A Formal Specification and Verification Framework for Timed Security Protocols

ABSTRACT

Time is a double edged sword for security protocols. On one hand, time, as a globally shared measurement, provides a simple way to synchronize and coordinate multiple processes. Thus, it is used in many security protocols as a powerful tool. For instance, distance bounding protocols, use transmission time to measure the distance between protocol participants; interactive protocols limit the lifetime of messages to achieve better security. In fact, timeout is used almost universally in practice. On the other hand, time also introduces a range of attack surfaces. For instance, a security protocol, whose correctness heavily relies on time, could be broken if the expected timing coordination is compromised; or given a session key with limited lifetime, the adversary might be able to extend its lifetime without proper authorization.

EXISTING SYSTEM

In Existing System, protocols often use time to provide better security. For instance, critical credentials are often associated with expiry dates in system designs. However, using time correctly in protocol design is challenging, due to the lack of time related formal specification and verification techniques. Thus, we propose a comprehensive analysis framework to formally specify as well as automatically verify timed security protocols. A parameterized method is introduced in our framework to handle timing parameters whose values cannot be decided in the protocol design stage.

DIS ADVANTAGES

- The critical information is leaked.
- Message transmission delay.

PROPOSED SYSTEM

In Proposed System, we first propose timed applied calculus as a formal language for specifying timed security protocols. It supports modeling of continuous time as well as application of cryptographic functions. Then, we define its formal semantics based on timed

logic rules, which facilitates efficient verification against various authentication and secrecy properties. Given a parameterized security protocol, our method either produces a constraint on the timing parameters which guarantees the security property satisfied by the protocol, or reports an attack that works for any parameter value. The correctness of our verification algorithm has been formally proved. We evaluate our framework with multiple timed and untimed security protocols and successfully find a previously unknown timing attack in Kerberos V.

ADVANTAGES

- Lifetime of messages to achieve better security.
- Reducing system execution time.

SYSTEM REQUIREMENTS

H/W System Configuration:-

Processor	-	Pentium –III
RAM	-	256 MB (min)
Hard Disk	-	20 GB
Key Board	-	Standard Windows Keyboard
Mouse	-	Two or Three Button Mouse
Monitor	-	SVGA

S/W System Configuration:-

Operating System	:	Windows95/98/2000/XP
Application Server	:	Tomcat5.0/6.X
Front End	:	HTML, Jsp
Scripts	:	JavaScript.
Server side Script	:	Java Server Pages.

Database : MySQL 5.0

Database Connectivity : JDBC