APPLYING FORMAL METHODS TO CRYPTOGRAPHIC PROTOCOL ANALYSIS: EMERGING ISSUES AND TRENDS

Catherine Meadows
Code 5543
Center for High Assurance Computer Systems
US Naval Research Laboratory
Washington, DC 20375
meadows@itd.nrl.navy.mil
http://chacs.nrl.navy.mil
A cryptographic protocol is a communication protocol that uses encryption to:
- Distribute keys
- Authenticate principals
- Process transactions securely

Must operate in hostile environment in which traffic may be intercepted, altered or destroyed

Distributed programs are hard to design; distributed programs running in hostile environments are harder

One way of addressing problem: develop automated techniques for the analysis of cryptographic protocols
EXAMPLE: CCITT DRAFT STANDARD X.509 (1987)

• A and B want to verify origin and recency of messages

• Protocol uses public key crypto

  – A and B possess public keys $K_A$ and $K_B$, private keys $K_A^{-1}$ and $K_B^{-1}$
  – Anyone can send $K_A[X]$ to A, only A can read $X$
  – If A sends $K_A^{-1}[X]$, anyone can compute $K_A[K_A^{-1}[X]] = X$ and verify $X$ came from A

• A and B both have the capacity to generate nonces

  – A generates a nonce $N$ (random number) and sends it to B
  – B returns $K_B^{-1}[X,N]$
  – A knows B sent $X$ after A created $N$
THE PROTOCOL (simplified)

Bob knows third message is recent
Third message appears to be linked to second by \(N_B\)
Second message appears to be linked to first by \(N_A\)

Is this enough?
NO! (Burrows, Abadi, Needham, 1989)

Intruder causes A to initiate communication with it

A, $K_A^{-1}[N_A,B,X_A]$
(Old message from A)

B, $K_B^{-1}[N_B,A,N_A,X_B]$

A, $K_A^{-1}[N'_A,I,X'_A]$

I, $K_i^{-1}[N_B,A,N'_A,X_i]$

$K_A^{-1}[N_B]$

$K_A^{-1}[N_B]$
MAIN TECHNIQUES USED

- Theorem proving
  - State properties of protocols as theorems to be proved
  - Prove or check proofs automatically

- Model Checking
  - Two components
    - A finite state system
    - A specification of properties (typically stated in temporal logic) that the system must satisfy
  - Exhaustively search the state space to determine whether or not properties always satisfied

- A combination seems to work best for crypto protocols
  - Benefits of theorem proving
    - Crypto protocols are infinite state systems
    - Inductive theorem proving helps to reduce infinite state space to a finite one
  - Benefits of model checking
    - Exhaustive search finds attacks if they exist
    - Usually more informative than inability to prove a security property
SOME ISSUES

• Incorporating cryptographic notions of correctness into security proofs
  – What properties do you need to be able to prove about the encryption functions a protocol uses?

• Protocols with unbounded number of participants
  – E.g. group key distribution protocols

• Probabilistic behavior of protocols
  – Some protocols designed to decrease probability of successful attack
    • Protocols designed to resist traffic analysis
    • Protocols designed to resist denial of service attack

• Scaling up, responding to change, etc.

• Much good work being done on these topics
IN WHAT WAYS CAN CRYPTOGRAPHIC PROTOCOLS INCREASE TRUST IN A SYSTEM

They can guarantee that communication is kept secret
   Keys only distributed to principals that are supposed to have them

They can guarantee that communication is authenticated
   A message is from who it says its from, and it was sent in the declared context

They can guarantee some other properties as well
   Resistance to traffic analysis (hide source and destination from outsiders)
   Resistance to denial-of-service attacks

Much of formal analysis of cryptographic protocols consists of precisely formulating and verifying these properties
WHAT CRYPTOGRAPHIC PROTOCOLS CAN’T DO

• Can’t guarantee that entities sending and receiving data are themselves trustworthy
• Can’t provide any guarantees about what is done with data once it is received
• Can’t guarantee even that there is any coherent policy for handling data

All these can be only guaranteed by an analysis of the system as a whole
QUESTIONS ABOUT CRYPTOGRAPHIC PROTOCOL ANALYSIS AND SYSTEM TRUST

- **Given**
  - A distributed system that uses cryptographic protocols to communicate
  - A particular policy that that system must enforce

- **How**
  - Do you derive the security properties that the cryptographic protocols must satisfy?
  - Do you prove that these security properties hold?
  - Do you decide what are the responsibilities of the protocol and what are the responsibilities of other parts of the system?

- **In short, how do you integrate cryptographic protocol analysis into secure system analysis as a whole?**