Stepping Stone Detection

Yin Zhang (Cornell University)

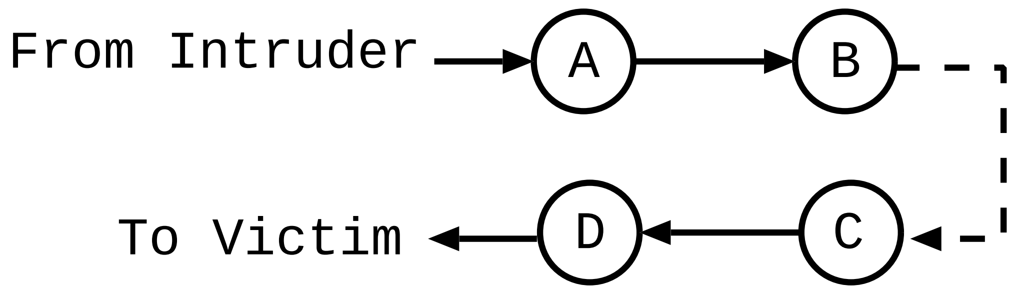
yzhang@cs.cornell.edu

Vern Paxson (ACIRI)

vern@aciri.org

Stepping Stone Detection

- stepping stone: widely used by intruders to preserve anonymity



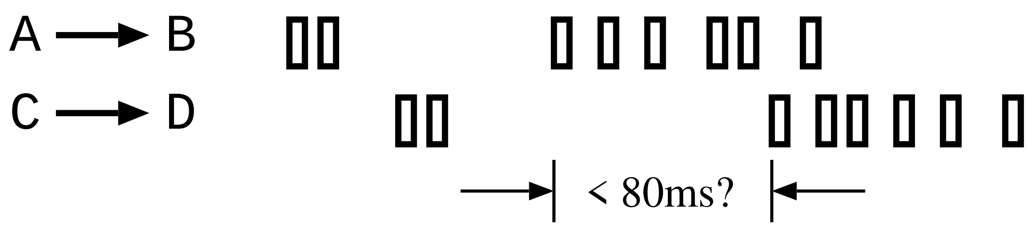
- stepping stone detection: detect stepping stones by monitoring network traffic
- goal: raise the bar
  - detect pass-through site (stepping stones)
  - back tracing intruders

Design Space

- content-based approach. pro: natural; con: opportunity, cost
- behavior of IDS. passive monitoring vs. perturbation
- single vs. multiple measurement point(s)
- filter as much as possible
- traffic type e.g. on/off vs. continuous
- timing lag
- A-B-C vs. A-B-...-C-D
- short-lived and/or few bytes
- robustness. tolerate clock skew, propagation delay, loss, packetization variations.

Our Solution

- general approach:
  - finding invariants
  - leverage particulars of how interactive traffic behaves
- timing correlation when idle periods end



  - only consider the end of idle periods
    idle period: no activity for $\geq$ 0.5 sec (a big filtering win!)
  - two idle periods considered correlated, if ending time differ by less than 80 ms;
  - detection criteria:
    * number of correlated idle periods
    * $\frac{\text{number of correlated idle periods}}{\text{total number of idle periods}}$

Performance Evaluation

- status: implemented in Bro, running on UCB DMZ
- performance:
  - accuracy:
    * trace: 3831 conns, 626 hosts, 23 stones, 2 FN, 0 FP
  - efficiency: capable of real-time detection
  - failures:
    * wall's lead to non-stepping-stone correlations
    * phase-drift in periodic traffic leads to false coincidences (now filtered out)
    * excessively short connections

Backdoor Detection: A Parallel Project

- backdoor detection = interactive traffic on non-standard ports
- key idea: filter to only small packets