BSMTRACE

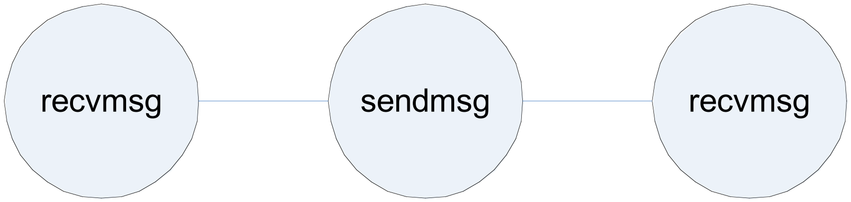
Audit driven HIDS

BSMTRACE

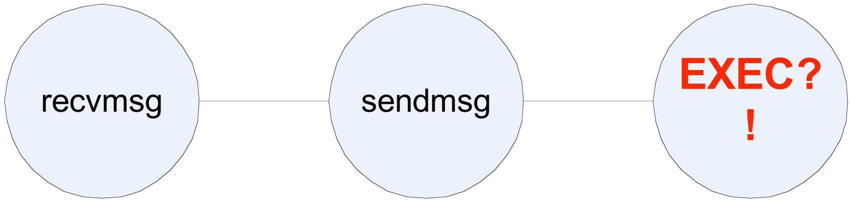
- Audit driven Host based IDS operating on finite state machine principals
- Uses audit pipes to tap into real time audit feeds
- Optionally run it on audit trail files (Solaris and OS X supported also)
- Makes intrusion decisions based on events that have definitively occurred

BSMTRACE

- Observes a process’s execution patterns (user specified sequences)

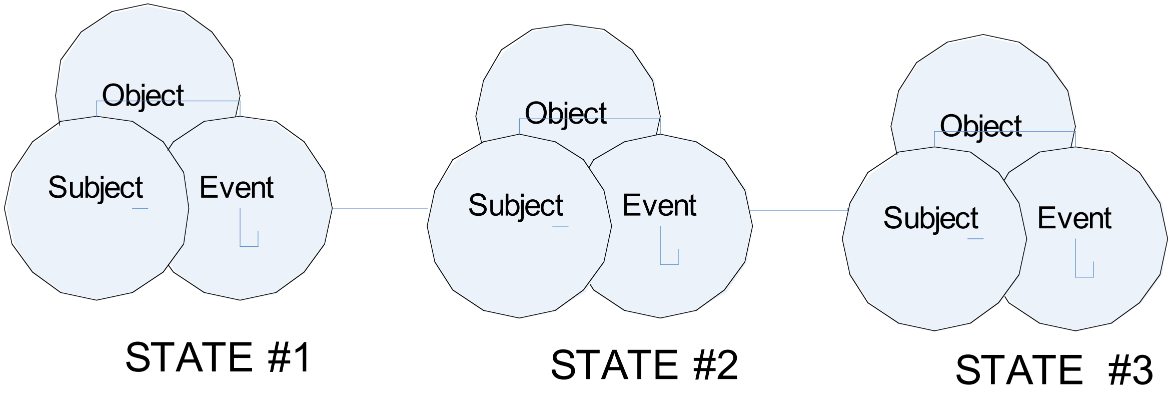


- Compromised processes typically change execution patterns



BSMTRACE

- "States" in detail

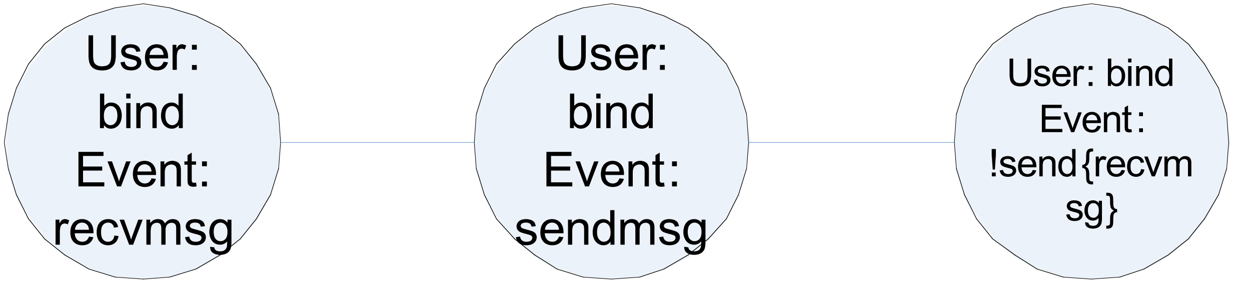


Object
Subject
Event
STATE #1

Object
Subject
Event
STATE #2

Object
Subject
Event
STATE #3

- Example sequence:



User: bind
Event: recvmsg

User: bind
Event: sendmsg

User: bind
Event: !send{recvmsg}

BSMTRACE

- Test it, break it, report it!
  - csjp@FreeBSD.org OR
  - alm@FreeBSD.org

- http://people.freebsd.org/~csjp/bsmtrace-1.0.1.tar.gz

- Perforce development
  - //depot/user/csjp/bsmtrace/…