UNIVERSITÀ DEGLI STUDI DI "ROMA TRE"
FACOLTÀ DI S.M.F.N.

Sintesi della tesi di Laurea in Matematica
di

Rosa Angela Prestileo

Metodi formali per lo studio dei protocolli crittografici

Relatore

Prof. Alberto Berretti

ANNO ACCADEMICO 2001 - 2002

Luglio 2002

Classificazione AMS: 94A60, 03B42, 94A62;

Parole chiave: Protocolli crittografici, metodi formali, BAN Logic, UEPS.

Sintesi

La storia dell'applicazione dei metodi formali all'analisi dei protocolli crittografici abbraccia quasi vent'anni e recentemente ha mostrato segni di nuova maturità e consolidamento: sono stati sviluppati un certo numero di strumenti specifici ed altri sono stati efficacemente utilizzati per dimostrare che quelli attuali, a scopo generale, possono essere applicati a tali problemi con buoni risultati. Tuttavia, questa migliore conoscenza del settore fa nascere nuove problematiche forzando i limiti degli strumenti attuali che vengono, principalmente, applicati al problema di stabilire se una chiave è stata correttamente autenticata.

Ma ora che si stanno adattando i protocolli crittografici a nuovi tipi di esigenze, quali la comunicazione di gruppo, operazioni finanziarie, trattative di algoritmi e di chiavi, ci si trova, anche, ad affrontare nuovi tipi di problemi, come il *Denial of Service*[1] e le più vecchie minacce, che stanno diventando sempre più preoccupanti e che, in molti casi, gli strumenti attuali non riescono a gestire.

[1]Un attacco DoS impedisce, ad un calcolatore o all'utente di una rete, di accedere a determinate risorse, ad esempio, e-mail ed Internet. Si può effettuare un tale tipo di attacco tentando di intasare la rete.

I protocolli crittografici sono protocolli che fanno uso della crittografia. Essi nascono per consentire ad agenti di rete di comunicare tra loro:

1. *IN MODO INTRINSECAMENTE SICURO:*
   sono due le proprietà, evidenziate dalla letteratura sull'argomento, richieste
   - Segretezza(Secrecy, Confidentiality)
   - Autenticità(Authentication)
2. *SU UNA RETE INTRINSECAMENTE NON SICURA:*
   ciò che viene scambiato tra gli agenti accreditati alla comunicazione può essere utilizzato da ulteriori agenti non autorizzati esplicitamente (INTRUDERS o ATTACKERS)
   - per impadronirsi di informazioni
   - per inserirsi nella comunicazione

In un sistema distribuito, l'autenticazione è il processo attraverso il quale un agente (che può essere una persona, un computer o un server) prova la sua identità; tipicamente, ognuno di essi condivide un segreto con qualche meccanismo del quale si fida, chiamato server di autenticazione, e provando il possesso di questo segreto riescono a dimostrare la veridicità della loro identità.
Un esempio, di quanto appena detto, è l'uso della password in una situazione di multiutenza.
Generalmente, in un sistema di autenticazione, il segreto comune viene utilizzato come chiave di codifica il cui schema ha la proprietà che un utente non

può generare o decodificare messaggi crittati senza il possesso della chiave.
In un vasto sistema distribuito, l'autenticazione è un processo "provocatorio" poiché gli agenti comunicano su una rete vulnerabile a molteplici attacchi. Un intruder passivo può inserirsi, di nascosto, su una linea ed ottenere informazioni riservate; di più gravi conseguenze è l'intruder attivo che può modificare il processo del messaggio bloccando la trasmissione dei pacchetti ed inserendo i suoi. Un intruder può, perfino, fingere di essere un agente intercettando, così, tutti i suoi diritti e privilegi. L'operazione di codifica può ostacolare gli attacchi di un intruder attivo; difatti, molti schemi di codifica preservano la proprietà d'integrità nel senso che se qualche dato viene modificato allora la decodifica fallisce.
La maggior parte dei sistemi di autenticazione usati nella pratica sono simmetrici, cioè viene usata la stessa chiave per i processi di codifica e decodifica; quando due agenti vogliono comunicare, stabiliscono una chiave segreta che, essendo nota solo a loro, permette di instaurare un sicuro canale di comunicazione poiché un intruder attivo, che non conosce la chiave, non può interferire, con successo, nella loro comunicazione. In ogni caso, il problema di stabilire una tale chiave, chiamata chiave di sessione, è sicuramente non banale ed ha comportato una notevole quantità di ricerca che si focalizza sullo sviluppo dei protocolli ed è accompagnata da un più grande e interessante problema: l'analisi dei protocolli di autenticazione che sono, appunto, la descrizione di come questi segreti vengono distribuiti agli agenti e come essi li utilizzano per provare la loro identità.

Per queste ragioni si è pensato che i metodi formali potevano essere un

utile strumento per analizzare la sicurezza dei protocolli crittografici. Tali metodi consentono:

- di fare un'accurata analisi dei differenti percorsi che un intruder può intraprendere;
- di specificare precisamente le assunzioni ambientali che sono state fatte.

Esistono diversi approcci per quanto riguarda l'applicazione dei metodi formali all'analisi di un protocollo di autenticazione. Usiamo lo schema di classificazione presentato da Meadows e suddiviso in quattro tipi:

I TIPO Modella e verifica un protocollo usando linguaggi di specificazione e strumenti di verifica non appositamente sviluppati per l'analisi dei protocolli crittografici.

II TIPO Sviluppa esperti sistemi che un progettista di protocolli può utilizzare per ampliare ed investigare diversi scenari dai quali può trarre conclusioni riguardanti la sicurezza dei protocolli che devono essere studiati.

III TIPO Modella e verifica un protocollo usando logiche appositamente sviluppate per l'analisi di conoscenza e credenza.

IV TIPO Sviluppa un metodo formale basato sulle proprietà algebriche term-rewriting dei sistemi crittografici.

Probabilmente, la prima menzione di metodi formali, come un possibile strumento per l'analisi dei protocolli crittografici, è dovuta a Needham e

Schroeder; tuttavia, il primo lavoro realmente portato a termine, in questa area, è stato fatto da Dolev e Yao e poco dopo da Dolev, Even e Karp che hanno sviluppato un insieme di algoritmi a tempo polinomiale per stabilire la sicurezza di una ristretta classe di protocolli. Sfortunatamente, però, è stato ben presto scoperto che riducendo le restrizioni sui protocolli, anche di poco, il problema della sicurezza non era di facile soluzione, rendendosi conto che il lavoro fatto fino a quel momento non poteva spingersi oltre.
Tuttavia, il lavoro di Dolev e Yao ha avuto una certa rilevanza, se non altro per aver sviluppato un modello formale di un ambiente nel quale:

- possono essere eseguite, simultaneamente, molteplici esecuzioni del protocollo;
- gli algoritmi crittografici si comportano come scatole nere che obbediscono ad un insieme limitato di proprietà algebriche;
- un intruder può leggere, alterare, distruggere il traffico e perfino controllare alcuni membri legittimi del sistema.

Successivamente, il lavoro sull'analisi formale dei protocolli crittografici ha fatto riferimento a questo modello o a qualche sua variante, inclusi l'Interrogator, l'NRL Protocol Analyzer ed il sistema di Longley-Rigby. La maggior parte di questo lavoro ha utilizzato un certo tipo di tecnica di esplorazione degli stati: viene definito uno spazio di stato e successivamente esplorato dallo strumento per determinare l'esistenza di percorsi, all'interno dello spazio, corrispondenti ad un attacco da parte dell'intruder.
Tuttavia, quest'area è rimasta abbastanza misteriosa almeno fino a quando

viene pubblicata, nel 1989, la logica di Burrows, Abadi e Needham (BAN Logic), momento in cui, il problema dell'analisi formale di un protocollo crittografico richiama l'attenzione di una più grande comunità di ricerca. La logica di Burrows, Abadi e Needham usa un approccio molto differente da quello degli strumenti d'esplorazione degli stati; essa è un esempio di una logica di conoscenza e credenza, che consiste in un insieme di possibili credenze possedute dagli agenti, ed un insieme di regole d'inferenza per derivare nuove credenze da quelle vecchie. Inoltre, il metodo convenzionale per descrivere un protocollo, elencando simbolicamente la sorgente, la destinazione ed i contenuti, viene sostituito da formule logiche. Tale rappresentazione mira a formulare ogni singolo step del protocollo in modo da poter visualizzare le informazioni essenziali. Questo processo va sotto il nome di *idealizzazione* del protocollo, il quale, viene successivamente *annotato* con asserzioni che, generalmente descrivono le credenze degli agenti in quel punto del protocollo. Allo stesso tempo, il protocollo viene analizzato passo dopo passo usando un insieme di *regole di inferenza*, che abbiamo ampiamente descritto nel capitolo 3 della tesi. Durante il processo di idealizzazione, il protocollo è rappresentato tramite degli step, ognuno dei quali include il mittente ed il destinatario di quel messaggio. Una tipica rappresentazione, per uno step di un protocollo, è la seguente:

$$A \rightarrow B : \{A, K_{ab}\}_{K_{bs}}$$

Questa scrittura denota il fatto che l'agente A spedisce il messaggio $\{A, K_{ab}\}$ codificato con la chiave K_{bs} e che B lo riceve; se, quest'ultimo, conosce la chiave K_{bs}, il messaggio gli suggerisce che K_{ab} è una chiave per comunicare

con A. Lo step idealizzato procede come segue:

$$A \rightarrow B : \left\{ A \overset{K_{ab}}{\leftrightarrow} B \right\}_{K_{bs}}$$

Questo significa che A spedisce e B riceve un messaggio codificato con una chiave comune K_{bs}. Il messaggio stesso include una chiave comune K_{ab} che solo A e B possono utilizzare. Quando il messaggio viene spedito a B, può essere dedotto che

$$B \triangleleft \left\{ A \overset{K_{ab}}{\leftrightarrow} B \right\}_{K_{bs}}$$

ed indica che il destinatario è al corrente del messaggio (B vede il messaggio) e può agire su di esso.

Lo scopo dell'idealizzazione è di omettere le parti di un messaggio che non contribuiscono alle credenze del destinatario. In BAN Logic, un protocollo idealizzato omette le parti di testo in chiaro, in quanto, non essendo protette dalla codifica, possono essere manomesse e pertanto non danno alcun contributo all'autenticazione.

Per quanto riguarda l'analisi del protocollo, in BAN Logic, essa si divide nei quattro seguenti passi:

- il protocollo idealizzato è derivato da quello originale;
- vengono scritte le assunzioni riguardo lo stato iniziale;
- vengono assegnate delle formule logiche alle dichiarazioni del protocollo sottoforma di asserzioni riguardanti lo stato del sistema dopo ogni dichiarazione;
- vengono applicate le regole di inferenza alle assunzioni ed alle asserzioni per indagare sulle credenze possedute dalle parti nel protocollo.

Il traguardo raggiunto dagli autori, grazie a questo modello logico, è stato quello di esere in grado a rispondere a molteplici domande sui protocolli, quali:

- Cosa realizza tale protocollo?
- Questo protocollo ha bisogno di più assunzioni rispetto ad un altro?
- Durante l'esecuzione del protocollo vengono eseguiti degli step superflui che potrebbero essere omessi senza danneggiarlo?
- Questo protocollo codifica un messaggio che potrebbe essere spedito in chiaro senza comprometterne la sicurezza?

Gli autori specificano, inoltre, che problemi come gli errori introdotti da implementazioni concrete di un protocollo o l'uso inappropriato di un crittosistema non vengono considerati; tale sistema si occupa dei protocolli di autenticazione solo su un livello astratto.

Nel quarto, ed ultimo, capitolo della tesi abbiamo applicato il modello logico di Burrows, Abadi e Needham al sistema di pagamento UEPS, con particolare riferimento al protocollo di transazione, che viene utilizzato per accertare l'integrità di ogni step del percorso del contante: dalla banca al cliente, al rivenditore, al compensatore e, infine, nuovamente alla banca.
UEPS è stato progettato nel 1991 dalla casa di sistemi Net One per il suo cliente, la Permanent Building Society di Johannesburg, ed implementato quello stesso anno. Il suo scopo è stato quello di estendere i moderni servizi

bancari, a basso costo, alla popolazione del Sud Africa dove, le difficili telecomunicazioni rendono necessarie le operazioni offline. UEPS sfrutta una smartcard preprogrammata con la funzione di portafoglio elettronico: il denaro viene "caricato" sulla carta del cliente, del rivenditore ed, infine, ritornato alla banca attraverso un sistema di compensazione. La smartcard ha un microprocessore a circuito integrato(chip) fissato su un supporto di plastica.
La sicurezza di UEPS è basata su due livelli di autenticazione. Lo strumento base di pagamento è un assegno elettronico che viene generato dalla carta cliente. L'assegno ha due codici di autenticazione: uno generato con una chiave nota soltanto all'emittente del modulo di sicurezza della banca ed alla carta cliente, ed uno generato con una chiave controllata da una "clearing house" (stanza di compensazione) e caricata sulla carta prima che venga fornita alla banca. L'ultimo codice viene controllato prima che i fondi monetari siano accreditati al rivenditore che presenta l'assegno, mentre il primo viene controllato solo in caso di controversie.
La transazione di acquisto può essere idealizzata come segue:

$$C \to R : \{C, N_C\}_K \qquad (= L)$$

$$R \to C : \{R, N_R\}_L \qquad (= M)$$

$$C \to R : \{X\}_M$$

Tale protocollo ha la robusta proprietà che tutte le reciproche informazioni tra le due parti vengono rese esplicite essendo state inserite dentro le chiavi del messaggio. In effetti, il prodotto intermedio di ogni doppia codifica viene utilizzato come seconda chiave nella codifica successiva. In questo modo, ogni

blocco funge da autenticatore per tutti i messaggi precedenti del protocollo e l'informazione può essere scambiata efficientemente. Per validare il protocollo si è dovuto, però, considerare uno semplificato dove l'informazione viene accumulata senza concatenamento:

$$C \rightarrow R : \{C, N_C\}_K$$

$$R \rightarrow C : \{R, N_R, C, N_C\}_K$$

$$C \rightarrow R : \{C, N_C, R, N_R, X\}_K$$

Questo può essere analizzato in modo diretto usando BAN Logic. Il trucco è di iniziare dal risultato voluto e lavorare a ritroso; in questo caso vogliamo dimostrare che il rivenditore si fida dell'assegno, cioè $R \models X$ (in questo contesto e, per il nostro scopo, la sintassi di assegno e chiave crittografica è simile).

Anche se in minima parte, il successo di UEPS è dovuto al fatto di aver utilizzato i metodi formali per verificare il relativo prototipo; difatti, oltre agli effetti commerciali che BAN Logic ha determinato sul prodotto, e di conseguenza all'interno dell'industria bancaria, ci sono stati notevoli benefici scientifici. Abbiamo visto che BAN Logic non si limita a verificare la mutua autenticazione e lo scambio delle chiavi, ma è anche uno strumento utile e pratico per il design di un protocollo crittografico efficiente. Qual è stato l'effetto? Aver fornito stimoli intellettuali di una certa portata a progettisti e programmatori ed aver rafforzato, notevolmente, la fiducia dei clienti nei confronti del sistema.

Bibliografia

[1] Net1 ueps version 10. da URL: http://www.aplitec.co.za/aplitec/ueps.

[2] M. Abadi and R.M. Needham. Prudent engineering practice for cryptographic protocols. DEC SRC Research Report n° 125, 1994.

[3] R.J. Anderson. Papers on smartcard engineering. Technical report, University Computer Laboratory,University of Cambridge.

[4] R.J. Anderson. Ueps-a second generation electronic wallet. In *Computer Security-ESORICS 92*, volume 648 of *LNCS*, pages 411–418, 1992.

[5] R.J. Anderson. Why cryptosystem fail. In *Communications of the ACM*, volume 37, pages 32–40, november 1994.

[6] R.J. Anderson. The formal verification of a payment system, 1997. Computer Laboratory, University of Cambridge.

[7] R.J. Anderson and R.M. Needham. Programming satan's computer. In *Computer science today*, volume 1000, pages 426–441. Springer LNCS.

[8] M. Burrows, M. Abadi, and R.M. Needham. A logic of authentication. In *Proceedings of the Royal Society of London*, volume 426, pages 233–271, 1989.

[9] O. Fadiran Oladipo. Smartcards: smart security? da URL: http//rrsg.ee.uct.ac.za/fadiran/smartcard.pdf.

[10] R. Kemmer, C. Meadows, and J. Millen. Three systems for cryptographic protocol analysis. In *Journal of Cryptology*, volume 7, pages 79–130, 1994.

[11] C. Meadows. Open issues in formal methods for cryptographic protocol analysis. *Lecture Notes in Computer Science*, vol. 2052, 2001.

[12] A.D. Rubin and P. Honeyman. Formal methods for the analysis of authentication protocols. CITI Technical report 93-7, 1993.

[13] B. Schneier. *Applied Cryptography.* John Wiley and Sons, second edition, 1996.