

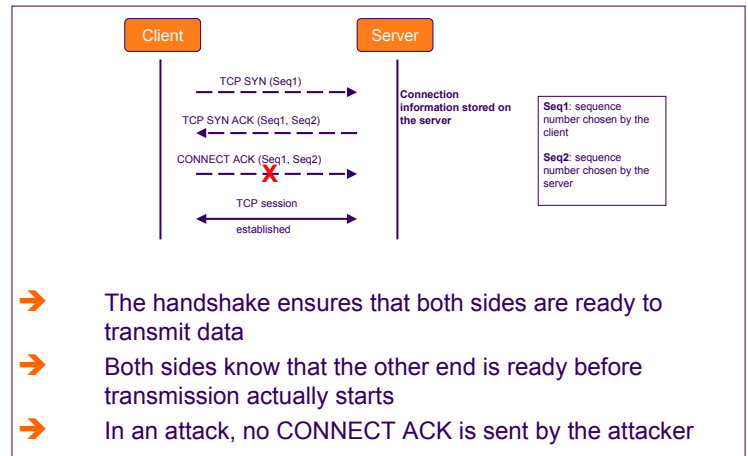


# TCP SYN flood use-case

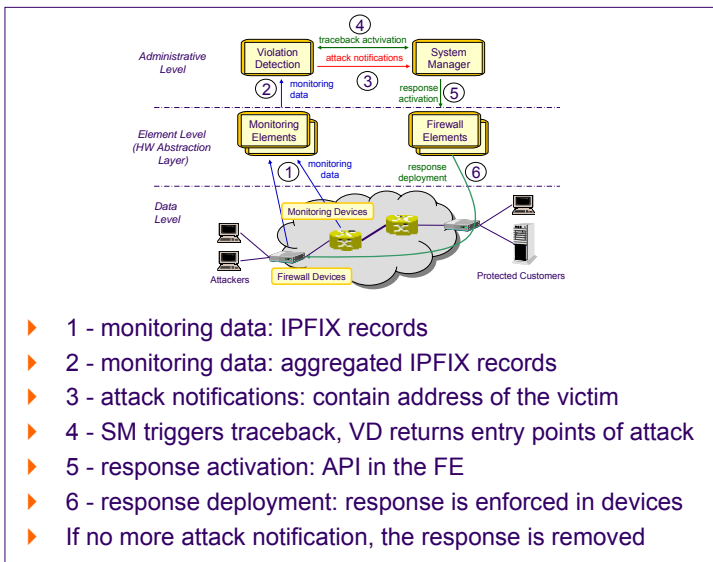
## Motivations

- ➔ SYN flood attacks are very common
  - ▶ Inferring Internet Denial-of-Service Activity (2006)
  - ▶ In 3 years: 68,700 attacks, 34,700 distinct targets
- ➔ Attack tools widely available
  - ▶ Trinoo, Tribe Flood Network, TFN2K, Stracheldraht
  - ▶ Ability to manage the agent network
  - ▶ Sophisticated (decoy packets sent to non-target networks, encryption, no communications from agents to master)
- ➔ Can target many services (web, e-mail, authentication,...)

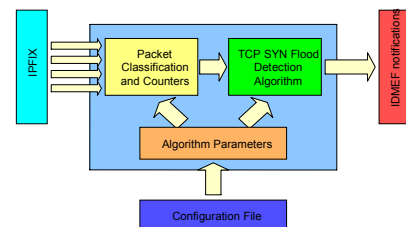
## SYN flood attack



## Demo overview

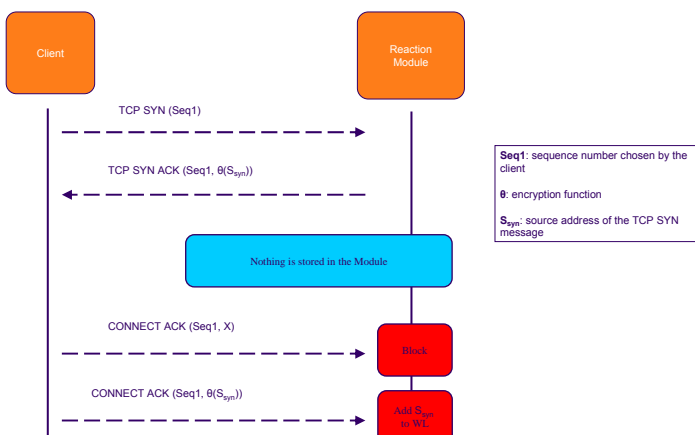


## Detection



- ▶ Uses widely known cumulative sum algorithm (CUSUM) – a good function for attack detection
- ▶ Counts TCP SYN and SYN/ACK packets
- ▶ Attack is detected when a given threshold is exceeded

## Reaction Function



## Conclusion

- ➔ Benefits
  - ▶ Programmable devices
  - ▶ Flexible detection and reaction systems
- ➔ Evaluation results
  - ▶ ~40 seconds for detecting and responding to attacks
  - ▶ Attack blocked at entry points
  - ▶ Victim available to legitimate clients