Tracking the Role of Adversaries in Measuring Unwanted Traffic

Mark Allman  (ICSI)
Paul Barford  (Univ. Wisconsin)
Balachander Krishnamurthy  (AT&T Labs - Research)
Jia Wang  (AT&T Labs - Research)
How do adversaries impact measurements?

- While measurement systems are widespread, attention to impact of unwanted traffic is light
- Currently only arbitrary subset of attacks are considered
- Systematic evaluation of adversaries’ impact on measurement systems is needed
How adversaries impact malware measurements

- Focus on malware measurements as opposed to general measurements
- In general measurements, gaming is common - consider Keynote – which measures from \( n \) sites but measures know them and can counteract
- In security related measurements, system could be compromised and inference could be flawed
Background on measuring unwanted traffic

Other categorizations possible but broadly
- Firewall: maintain per-flow state and control connection set-up
- NIDS - network intrusion detection systems: anomaly detection (e.g., by matching signatures)
- Honeypots: monitor and responds to probes
- Application-level filters: e.g., spam filter
Challenges to security-related measurement systems

- Direct attacks
- Evasion
- Avoidance attacks
Direct attacks

- Attack an IDS by increasing its memory requirements -- make it maintain more state
- Increasing background noise (via legitimate requests)
- Compromise measurement platform (e.g. Witty worm compromise hosts running ISS)
Evasion

- Break payloads across packets ("ro" and "ot")
- Use non-standard port - port 80 for ssh
- Reorder and retransmit to fool NIDS
- Common victim: spam filters -- hence the use of random strings, deliberate mis-spellings
- Arms race - no easy way to defeat fully
Avoidance attacks

- Reverse blacklisting honeypots to avoid them
- Reverse blacklists exchanged between attackers
- One countermeasure is Mohonk technique of rotating blackhole prefixes
Taxonomy of how unwanted traffic pollutes measurement: concepts

- Two key concepts: consistency and isolation
  - Consistency: Set of packets $P_i$ always results in same set of log entries $A_j$
  - Isolation: Set of packets $P_i$ results only in log entries $A_j$

- Log entries vary across firewalls/NIDS and honeypots
  - Firewalls/NIDS logs: alarms with summary information from rule matching packets
  - Honeypot logs: packet traces with headers and/or payloads
Taxonomy of how unwanted traffic pollutes measurement

- **Consistent/isolated:**
  - $P_i \rightarrow A_i$ and no other $P_k$ will impact $A_i$
  - the baseline case - no pollution

- **Consistent/non-isolated:**
  - $P_i \rightarrow A_i$ but $P_i + P_j \rightarrow A_j$
  - measurement system behaves fine but log entries caused by unwanted traffic altered by other unwanted traffic

- **Inconsistent/isolated:**
  - $P_i \rightarrow A_{j1}$ at time $t_1$ and $P_i \rightarrow A_{j2}$ at time $t_2$
  - inconsistent behavior but limited impact

- **Inconsistent/non-isolated:** highly unpredictable
Consistent/non-isolated - example

Rule #1:  uri content:"/hsx.cgi";
          (raise an alarm if /hsx.cgi appears in the URI)

Rule #2:  uri content:"/hsx.cgi"; content:"../"; content:"%00"; distance:1;
          (/hsx.cgi appears in URI and content of ../.. followed
          by null byte in payload, raise an alarm)

Sequence S₁:  payload 1: POST /hsx.cgi HTTP/1.0\r\nContent-length: 10\r\npayload 2: ../
payload 3: ../
payload 4: \x00\x00\x00\x00

Sequence S₂:  payload 1: POST /hsx.cgi HTTP/1.0\r\nContent-length: 10\r\npayload 2: ../
payload 3: \x08/
payload 4: ../
payload 5: \x00\x00\x00\x00\x00

- Snort generates alarms 1 and 2 on sequence S₁ but only alarm 1 on S₂
- (backspace character in the fourth packet) - log entry changed by S₂
Inconsistent/isolated

- Measurement system generates different alarm sets $A_1, A_2$ for same set of packets $P$ arrived at time $t_1$ and $t_2$.
- Multiple backspace packets sent to Snort leads to unpredictable impact (inconsistency) on log entries but only signatures affected by backspace are problematic (isolated)
Inconsistent/non-isolated

Measurement system generates different log entries over time and is thus unpredictable
- Randomness in unwanted packet streams (beyond order of arrival)
- DoS: significantly increase resource use on measurement system
- What gets logged can be hard to predict
Adding resilience to measurement systems

- Situational awareness
- Separating an attack from a non-attack
- Bypassing attacks
- Graceful degradation
Summary

- We have examined impact of unwanted traffic on measurement systems
- An initial taxonomy of how such traffic pollutes measurement
- Helps us design resilient measurement systems