A Cost-Based Framework for Analysis of Denial of Service in Networks

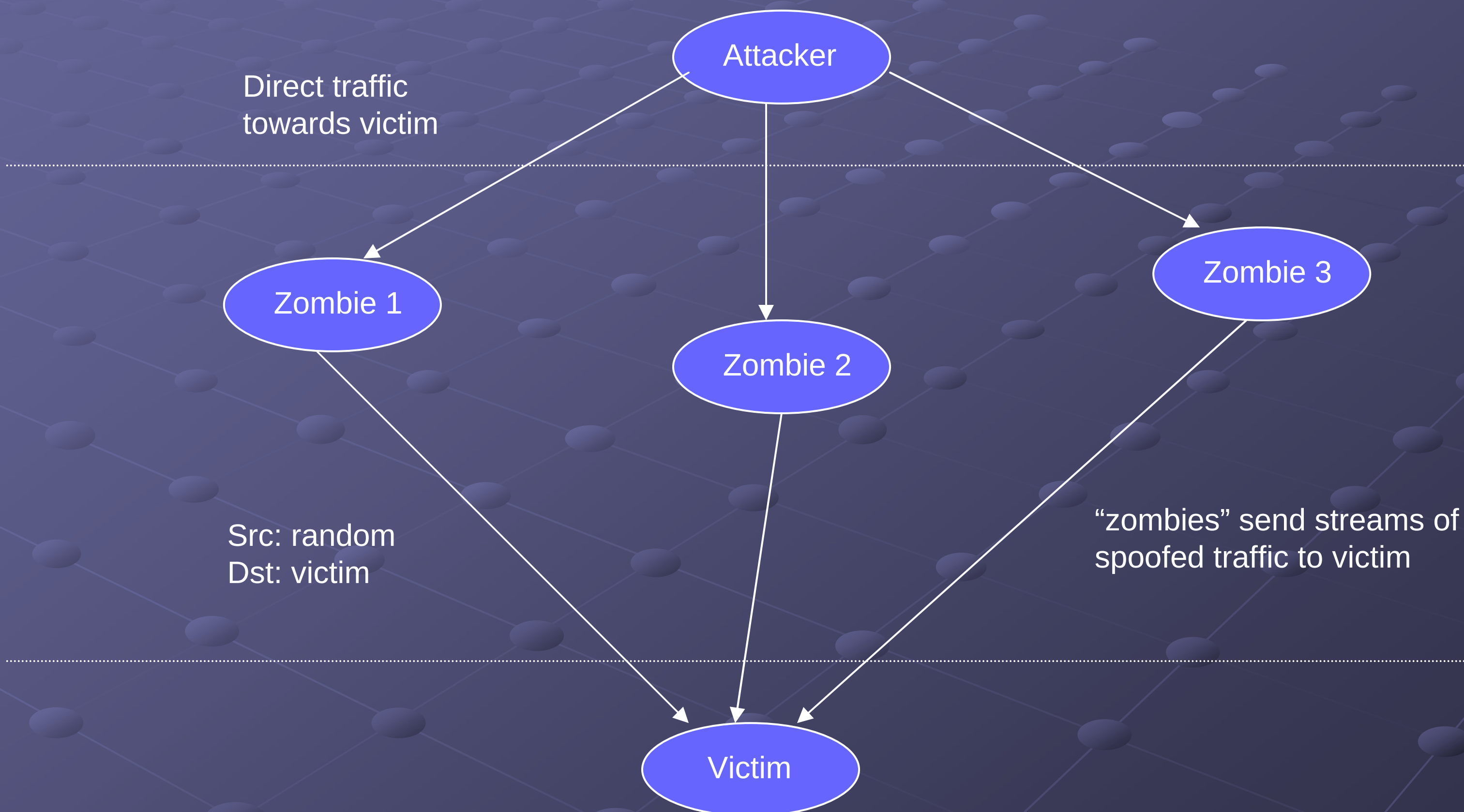
Author: Catherine Meadows

Presenter: Ajay Mahimkar

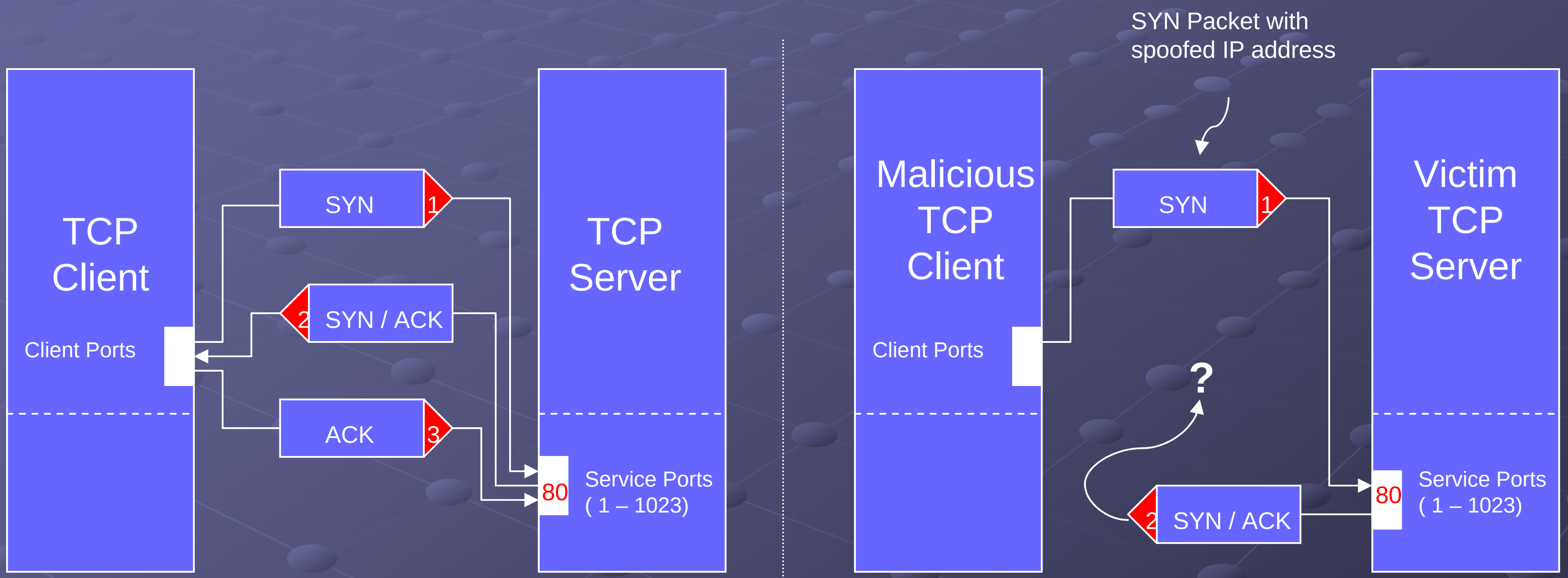
What is a DoS Attack ?

- Malicious attempt by a group of people to cripple an online service
- Flood the victim (server) with packets
  - Overload packet processing capacity
  - Saturate network bandwidth
- Two Types of DoS Attacks
  - Resource Exhaustion Attacks
  - Bandwidth Consumption Attacks

Attack Architecture – Direct Attacks



Example – SYN Flooding



- Establishment of TCP connection using three-way handshake
- Attacker makes connection requests aimed at the victim server with packets from spoofed source addresses

Attacker v/s. Defender

- Goal of the attacker
  - Make the defender waste its resources by interacting with the attacker
  - Prevent the defender from learning its identity
- Defense against DoS Attacks
  - Reduce the cost to the defender of engaging in the protocol
  - Introduce some sort of authentication
- Formal methods are a good way to analyze DoS

Contribution of the paper

- Framework to evaluate a protocol for resistance to DoS attacks
- Cost-based Model for the list of actions taken by the attacker and the defender
- Compare the cost to the attacker with the cost to the defender

Framework

- Assign costs of engaging in individual actions
- Compare costs of defender and attacker
- Incorporate Gong-Syverson's fail-stop model
  - A protocol is fail-stop if it halts upon detection of any bogus message (replay or message from intruder)
  - Requires strong authentication making itself vulnerable to DoS attacks

Framework

- Modified Fail-stop Protocol
  - Extension to any action taken by a principal, not just the acceptance of a message
  - Define a function *F* from actions to costs
    - Protocol is fail-stop with respect to *F*, if a principal cannot be tricked into engaging in a protocol up to and including action *A*, unless attacker expends an effort of more than *F(A)*
    - Protocol is insecure against DoS attacks, if *F(A)* is trivial for the attacker as compared to that of the defender

Station to Station Protocol

- Uses Diffie-Hellman protocol along with digital signatures for key exchange and key authentication between two principals

$A \longrightarrow B : g^{X_A}$

$B \longrightarrow A : g^{X_B}, E_K(S_B(g^{X_B}, g^{X_A}))$

$A \longrightarrow B : E_K(S_A(g^{X_A}, g^{X_B}))$

- g – generator of the group
- X_A – A's secret
- X_B – B's secret
- K – shared secret between A & B

$K = g^{X_B \cdot X_A}$

Alice-and-Bob Specifications

- It is a sequence of statements of the form

  $A \longrightarrow B : T_1, T_2, \ldots, T_k \mid\mid M \mid\mid O_1, O_2, \ldots, O_n$

  T_i – operations performed by A, and

  O_j – operations performed by B
- Three Types of Events
  - Normal Events (send and receive)
  - Verification Events (occur only at receiver)
  - Accept Event (O_n)
- Desirably precedes relation

Protocol Specification

1. A $\longrightarrow$ B : *preexp*$_1$, *storename*$_1$ || g^{X_A} ||
   storenonce$_1$, *storename*$_2$, *accept*$_1$

2. B $\longrightarrow$ A : *preexp*$_1$, *sign*$_1$, *exp*$_1$, *encrypt*$_1$ || g^{X_B} , E_K (S_B(g^{X_B} , g^{X_A})) ||
   checkname$_1$, *retrievenonce*$_1$, *exp*$_2$, *decrypt*$_1$,
   checksig$_1$, *accept*$_2$

3. A $\longrightarrow$ B : sign$_2$, encrypt$_2$ || E_K (S_A(g^{X_A} , g^{X_B})) ||
   checkname$_2$, retrievenonce$_2$, decrypt$_2$, checksig$_2$,
   accept$_4$

Cost Functions

- Cost Set
  - *expensive > medium > cheap > 0*
- Cost Function
  - Function from set of events by an annotated Alice-and-Bob Specification *P* to a cost set *C*
- Attacker Cost Functions
  - Attacker cost set augments *very expensive* and *maximal*

Definition

- Let
  - *C* – Defender cost set
  - *G* – Attacker cost set
  - δ – Event cost function defined on the annotated Alice-and-Bob protocol (*P*) and the cost set (*C*)
  - $\delta' (V_i)$ – Message processing cost function associated with δ on verification events
    - Cost of processing a message upto and including a failed verification event
    - $\delta' (V_i) = \delta (V_1) + \delta (V_2) + \ldots + \delta (V_i)$
  - $\Delta (V_n)$ – Protocol engagement cost function associated with δ on accept events
    - Cost of processing the last message + cost of composing any message sent as the result of that last message
    - Expensive for all accept events in the Station-to-Station protocol
  - θ – Attack cost function

Definition

- Alice-and-Bob specification of a cryptographic protocol is fail-stop if
  - Whenever a message is interfered with, then no accept event desirably-after the receiving of that message will occur

- Tolerance Relation
  - Defined as the subset of *C x G* consisting of all pairs *(c,g)*, such that attacker cannot force defender to expend resources of cost *c* or greater without expending resources of cost *g* or greater
  - *(c', g')* is within the tolerance relation if there is a *(c, g)* in the relation such that *c'* <= *c* and *g'* >= *g*

Evaluating Protocol Security

- Steps
  - Decide
    - Intruder Capabilities
    - Intruder Cost Function
  - Decide
    - Tolerance Relation
  - Determine the minimal attack cost functions with respect to which the protocol is fail-stop
  - For each attack cost function θ determine:
    - If event E_1 is an event immediately preceding a verification event E_2, then $(\delta' (E_2), \theta (E_1))$ is within the tolerance relation
    - If E is an accept event, then $(\Delta (E), \theta (E))$ is within the tolerance relation

Station-to-Station Protocol

1. A $\longrightarrow$ B : *preexp*$_1$, *storename*$_1$ || g^{X_A} ||
   storenonce$_1$, *storename*$_2$, *accept*$_1$

2. B $\longrightarrow$ A : *preexp*$_1$, *sign*$_1$, *exp*$_1$, *encrypt*$_1$ || g^{X_B} , $E_K\,(S_B(g^{X_B}, g^{X_A}))$ ||
   checkname$_1$, *retrievenonce*$_1$, *exp*$_2$, *decrypt*$_1$,
   checksig$_1$, *accept*$_2$

   - θ (*checkname*$_1$) – cheap (within tolerance relation)
   - δ' (*checksig*$_1$) – expensive, θ (*decrypt*$_1$) – expensive to very expensive (may or may not be within tolerance relation)

3. A $\longrightarrow$ B : sign$_2$, encrypt$_2$ || $E_K\,(S_A(g^{X_A}, g^{X_B}))$ ||
   checkname$_2$, retrievenonce$_2$, decrypt$_2$, checksig$_2$,
   accept$_4$

   - δ' (*checkname*$_2$) – cheap (within tolerance relation)
   - δ' (*checksig*$_2$) – expensive, θ (*decrypt*$_2$) – atmost medium (not within tolerance relation)

Tools & Models

- Casper, Murϕ, NRL Protocol Analyzer
  - Incorporate degree of security provided by each message as it is processed
  - Keep a running tally of the cost involved, as an attack is constructed

Comments on the Paper

- A neat framework to evaluate protocol resistance to DoS attacks

- Framework could be viewed as a game model between a defender and multiple attackers
  - However, this may or may not resolve bandwidth consumption attacks

Questions ???