A system for distributed queries of security-relevant data

Dr. Timothy Shimeall, George Jones, and Derrick H. Karimi

Contact: http://www.sei.cmu.edu/about/people/

Problem: integrating differing data on a common query

Description: Email is sent to all engineering staff at XYZ.com, fraudulently sourced from CIO, requiring participation in security survey at DoSurvey.com (with very short turn-around demanded)

- DNS cache poisoning of DoSurvey at XYZ, redirection to dynamic DNS domain
- Survey asks for “free registration” (email address and user-specified password)
- Survey questions on what network detection is present at XYZ, which servers are used most often
- Users are told responses would enable drawing for cash prize

Overview of Quilt

Architecture of Quilt

Pattern ::= UNTIL(pattern, pattern) | CONCURRENT(pattern, pattern, ...) | FOLLOWS(dt, pattern, pattern) | expr
Expr ::= AND(expr, expr, ...) | OR(expr, expr, ...) | NOT(expr) | condition
Condition ::= Term > Term | Term >= Term | Term < Term | Term <= Term | Term == Term | Term != Term
Term ::= Term ^ Term | Term * Term | Term / Term | Factor
Factor ::= Factor + Factor | Factor - Factor | Factor
Value ::= (pattern) | literal | source.field
literal ::= string | numeric
source ::= identifier
field ::= identifier [ term ]