

AProVer

An User-Friendly tool for security protocol verification

USER MANUAL

Introduzione

L'applicazione rappresenta la componente Front End di un sistema che permette di effettuare la verifica formale dei criteri fondamentali di sicurezza nei protocolli di comunicazione.

In particolare, si potranno analizzare tutti quei protocolli progettati per permettere comunicazioni su reti non sicure.

La progettazione dei protocolli di sicurezza, nonostante la loro apparente semplicità, è particolarmente soggetta a errori, per questo motivo nel mondo dei protocolli di sicurezza, la verifica formale è richiesta per garantire la protezione da possibili minacce e incidenti.

Generalmente i test funzionali non riescono a rilevare tutte le vulnerabilità in quanto non prendono mai in considerazione la presenza di un utente "malintenzionato".

Con un sistema che permette la verifica formale si rafforza il controllo della sicurezza sin dalla fase di progettazione.

AProVer consente di rappresentare le informazioni di un'ampia gamma di protocolli permettendo di specificare gli attori che rappresentano i principali soggetti che partecipano allo scambio di informazioni, il contenuto dei messaggi scambiati e gli obiettivi del protocollo (che spesso possono essere espressi con un elenco di proprietà di sicurezza desiderate).

Gli attori che si scambiano messaggi (nei protocolli generalmente indicati dai simboli A, B e S) sono rappresentati nell'applicazione dai nomi Alice, Bob e Server con l'aggiunta del soggetto "malintenzionato" che è indicato con il nome Eye.

Per ciascuno degli attori è possibile specificare quali sono le chiavi per la crittografia e per la firma in suo possesso scegliendo tra le varie tipologie: Asimmetriche Pubbliche o Private, Simmetriche e per l'applicazione della funzione di hash.

Successivamente a questa fase è possibile inserire le informazioni scambiate tra i vari attori. Per ogni messaggio si descrivono nel payload i campi corredati dalle eventuali chiavi utilizzate per l'applicazione degli algoritmi di sicurezza.

Terminate le due fasi precedenti si inseriscono le informazioni relative alle proprietà di sicurezza da verificare.

Nei capitoli seguenti verranno specificate le modalità operative con cui si inseriscono i dati per le tre fasi.

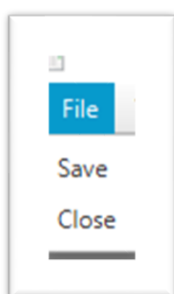
La Barra del Menu



La barra del menu (o dei menù) è il componente dell'interfaccia grafica costituito da tre elementi (File, Tool e Help) che, una volta attivati, visualizzano un menu a tendina mostrando le operazioni eseguibili dall'utente.

Il Contenuto delle opzioni dei menu potranno diversificarsi in base alle finestre visualizzate.

Menu – File



Tramite il menu File, selezionando l'opzione Save è possibile effettuare il salvataggio delle informazioni inserite nell'applicazione.

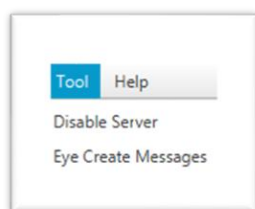
Il file è salvato con estensione **avr** nella cartella **AProVerFile** e con il nome:

protocol-AAAA-MM-GG hh-mm-ss.

Dove AAAA rappresenta l'anno, MM il mese, GG il giorno, hh l'ora, mm i minuti e ss i secondi dell'attimo in cui viene registrato il file.

Con l'opzione Close si effettua invece la chiusura della finestra e di conseguenza dell'applicazione.

Menu – Tool

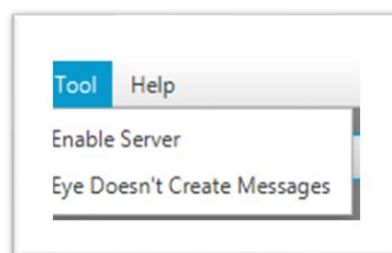


Con il menu Tool è possibile impostare le opzioni di configurazione dell'applicazione.

Tramite l'opzione "Disable Server/Enable Server" è possibile eliminare o reintegrare il **Server** tra gli Attori del protocollo.

Selezionando "Disable Server" l'Attore

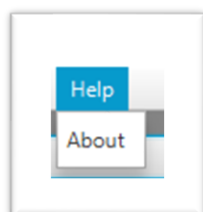
Server sarà eliminato e la voce del menù verrà modificata in "Enable Server" per permettere di reintegrare il **Server** tra gli Attori del protocollo. Lo stesso effetto può essere ottenuto utilizzando il pulsante presente nella Sezione Informativa descritta nel capitolo successivo.



L'opzione "Eye Create Messages/Eye Doesn't Create Messages" permette invece di abilitare o disabilitare la possibilità di configurare i messaggi per l'invio o la ricezione da o per l'Attore **Eye**.

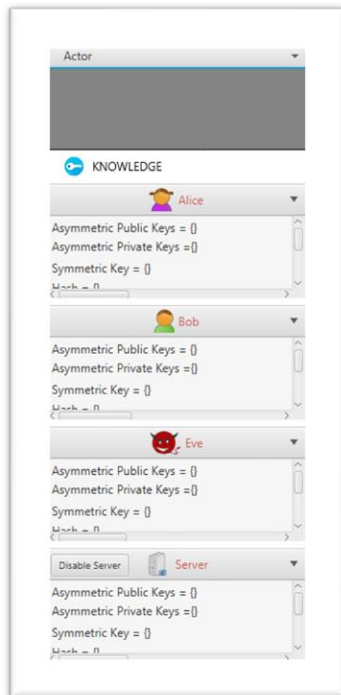
La selezione delle opzioni di questo menu sarà disabilitata dopo l'inserimento del primo messaggio.

Menu – Help



Il menu help contiene una sola opzione che consente di aprire un file PDF contenente il manuale utente e le istruzioni per l'utilizzo dell'applicazione.

Sezione Informativa

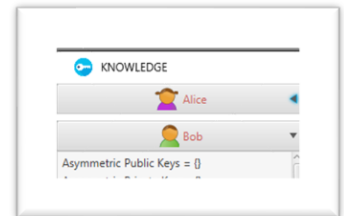


Nel lato sinistro dell'interfaccia grafica sono presenti le informazioni relative alle conoscenze di ogni Attore (Knowledge).

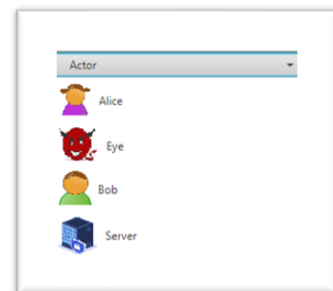
Per ogni Attore, **Alice**, **Bob**, **Eve** e **Server** (se non disabilitato con l'opzione presente nel menu Tool) sono presenti le chiavi in loro possesso relative a:

- Asymmetric Public Key (chiave pubblica per crittografia asimmetrica)
- Asymmetric Private Key (chiave pubblica per crittografia asimmetrica)
- Symmetric Key (chiave per crittografia simmetrica)
- Hash (chiave per algoritmo di hash)

Cliccando sul triangolino presente nel lato destro del riquadro per ogni Attore è possibile nascondere/visualizzare le informazioni di Knowledge.



Nella sezione informativa è presente una **Casella Combinata** (combo box) che permette di effettuare la selezione dell'Attore per il quale inserire le informazioni relative alle chiavi conosciute.



Tramite il pulsante "Disable Server/Enable Server" è possibile eliminare o reintegrare il **Server** tra gli Attori del protocollo. Selezionando "Disable Server" l'Attore Server sarà eliminato e la voce del menù verrà modificata in "Enable Server" per permettere di reintegrare il **Server** tra gli Attori del protocollo.

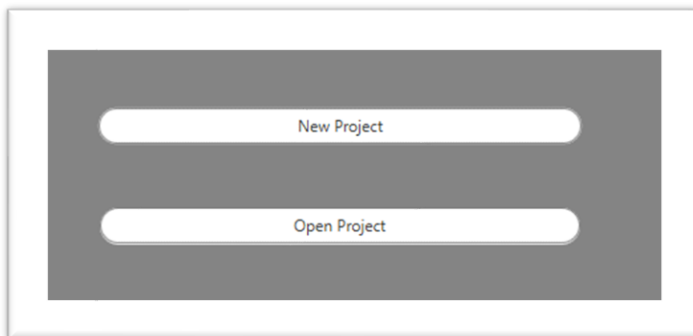
Avvio dell'Applicazione

Quando si avvia l'applicazione AProVer si visualizza una pagina che permette di avviare un nuovo inserimento di dati o modificare le informazioni prelevandole da un file creato in precedenza.



All'avvio la **Sezione Informativa** si presenta Disabilitata. È però possibile selezionare uno dei due pulsanti presenti al centro dell'interfaccia grafica.

Dal menu **Tool** è possibile selezionare l'opzione "**Disable Server**" per eliminare il Server dalla Sezione Informativa.



Cliccando sul pulsante con l'etichetta "**New Project**" si chiude la pagina aprendone una nuova che permetterà di inserire nuovi dati.

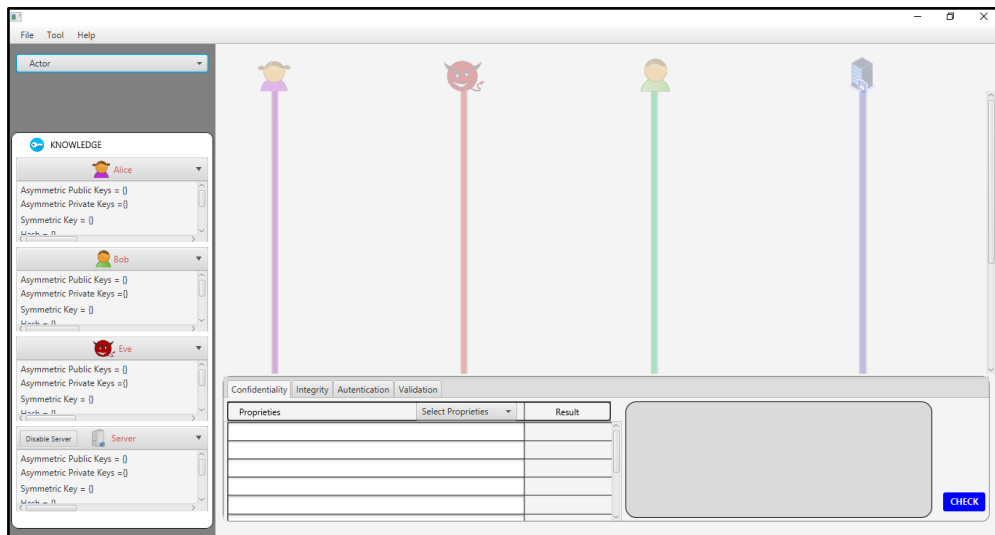
Selezionando il pulsante "**Open Project**" si apre l'applicazione di Esplora Risorse per la ricerca di file con estensione **.avr**

Una volta selezionato il file si chiude la pagina iniziale e si apre una nuova pagina

con i dati contenuti nel file appena selezionato.

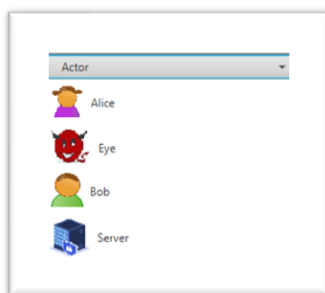
Inserimento Informazioni del Protocollo

La pagina aperta, dopo la scelta dell'opzione di creare un nuovo progetto o aprirne uno progetto già creato, permette di avviare le operazioni di inserimento e modifica delle informazioni del protocollo.

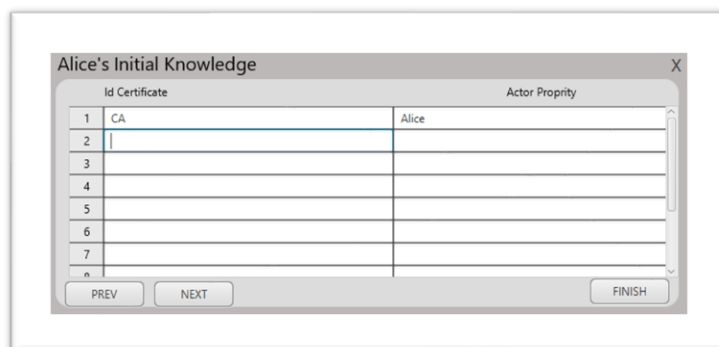


La pagina si compone di quattro sezioni. In alto è presente la **Barra del menu**, a sinistra è possibile visualizzare la **Sezione Informativa**, al centro si visualizzano le icone degli **Attori con le proprie line del tempo**, infine, in basso è presente la **Sezione delle Proprietà di Sicurezza** che dovranno essere verificate sul protocollo.

Inserimento Knowledge



Per configurare le informazioni relative a quali chiavi sono a conoscenza di ogni soggetto coinvolto nel protocollo è necessario **selezionare l'Attore** dalla Casella Combinata (combo box) presente nella Sezione Informazioni.



Dopo aver selezionato l'Attore si apre una nuova sezione composta da varie pagine che permetterà l'inserimento delle informazioni di Knowledge.



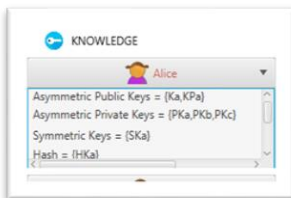
Per passare da una pagina a quella successiva (o precedente) si utilizzano i pulsanti “**Next**” e “**Prev**” presenti in fondo alla sezione.

Con il pulsante “**Finish**” si effettua il salvataggio e la chiusura della finestra.

FINISH

La sequenza delle pagine visualizzate permette di inserire le seguenti tipologie di chiavi e informazioni del payload:

- Asymmetric Public Key (chiave pubblica per crittografia asimmetrica) e corrispettiva Asymmetric Private Key (chiave pubblica per crittografia asimmetrica)
- Symmetric Key (chiave per crittografia simmetrica)
- Hash (chiave per algoritmo di hash)
- Bitstring
- ID Certificate (identificativo del certificato) e Actor Property (attore proprietario del certificato)
- Nonce (identificativo di un numero arbitrario che può essere utilizzato una sola volta)
- Signature Public Key (chiave usata per verificare la firma) e corrispettiva Signature Private Key (chiave usata per firmare digitalmente)
- Timestamp (marca temporale)
- Digest (risultato di funzione hash)




L'applicazione riporterà i dati inseriti in questa fase nella Sezione Informativa.

Al termine dell'inserimento dei Knowledge di **tutti gli Attori** si abiliterà la possibilità di inserire i messaggi del protocollo.

In questa fase è ancora possibile escludere dalla configurazione del protocollo l'Attore Server. Come descritto nel paragrafo relativo alla barra del menu ed in particolare al menu tool è possibile escludere o riattivare l'Attore Server selezionando l'opzione “Disable Server” / “Enable Server”.


Inserimento Messaggi

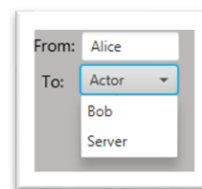
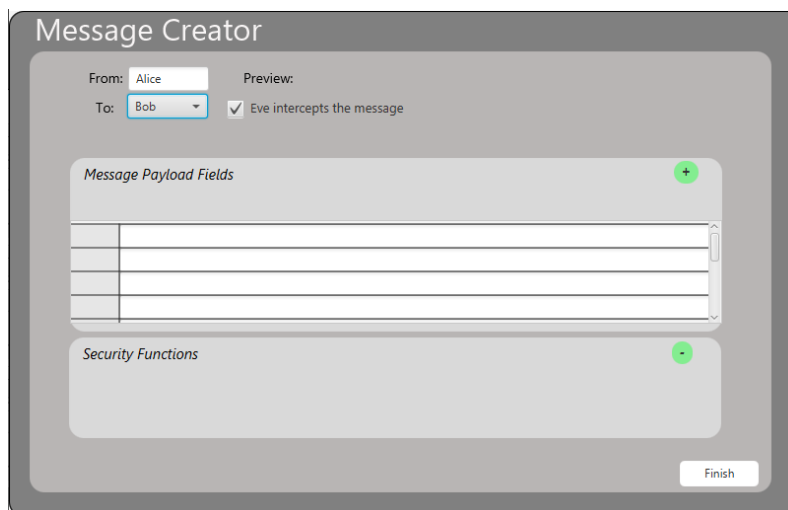
Dopo aver inserito le informazioni di knowledge per tutti gli Attori coinvolti nel protocollo di comunicazione si attiva la possibilità di inserire i messaggi attraverso i pulsanti con il testo “+”  che compaiono sulla **Barra del Tempo** sotto l'icona di ogni singolo attore.



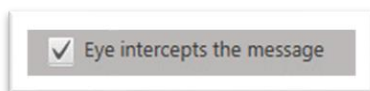
Se il protocollo sul quale si vuole effettuare la verifica non prevede che i messaggi vengano creati o ricevuti direttamente dall'Attore Eye (Attore “Malintenzionato”) è possibile disattivare questa possibilità selezionando l'opzione “Eye Create Messages/Eye Doesn't Create Messages” presente nel menu tool.

L'applicazione imposta di default la disattivazione della creazione dei messaggi da parte dell'Attore Eye.

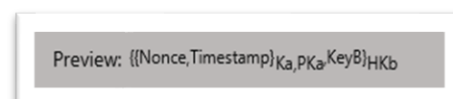
Dopo aver cliccato sul pulsante  si apre la finestra per l'inserimento del Payload del messaggio. La finestra visualizza il nome dell'attore dal quale parte il messaggio (**From**) determinandolo in base a quale pulsante è stato selezionato. È necessario invece selezionare il destinatario del messaggio (**To**) dell'apposita **Casella Combinata** (combo box).

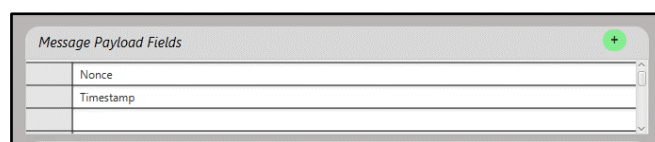
Una delle opzioni che possono essere selezionate nella creazione del messaggio è quella di indicare se l'Eve ha la possibilità di intercettarlo e quindi di verificarne il contenuto. Questo può essere configurato attraverso l'apposita **Casella di Controllo** (check box).




Nella parte alta della finestra l'applicazione visualizzerà il **Preview** del messaggio che viene creato utilizzando le apposite funzionalità descritte in questo paragrafo.



Nella finestra per la creazione del messaggio sono presenti inizialmente due sezioni, una per indicare i campi del payload (**Message Payload Fields**) e l'altra per specificare quale funzione di sicurezza e con quali chiavi applicare (**Security Functions**) ai campi indicati nella prima sezione.



Il messaggio completo (payload) è costruito per fasi in base a come e su quali parti del messaggio applicare le funzioni di sicurezza.

Dopo aver inserito l'elenco dei campi che fanno parte del messaggio si clicca sul pulsante "+"  per passare alla sezione per indicare quale funzione di sicurezza applicare a quel gruppo di campi.

Nella sezione **Security Functions**, cliccando sul pulsante “-” le informazioni dei campi vengono riportate nella sezione dove indicare i campi del payload.

Attraverso l’apposita **Casella Combinata** (combo box) è possibile selezionare le funzioni di sicurezza che verranno applicate alla parte del messaggio appena inserito.

È importante ricordare che le funzioni di sicurezza vengono applicate sequenzialmente in base alla selezione effettuata.

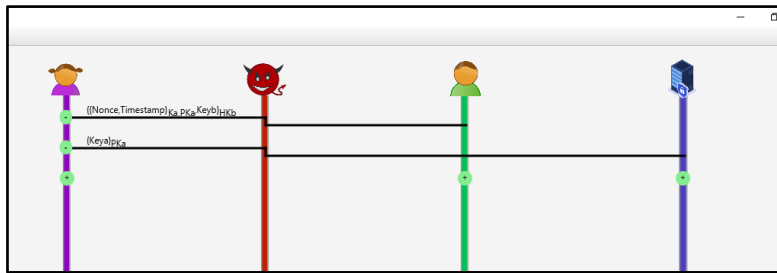
Al termine dell’operazione di assegnazione delle funzioni di sicurezza si clicca il pulsante “**Update Message**” per registrare le informazioni inserite.

Successivamente alla registrazione del primo gruppo di campi si attiva una nuova sezione (**Message Payload Group**) all’interno della finestra.

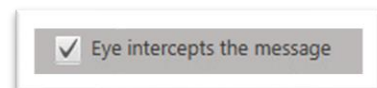
La Message Payload Group è utilizzata per legare parti del messaggio già registrato ad ulteriori nuovi valori; grazie a questa opzione sarà possibile applicare nuove funzioni di sicurezza a tutto il messaggio e non solo alle ultime informazioni inserite.



Successivamente alla chiusura della finestra, effettuata attraverso il pulsante “**Finish**” FINISH l’applicazione visualizza nella “**Barra del Tempo**” una riga che parte dall’Attore che genera il messaggio e termina sull’Attore destinatario.



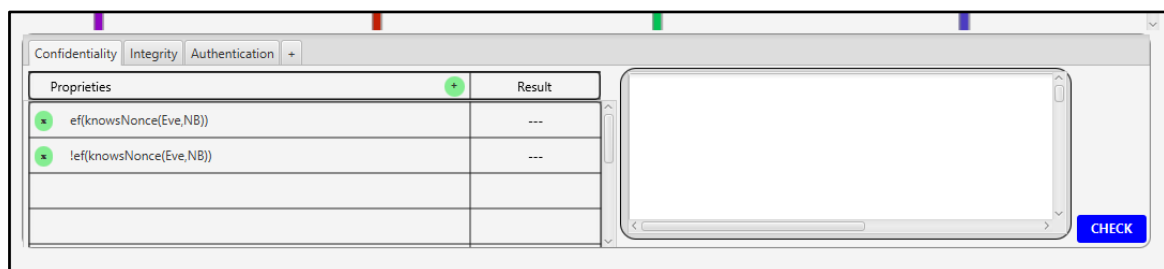
Nella figura è possibile vedere due tipologie diverse di messaggio; nel primo caso il messaggio parte dall'Attore Alice, ha come destinatario BOB ma l'Attore Eye ha la possibilità di vedere il messaggio che transita nella rete; nel secondo caso il messaggio viene generato sempre dall'Attore Alice ma termina al Server senza che l'Attore Eye possa osservarlo. La differenza rispetto alla possibilità che Eye veda o meno il messaggio è dovuta al fatto di aver utilizzato l'opzione **"Eye intercepts the message"** durante la fase di creazione del messaggio



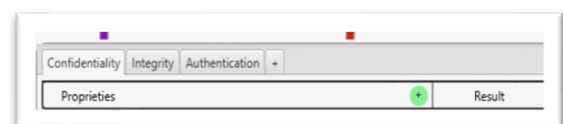
La cancellazione del messaggio avviene cliccando sul pulsante **"-"** presente sulla Barra del Tempo e relativo al messaggio da eliminare.

Verifica delle proprietà

Dopo aver definito tutti i messaggi che si scambiano gli attori tra loro previsti dal protocollo sul quale si vuole effettuare la verifica di sicurezza si procede alla fase di controllo (**Check**).



Si inseriscono le proprietà da verificare all'interno delle varie "Tab" che rappresentano la Confidenzialità, l'integrità e l'Autenticazione; è poi possibile inserire altre proprietà specifiche per il protocollo analizzato.

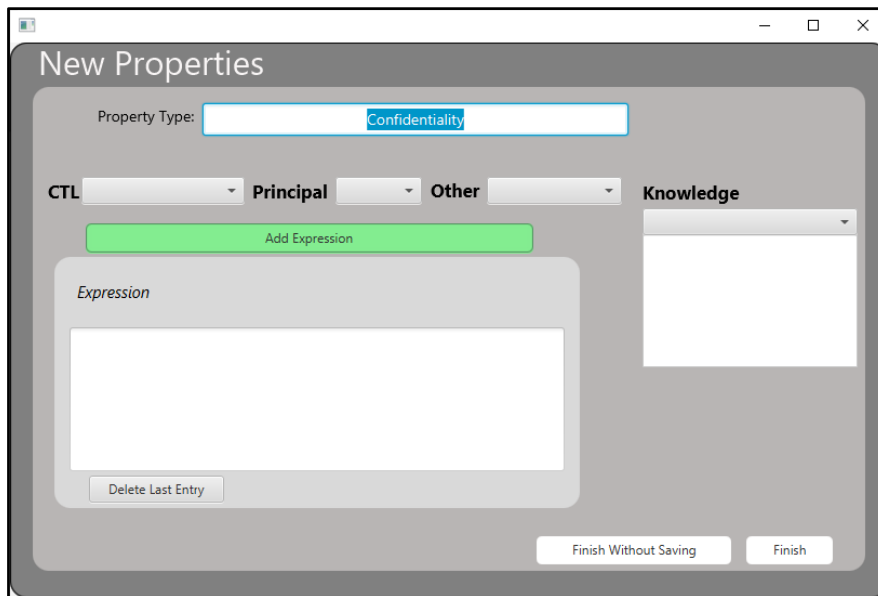


Tramite il pulsante **+** si inseriscono le proprietà del tipo di elemento di sicurezza da verificare.

Nella tabella presente all'interno del tab saranno visualizzate le proprietà inserite, per ognuna di queste, sulla sinistra è presente il pulsante **+** che permette la loro modifica o cancellazione delle stesse.

Inserimento delle proprietà

Le proprietà vengono espresse attraverso il CTL (Computation Tree Logic), un linguaggio formale utilizzato per specificare proprietà temporali dei sistemi reattivi.



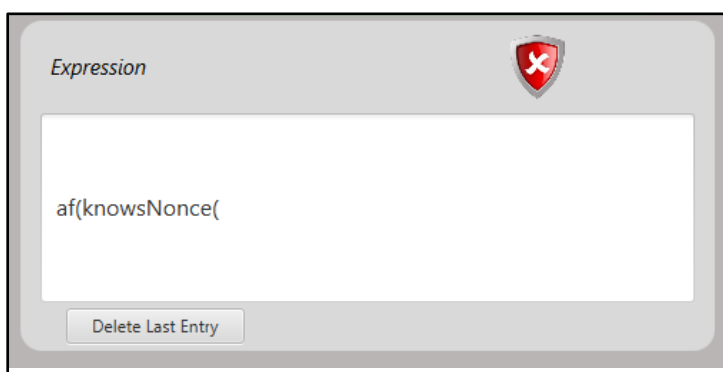
La pagina che permette l'inserimento delle proprietà temporali è composta dall'header dove si trova il nome della proprietà temporale che si vuole verificare. Per le proprietà definite dall'utente deve essere inserito obbligatoriamente il "Property Type".

Sotto l'header ci sono gli elementi che permettono all'utente di costruire le formule delle proprietà temporali.

Una volta selezionato uno solo degli elementi l'utente deve aggiornare l'espressione cliccando sul pulsante "Add Expression".



Ogni volta che viene selezionato il pulsante "Add Expression" si aggiorna il riquadro che contiene l'espressione"



L'applicazione effettua un controllo formale sull'espressione e indica il risultato della verifica attraverso due icone distinte:



il controllo ha dato esito negativo



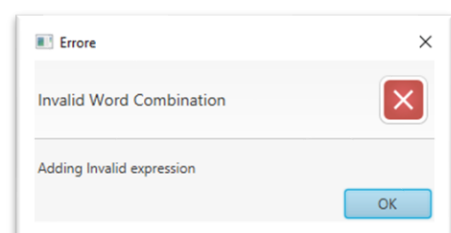
il controllo ha dato esito positivo

la verifica che viene effettuato è esclusivamente sulla correttezza dell'uso delle parentesi mentre alcune combinazioni di caratteri viene impedita nel momento dell'inserimento.

Un esempio di combinazione non valida è "(").

Cliccando sul pulsante "Delete Last Entry" si elimina l'ultimo inserimento effettuato.

Tra le cose che possono essere inserite all'interno dell'espressione si hanno i quantificatori e gli operatori temporali che sono utilizzati per specificare la validità delle proprietà rispetto a tutti i possibili percorsi o solo ad alcuni di essi.



L'applicazione permette di inserire i principali operatori temporali delle CTL:

- X (next): rappresenta il prossimo stato.
- F (eventually): rappresenta che una certa proprietà deve verificarsi in futuro.
- G (globally): rappresenta che una certa proprietà deve essere valida in tutti i futuri stati.

Gli operatori temporali sono abbinati ai due quantificatori e alla loro negazione:

- A (for all): rappresenta che una certa proprietà deve valere per tutti i percorsi.
- E (exists): rappresenta che una certa proprietà deve valere per almeno un percorso.
- !A (for all): rappresenta che una certa proprietà NON deve valere per tutti i percorsi.
- !E (exists): rappresenta che una certa proprietà NON deve valere per almeno un percorso.

Attraverso il menu a tendina "Principale" è possibile selezionare l'attore da inserire nell'espressione che dovrà essere verificata.

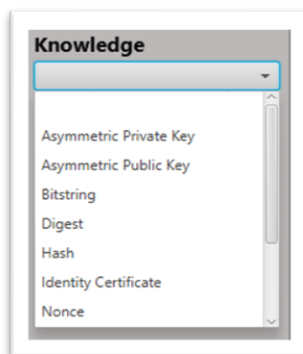
Il menu a tendina "Other" permette di selezionare gli operatori booleani, i tipi di conoscenze verificabili e i segni di punteggiatura.

Gli operatori booleani selezionabili sono nel menu a tendina "Other":

- AND (\wedge): congiunzione di espressioni; restituisce un valore vero solo se entrambe le espressioni che collega sono vere;
- OR (\vee): restituisce un valore vero se almeno una delle due espressioni che collega è vera.
- ! (\neg): negazione (NOT) restituisce un valore vero se l'espressione (o il gruppo di espressioni) sono false.

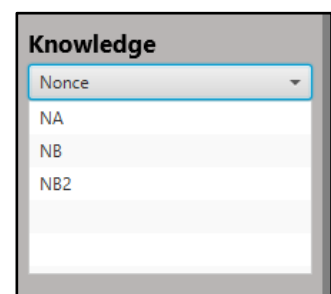
I tipi di conoscenze inseribili nell'espressione:

- knowsNonce
- knowsAsymPubKey
- knowsSymKey
- knowsIdentityCertificate
- knowsBitString
- knowsAsymPrivKey
- knowsSignPubKey
- knowsSignPrivKey
- knowsTag
- knowsDigest
- knowsHash
- knowsTimestamp
- knowsOther



Altra componente dell'espressione che può essere inserita nell'espressione è quella delle componenti del payload.

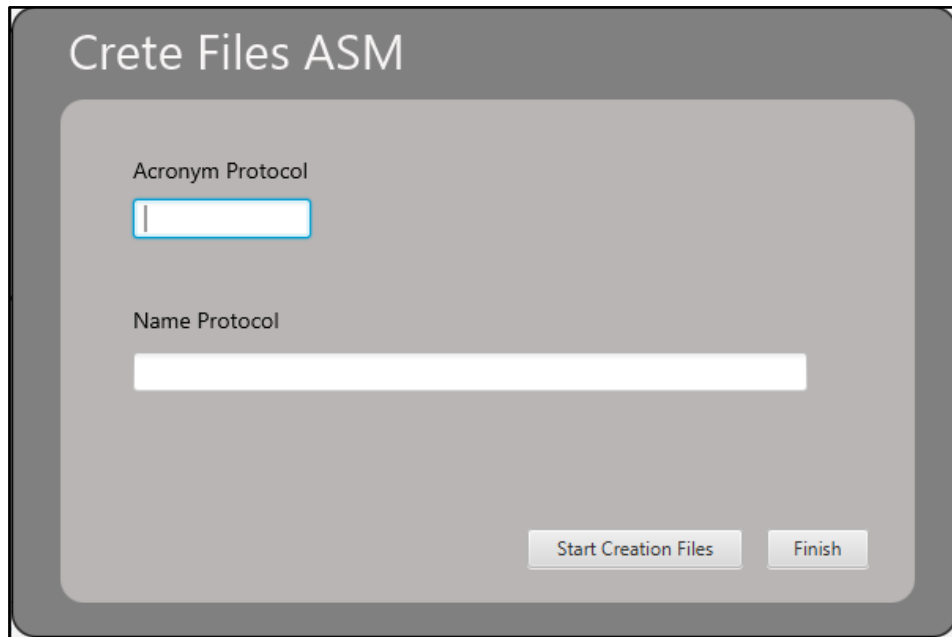
Attraverso l'apposito menu si seleziona il tipo di dato che si vuole inserire nell'espressione e successivamente si seleziona il campo desiderato.



Al termine dell'inserimento dell'espressione si conferma utilizzando il pulsante "Finish" o annullando l'inserimento con il pulsante "Finish Without Saving".

Generazione della macchina virtuale (ASM)

Attraverso il pulsante “*Check*” è possibile generare un file contenente il programma scritto in AsmL (Abstract State Machine Language) che modella il protocollo disegnato con l’applicazione.



Crete Files ASM

Acronym Protocol

Name Protocol

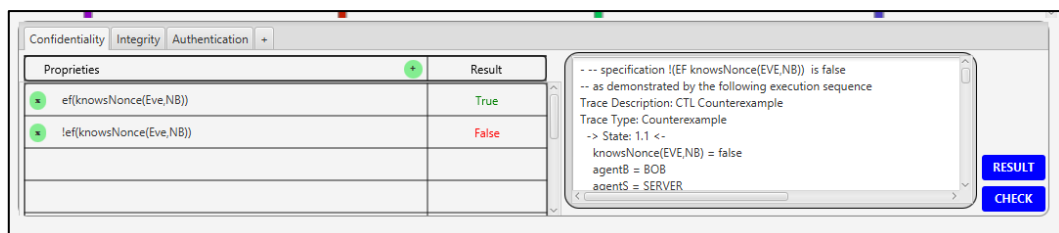
Start Creation Files Finish

Nella pagina che compare dopo aver premuto il pulsante “*Check*” devono essere inseriti l’acronimo e il nome del protocollo. Queste informazioni sono utilizzate dall’applicazione per generare i due file che rappresentano il modello ASM del protocollo.

Dopo aver inserito le due informazioni si genera il file cliccando sul pulsante “*Start Creation File*” e si esce dalla pagina cliccando “*Finish*”.

Caricamento Risultato elaborazione


Dopo aver generato e successivamente eseguito la macchina virtuale è possibile caricare le informazioni della console contenente il risultato dell’elaborazione.



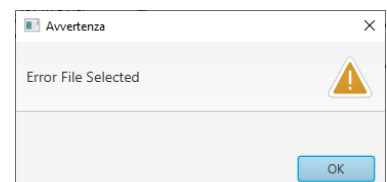
Proprieties	Result
ef(knowsNonce(Eve,NB))	True
!ef(knowsNonce(Eve,NB))	False

--- specification !(EF knowsNonce(Eve,NB)) is false
-- as demonstrated by the following execution sequence
Trace Description: CTL Counterexample
Trace Type: Counterexample
-> State: 1.1 <-
knowsNonce(Eve,NB) = false
agentB = BOB
agentS = SERVER

RESULT CHECK

Attraverso il bottone “*Result*”  si procede alla selezione del file di tipo testo contenente il risultato dell’elaborazione.

Qualora si dovesse essere selezionato un file errato l’applicazione segnala l’errore.



Dopo che il file è stato acquisito l'applicazione visualizza il risultato (True o False) associato ad ogni proprietà inserita.

Cliccando sul risultato è possibile visualizzare il dettaglio della console con i dati dell'elaborazione.

