Opening and Closing Problems in Security Protocols Research

Simon S. Lam
Department of Computer Sciences
The University of Texas at Austin
Baseball analogy

- Baseball pitchers
  - starters
  - middle relievers
  - closers

- A line of research is like a baseball game with starters, middle relievers, and closers

- But unlike baseball games,
  - lines of research in an area are related and form a tree
  - a middle reliever can become a closer or starter during a “game”
Authentication protocols for computer networks

- Starter: Needham and Schroeder protocols (1978)
  - public key crypto (Diffie and Hellman, 1976)
  - authentication and secrecy concerns

- Two lines of ensuing research
  - verification of security protocols
  - design and implementation of authentication services
Verification of security protocols

- Starter: Dolev and Yao (1981)
  - secrecy concerns only

- Starter: BAN logic (1989)
  - authentication concerns
    - e.g., after authentication, two principals believe that they are communicating with each other and not with intruders

- More on BAN logic
  - high level of abstraction
  - protocol idealization—potentially large semantic gap
  - secrecy concerns not addressed
Verification—middle relievers

... (numerous)

- **Woo-Lam protocol model (1993)**
  - state transition semantics
  - formalize authentication as well as secrecy properties
  
  
  correspondence assertion:  \( X \leftarrowarrow Y \)

  if event \( X \) occurs, then event \( Y \) must have occurred in the past

- **CMU model checker for security protocols (1997)**

  ...

  (game in progress)
Authentication service for client-server Internet applications

- Starter: Kerberos (MIT, 1988)
  - also a closer: used in ftp, rcp, rlogin, ssh, ...

- Middle relievers:
  - SPX (DEC, 1991)
  - KryptoKnight (IBM, 1992)
  - GSS-API (1993)
  - ...

- Disadvantage:
  - each system has its own user interface
  - applications need to work with "low-level" security concepts

- “Kerberizing an application is the most difficult part of installing Kerberos.”
The accidental closer

SNP (1993), the first secure sockets layer
- demonstrated to NSA, 1993
- USENIX conference, June 1994

- Idea: clean separation of concerns—application programmer does not need to deal with security operations

- Goal: “toward secure network programming for the masses”
Secure Network Programming

- Easy to use and to retrofit
  - Secure sockets interface very similar to sockets interface
  - Only minor, mostly syntactic, modifications are needed to convert an application’s socket program into a secure network program

- For most socket calls,
  - connect() → snp_connect()
  - accept() → snp_accept()
  - write() → snp_write()
  - read() → snp_read()
  - shutdown() → snp_shutdown()
  - ...

- Only new call necessary is snp_attach() for application to provide credentials to support its claim of identity
Historical context

- November 1992, only 26 reasonably reliable www servers exist
- October 1993, over 200 www servers in the world
- February 1993, first Alpha release of Mosaic for X browser
- April 1994, Netscape founded
- October 1994, Beta release of Netscape browser
- E-commerce (circa 1995)
What are some new concerns?

- By mid 1990s, protocol design to address client-server authentication and secrecy concerns understood.

- Our new concerns: efficiency, latency, and scalability of security protocols to keep up with Internet’s growth.
  - multicast to large groups
  - real-time packet flows (multimedia)
  - high-speed transmissions
Problems we opened

- Secure group communications
  - Scalable key server using Key Tree approach (WGL 1998)
  - Scalable and reliable transport protocol for group rekeying
    - IP multicast or broadcast (ZLLY 2001)
    - Application-layer multicast (ZLL 2005)

- Efficient digital signature schemes for packet flows and multicasts (WL 1998)
  - Signed packets are individually verifiable
Conclusions

- Moral of the “accidental closer” story
  - In designing a protocol, think about its users. Make the protocol as easy to use as possible.

- Middle relief work
  - It pays the bills
  - It keeps us busy and thinking until the next big opportunity
  - Unlike baseball, our role is not determined by a manager. A middle reliever can become a starter or closer during a game.