Adaptation

Dina Katabi

Adaptive Defenses (1)

- Parameters of the defense system change with attack
  - Adapt the detection threshold [SRUTI05]
    - Desirable prob. of false positive & false negative change with attack severity [SRUTI05]
  - Adapt the authentication prob. [Kill-Bots]
    - Authenticate with prob. α function of attack rate and drop the rest → admission control to authentication
  - Anomaly detection systems learn the characteristics of normal traffic and adapt
  - Others?

Adaptive Defenses (2)

- Exploit adaptation in normal traffic
  - Stress Testing [SRUTI05]
    - TCP adapts to a drop
      - Use that to test for TCP friendliness
    - Web users retry after a timeout
      - Use it to check for a zombie

Adaptive Attacks

1. Attacks adapt their parameters
   - Change attack severity to cause oscillation in the detection system
2. Attack the adaptive behavior
   - Attacks on TCP timeout behavior [the shrews attack]
   - Teach an anomaly detection box to accept attack packets by slowly introducing the attack traffic

Adaptation Raises Many Questions

- Does adaptation create new exploits?
- Can we argue that adaptation is always better than no adaptation?
- Which parameters should adapt and which shouldn't?
- Can attacks on a protocol's dynamics cause oscillations? How severe are such attacks?