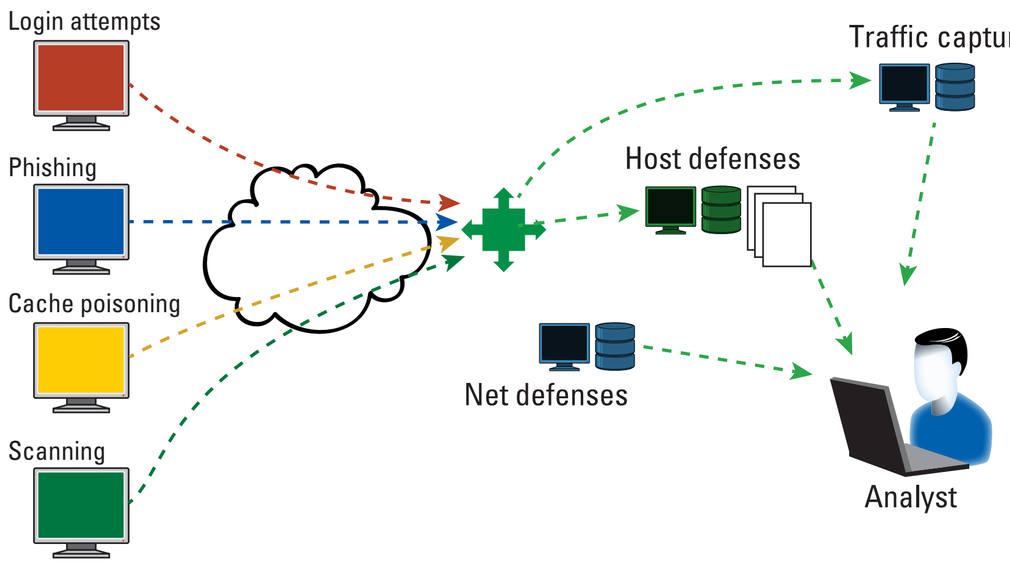
Quilt

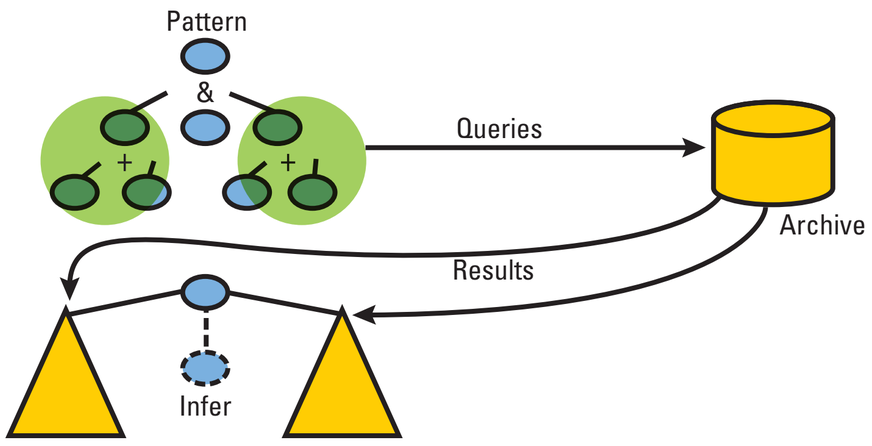
A system for distributed queries of security-relevant data

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

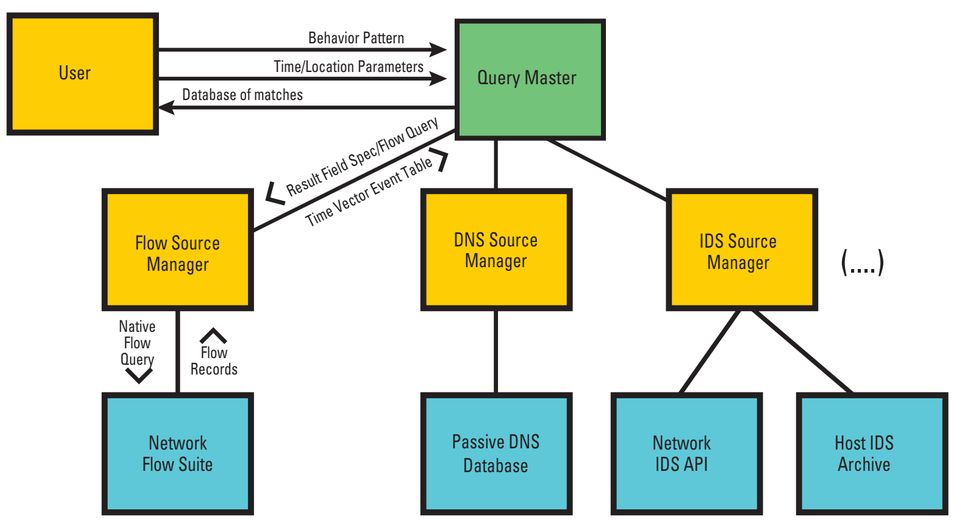
Contact: http://www.sei.cmu.edu/about/people/



Problem: integrating differing data on a common query



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 / Term | Factor
Factor ::= Factor + Factor |
            Factor - Factor | Value
Value ::= ( pattern ) | literal |
            source.field
literal ::= string | numeric
source ::= identifier
field ::= identifier | identifier [ term ]
```

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

action	condition	data needed
email received	*containing* a URL	- IDS Alert (phishing)
	while	- DNS data DNS
	poisoned for domain	- Blocklists
	followed by	
web hit		- Flow data
on Phishing blocklist		
	followed by	
brute force		- System Logs

- A Quilt sourceManager tracks each of several sources: DNS, Network Flow, Blocklists, email server logs, IDS alerts.
- An IDS alert fires indicating possible phishing. The alert indicates time and suspect URL.
- A user process formulates a quilt Query specifying the URL and the time the message was received.
- The query Master decomposes the quiltQuery into a series of sourceQueries
- The first source Query, sent to the DNS source Manager asks "was this DNS name poisoned at the time the mail was received"
- The second source Query, sent to a Netflow sourceManager asks "did we see web traffic to the poisoned address following receipt of the phishing email"?
- If the answer both answers are "yes", then return a match to the quiltQuery indicating a successful phishing attempt.

CERT
Software Engineering Institute
Carnegie Mellon