

Analyzing Information Assurance Technology Using Modeling and Simulation

Bill Blackert
The Johns Hopkins University
Applied Physics Laboratory
(240) 228-7808
william.blackert@ihuapl.edu



References

- W. J. Blackert, "Analyzing Computer Network Attack and Mitigation Technology Performance Using Modeling and Simulation," Presented at the 71st MORS Symposium, Quantico, Virginia, June 2003.
- W. J. Blackert, D. M. Gregg, A. K. Castner, E. M. Kyle, R. L. Hom, "Analyzing Interaction Between Distributed Denial of Service Attacks and Mitigation Technologies," Proceedings of DISCEX III, April 22-24, 2003.

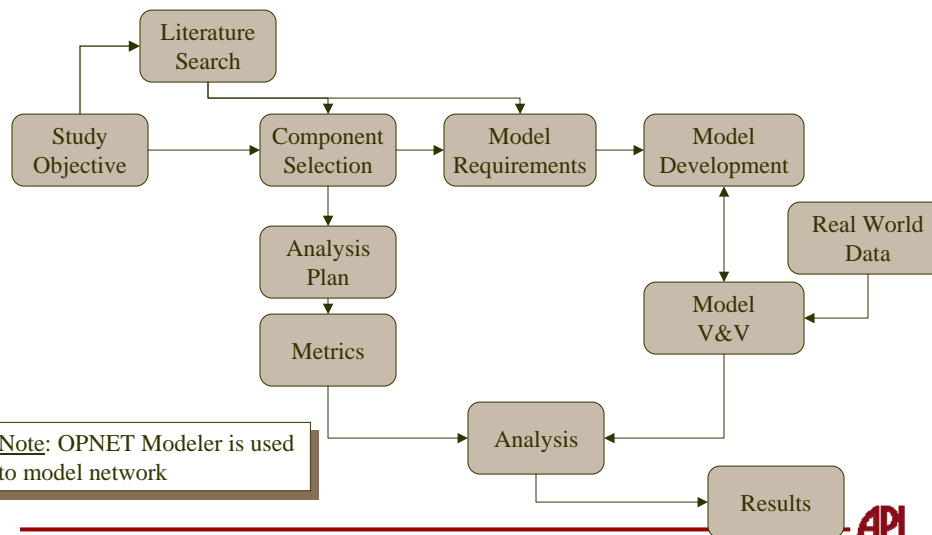


Key Findings

- Computer systems can be tuned to make them more robust against some DoS attacks
- Mitigation technologies based on classification schemes are vulnerable to attackers that can use misclassification to their advantage
- Rate limiting techniques that blindly discard packets can preserve bandwidth but degrade service to nodes sharing bandwidth with the attack
- Client puzzle protocols can be effective against a single attacker. However, they are susceptible to a distributed attack.
- Mitigation technologies can be successfully combined when they communicate or are designed not to interfere with each other. Otherwise, new vulnerabilities may be introduced.

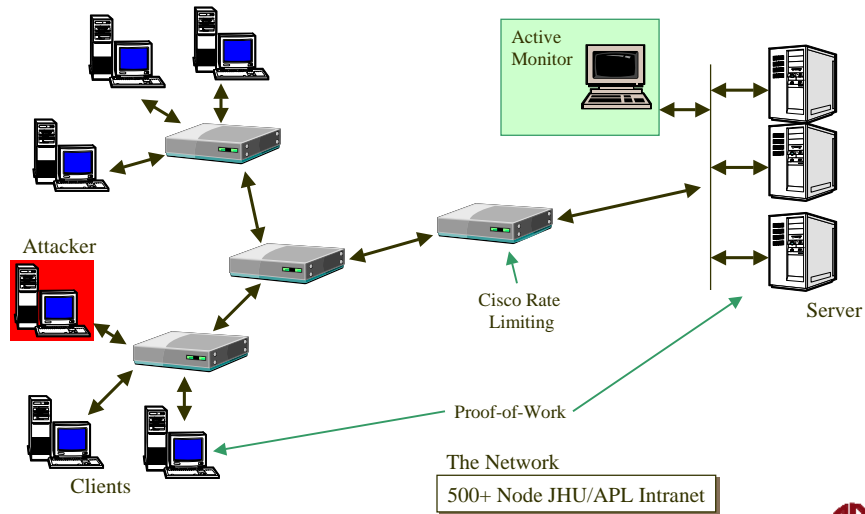
APL

Study Process

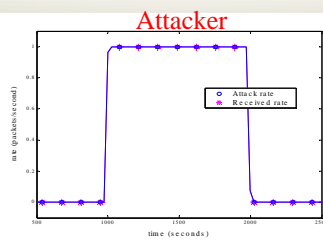


APL

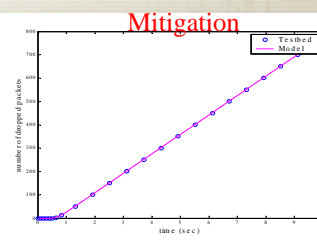
Analysis Components



Sample Verification & Validation Results

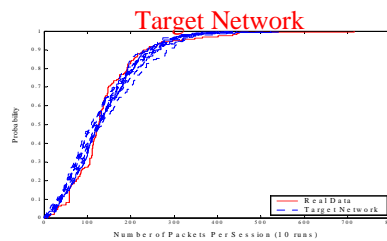


✓ **Verification:**
Attack Rate from
Attacker to Victim



✓ **Validation:** Rate
Limiter Number of
Dropped Packets for
a High Attack Rate
(TCP SYN-Flood)
(100 60-byte pps)
(first 10 seconds)

✓ **Validation:**
Aggregate Traffic to
SMS Server
(one hour)



APL

Metrics

- Attack
 - Effectiveness (e.g., Probability of Denied Service (PDS))
 - Adaptability (e.g., Additional effort necessary to increase PDS)
- Mitigation Technique
 - Technique effectiveness (e.g., change in PDS)
- User
 - Delay (e.g., Time to setup a TCP connection)

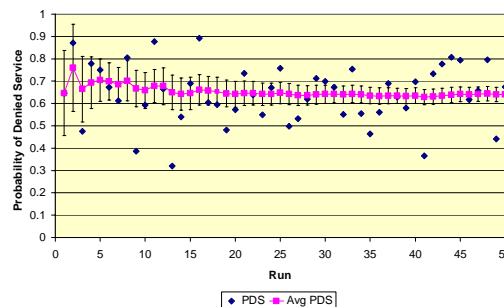
$$PDS = 1 - (\# \text{ of successes}) / (\# \text{ of attempts})$$

$$\Delta PDS \Rightarrow \begin{cases} + & \text{Attack is more effective} \\ - & \text{Attack is less effective} \end{cases}$$

APL

Baseline Results

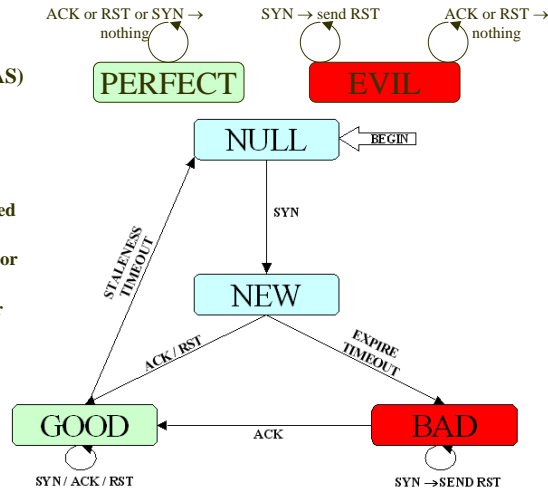
- Attack
 - 1000 packet per second SYN flood against a network web server
- Results with No Mitigation Present
 - With no attack, PDS = 0
 - Using a 39 Pending Connection Queue, typical of Windows 2000 system, PDS = 0.97 (50 Runs)
 - Tuning the system by increasing queue size to 8192, PDS = 0.64 (50 Runs)



APL

Active Monitoring

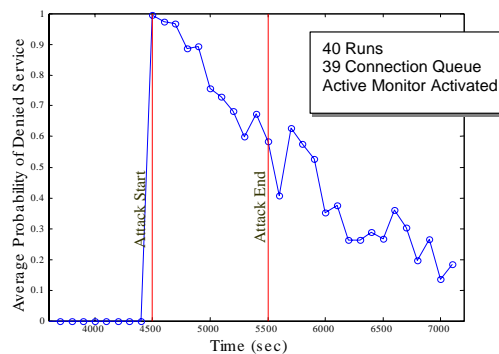
- Based on C. L. Schuba, et. al. "Analysis of a Denial of Service Attack on TCP" COAST (CERIAS) Laboratories
- The Active Monitor
 - Monitors traffic on a particular subnet
 - Classifies nodes based on observed traffic
 - Resets connections from "BAD" or "EVIL" hosts
 - Permits traffic from "GOOD" or "PERFECT" hosts



APL

Active Monitor Analysis Summary

- For the 39 Connection Queue
 - PDS = 0.81 during the attack ($\Delta PDS = -0.16$)
 - PDS = 0.39 after the attack ($\Delta PDS = +0.36$)
- Extension of Denied Service beyond the attack results from misclassification



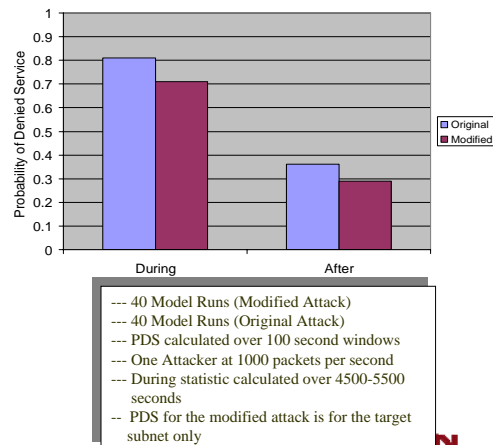
*CERIAS has been made aware of these findings

APL

Attacker Adaptation: Trying to Exploit AM

(500 Node Network, TCP SYN Flood: 1000 pps, No Server Tuning)

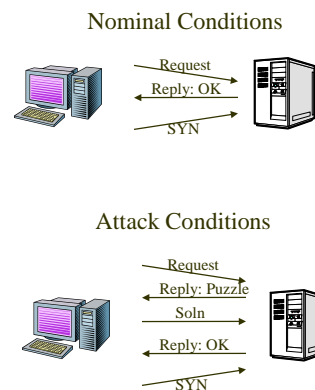
- An attacker can manipulate the Active Monitor's classification scheme
 - Fill up the pending connection queue (39 packets)
 - Spoof desired subnet(s) to exclude ($N \times 256$ packets)
 - These subnets now denied service, with far fewer packets sent



APL

Proof of Work Process

- Clients must “pay” for server usage by performing work
- Based on A. Juels and J. Brainard: “Client Puzzles: A Cryptographic Countermeasure Against Connection Depletion Attacks”



APL

Proof of Work: Initial Analysis

- **Baseline attack**
 - 1000 pps SYN Flood
 - PDS = 0 against 8192 queue
 - Since attacker doesn't "register" with Proof of Work, SYN packets are discarded
- **Proof of Work Aware Attacker**
 - 1000 pps attack from attacker accounting for Proof of Work
 - 8192 queue
 - Attacker CPU becomes overwhelmed, attack falters, and no denied service results (i.e., PDS = 0)

APL

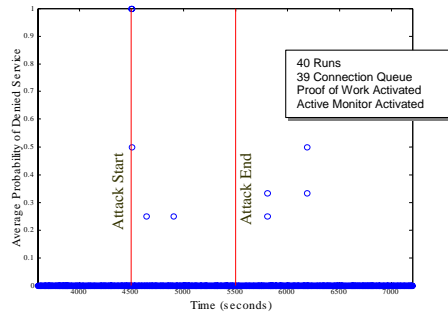
Distributing the Attacker

- Puzzle requires 0.45 seconds to solve
- By using 450 attackers, and having each send an attack after solving a puzzle, a 1000 pps attack results where each attacker solves one puzzle at a time
- Resulting PDS is 0.66 for an 8192 queue

APL

Active Monitor and Proof of Work Combined

- Single mitigation analysis shows
 - Active Monitor can misclassify nodes
 - Successfully attacking Proof of Work requires a transaction. Therefore, the attacker cannot spoof.
- Together against at 1000 pps SYN Flood attacker and a 39 queue, Average PDS drops to approximately zero. ($\Delta PDS = -0.97$)
- Some misclassification is still observed



APL

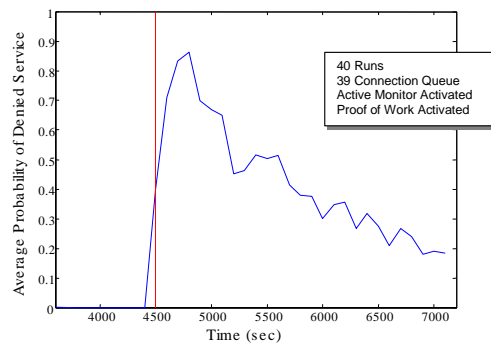
Exploiting the Proof of Work and Active Monitor

- Proof of Work drops SYN's if permission is not granted.
- The Active Monitor makes decisions based on three-way handshake observations.
- When subjected to a basic SYN flood, the Proof of Work discards SYN packets. The Active Monitor determines invalid handshakes and classifies these addresses as BAD.

APL

The Attack

- Service is denied to these addresses (PDS = 0.67 for 1000 seconds) even though the attack lasts a fraction of a second.
- Since Proof of Work by itself is not susceptible to the attack, $\Delta PDS = +0.67$.
- A vulnerability has been introduced because of the two mitigation techniques.



APL

Conclusions

- Analysis can provide insight into attack and defense interaction and performance.
- Key observations
 - Attacks fall into classes and behaviors are similar within a class
 - Required attacker effort can vary significantly from attack to attack
 - Tuning a system can provide a better defensive posture
 - Combining mitigation technologies can introduce vulnerabilities if the technologies interfere with each other

APL