and 12

**CS 458/658 - Computer Security and Privacy** **Fall 2018**

Lecture 11 and 12: October 16 - 18, 2018

*Lecturer: Ian Goldberg* *Notes By: Harsh Mistry*

# 11.1 Network Security Continued

## 11.1.1 Network Concepts

### 11.1.1.1 Web Site Vulnerabilities

- Web site defacements
- Attacked can examine returned HTML code for vulnerabilities
- Attacked can send malicious URL to web server
- HTTP protocol is stateless, so client is often asked to keep the state in the form of a cookie or URL. This can be abused by submitting modified state information to the server
- Cross-Site Scripting or Request Forgery attacked which are a form of code injection can be used to add HTML code to somebody else's page
- XSS : code steals sensitive information contained in the web page and sends it to attacker
- CSRF : Code performs malicious action at some web site if user is currently logged in there

## 11.1.2 Denial of Service

- Exploit knowledge of implementation details about a node to make node perform poorly
- A SYN flood is when a attacker initiates a TCP condition and doesn't send any acks
- DNS attacks are also common where a users cache can be filled with incorrect host info

### 11.1.2.1 Reflection and Amplification of DDoS Attack

- An attack where the victim is flooded with legitimate-looking traffic that originates from unsuspecting network nodes on the internet
- Amplification : A vulnerable network node runs a service that responds to queries with much more data than the query itself
- Reflection : The attacker spoofs the source address of the queries to that of the victim so that the vulnerable network nodes send responses to the victim

#### 11.1.2.2 Distributed Denial of Service

- Similar to DoS expect the attack is spread across a series of devices to mask the source
- This networks of devices are often refereed to as a botnets

### 11.1.3 Active code

- To reduce load on server, a server might ask a client to execute code on its behalf
- Obviously, this can be dangerous for clients as this code could possibly be malicious
- To combat this, its ideal to run untrusted code in a sandbox

### 11.1.4 Network Security Controls

- Ensure the design validates user inputs
- Separate services across multiple devices
- Ensure services are duplicated to ensure redundancy
- Use Firewalls to filter traffic
- Attempt to pass traffic through a few routers to enable easier monitors

### 11.1.5 Firewalls

- Firewalls allow for all traffic to be passed through choke points
- Types of firewalls
  - Packet filtering gateways : The simplest type which make decisions based on just the header
  - Stateful inspection firewalls: Keeps state to identify packets that belong together
  - Application proxy : All traffic for a specific application is passed through a proxy
  - Personal firewalls : Typically forbid everything unless explcity allowed and run on a users computer

### 11.1.6 DMZ

- Sub-network that contains an organizations external services
- Often is set-up between a internal and external firewall

### 11.1.7 Intrusion detection systems

- Firewalls do not protect agaonst inside attackers or insiders making mistakes can be subverted
- IDSs are next line of defense
- IDss monitor activity to identify malicious or suspicious events
- Host Based IDSs
  - Run on a host to protect the host
  - Can exploit lots of information, and misses out on information available to other hosts
- Network Based IDSs
  - Runs on dedicated node to protect all hosts on a network
  - Has to rely on on information available in monitored packets
- Distributed IDSs combine both Network and Host based approaches
- Signature Based IDSs
  - Attack signatures are compared aganist a collection of known signatures.
- Heuristic/anomaly Based IDSs
  - Looks for behaviour that is out the ordinary by modelling good behaviour and raising alerts when system activity no longer resembles this model
  - All activity is classified as good or benign, suspicious, or unknown
  - The primary disadvantage is that even goof IDs using this method take time to learn and classify unknown events.