle MITMA erlangt zzgl. des Wissens welches zur Analyse der Sicherheit des Modells notwendig ist.

Plugin Konfiguration

technische universität dortmund

Sequence Diagram Crypto Analyzer

ID:
carisma.check.sequencediagramcrypto
Description:
Sequence Diagram Crypto Analyzer

Parameters

Name	Value	Ask?
Report whole MITM knowledge:	◉ true ○ false	☐
Initial knowledge:	pub_client_key, pub_server_key	☐
Knowledge to check:	data_uri, data, username, password, session_key	☐

Initial knowledge

Beschreibt das initiale Wissen des MITMA. In dem Szenario sind dem MITMA der öffentliche Schlüssel des Clients (*pub_client_key*) und der öffentliche Schlüssel des Servers (*pub_server_key*) bekannt.

Plugin Konfiguration

technische universität dortmund

Sequence Diagram Crypto Analyzer

ID:
carisma.check.sequencediagramcrypto
Description:
Sequence Diagram Crypto Analyzer

Parameters

Name	Value	Ask?
Report whole MITM knowledge:	◉ true ○ false	☐
Initial knowledge:	pub_client_key, pub_server_key	☐
Knowledge to check:	data_uri, data, username, password, session_key	☐

Knowledge to check

Beschreibt das Wissen für welches überprüft werden soll, ob ein MITMA dieses erlangen könnte. In dem Szenario wäre diese die Adresse der Daten (*data_uri*), die Daten (*data*), der Benutzername (*username*), sein Passwort (*password*) und der geheime Session-Schlüssel (*session_key*).

Ausgabe des Plugins

```
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
Running check : Sequence Diagram Crypto Analyzer
Parameters:
Knowledge to check : data_uri, data, username, password, session_key
Report whole MITM knowledge : true
Initial knowledge : pub_client_key, pub_server_key
--------------------------------------------------------------------------------
INFO: %----------PHASE 1----------%
INFO: [MITM Knowledge] {enc(conc(password,username),pub_server_key),symenc(data,session_key),
                        symenc(data_uri,session_key),data,pub_client_key,model::Interaction1::send_data_0,
                        model::Interaction1::login_0,model::Interaction1::accept_0,
                        symenc(session_key,pub_client_key),data_uri,model::Interaction1::request_0,
                        session_key,pub_server_key}
INFO: Objekt :model::Interaction1::Client
INFO: Term :(Knows(enc(conc(password,username),pub_server_key)) & Knows(symenc(data_uri,session_key)))
INFO: Evaluation:true
WARNING: MITMA might be able to impersonate Object model::Interaction1::Client
INFO: Objekt :model::Interaction1::Server
INFO: Term :(Knows(symenc(session_key,pub_client_key)) & Knows(symenc(data,session_key)))
INFO: Evaluation:true
WARNING: MITMA might be able to impersonate Object model::Interaction1::Server
INFO: %----------PHASE 2----------%
WARNING: MITMA knows data_uri
WARNING: MITMA knows data
INFO: MITMA does not know username
INFO: MITMA does not know password
WARNING: MITMA knows session_key
```

Auswertung

Ausgabe des Plugins

```
INFO: %----------PHASE 1----------%
[..]
WARNING: MITMA might be able to impersonate Object model::Interaction1::Client
[..]
WARNING: MITMA might be able to impersonate Object model::Interaction1::Server
INFO: %----------PHASE 2----------%
WARNING: MITMA knows data_uri
WARNING: MITMA knows data
[..]
WARNING: MITMA knows session_key
```

Während die erste Phase deutliche Warnungen ausgibt, dass ein potenzieller MITMA in der Lage ist sich sowohl als Client als auch als Server auszugeben, gibt die zweite Phase sogar bekannt, dass ein MITMA Kenntnisse über data_uri, data und session_key erlangen kann!

Die Probleme:

1. Der Session-Schlüssel wurde nicht sicher genug übertragen!
2. Es wurde keine Vorkehrung (wie etwa das Nutzen von nonce) gegen Replay-Attacken vorgenommen!

Warum das Plugin nutzen?

Warum das Plugin nutzen?

technische universität dortmund

Mithilfe des Plugins lassen sich Kommunikations-Protkolle noch **vor** der Implementierung auf ihre sicherheitskritischen Eigenschaften bezüglich MITM-Angriffe überprüfen.

Erste Phase

Die erste Phase kann ein gegebenes Sequenz-Diagramm danach gehend untersuchen, ob ein MITMA der entsprechend viele Nachrichten gesammelt hat, in der Lage wäre z.B. per Replay-Angriff sich als ein Server oder als ein Client auszugeben.

Zweite Phase

Die zweite Phase kann wiederum untersuchen, ob ein MITMA welcher entsprechend viele Nachrichten gesammelt hat, in der Lage wäre bestimmte Informationen zu kennen.