CE0973a - Issues in Network Security
4: Attacks and Defences

James A Sutherland

Abertay University

Monday, 1st February 2016

Attacks

Attacks can generally be classified according to the CIA trio:

- C – Data compromise
- I – Defacement/impersonation
- A – Volumetric/DoS

Volumetric/DoS Attacks

Goal: overwhelm some critical component, disabling service, usually via amplification

- Ping – directed broadcast "smurf attack"
- DNS[1]
- DNSSEC[2] - 50:1
- NTP[3]

[1] http://www.cisco.com/web/about/security/intelligence/guide_ddos_defense.html

[2] https://blog.cloudflare.com/deep-inside-a-dns-amplification-ddos-attack/

[3] https://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attac

Open resolvers

Google, Verizon and Cisco (OpenDNS) run public open resolvers. How do they secure those?

Defences

- Block directed broadcasts, DNS etc
- Rate-limiting
- Anti-spoofing: reverse-path filter
- ISP BCP: disallow spoofed traffic
- BGP blackholing: block specific abuse sources

DDoS case studies

- CloudFlare links earlier
- Janet attack[4]
- Andrews & Arnold[5]
- Linode[6]

[4] http://www.theregister.co.uk/2015/12/15/janet_no_longer_shares_network_information_after_ddos/

[5] http://www.ispreview.co.uk/index.php/2015/11/uk-broadband-provider-aaisp-suffers-strong-ddos-assault.html

[6] https://blog.linode.com/2016/01/29/christmas-ddos-retrospective/

Commercial Services

- CloudFlare
- Akamai
- Generally: DNS hosting, geolocation, security issues
- Geofencing, proxies, VPNs

Lab Exercise

Design robust hosting for a company, protected against various attacks. How would you structure this and why?

- DNS
- SSL
- Email
- Database
- Backups
- Location of data storage.