Privacy Preserving Intrusion Detection

Jaideep Vaidya
Mikhail Atallah

Motivation

- Privacy and surveillance by intrusion detection are potentially conflicting organizational and legal requirements
- Companies do not want to reveal if attacks occurred, and whether they succeeded
- Companies producing IDS may not want to reveal their entire set of attack patterns, as that is a valuable business asset

Signature Matching Intrusion Detection

- Majority of commercial products based on matching attack signatures
- Real Time : Raw packet capture followed by signature matching
- Offline : Logs and audit trail database maintained, followed by offline signature matching

Offline Intrusion Dectection

- Real Time IDS cannot handle very high load before going “blind”
- Need to store audit databases anyway, to detect penetrations matching “new attacks” found

Pattern Matching

- Regexp (Regular Expression) is a common pattern matching language in the UNIX environment
- Regular Expressions are powerful enough to encode not just attack patterns, but also attacker profiles (since these can be represented by a string of “pertinent” attack patterns)

Problem

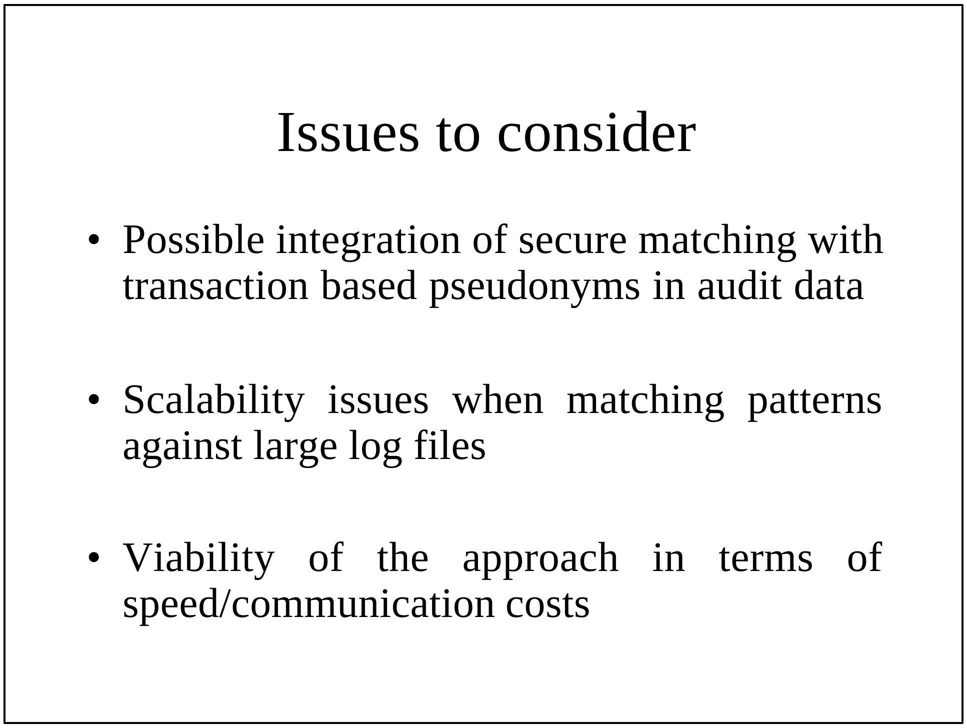
- How to detect patterns in the log files without revealing either the actual patterns or the log file information
- In effect, we need to create a finite automaton which works without the actual “true” input

Secure Database Access Problem

- How to find if a string q exists in a database of strings.
- The exact matching problem has been extensively considered in the literature
- Provides a yes/no answer

Regexp matching

- For regexp matching, we need to make three modifications in the solutions for SDA.
  - To allow matching of ranges
  - Specifying position from which to start matching
  - Reply should give position at which matched



Issues to consider

- Possible integration of secure matching with transaction based pseudonyms in audit data
- Scalability issues when matching patterns against large log files
- Viability of the approach in terms of speed/communication costs