National CSIRT Contact

DDoS-Related Policy and Legal

POLICY/LEGAL REFERENCE	ORGANIZATION	DATE

Updated by

A DISTRIBUTED DENIAL-OF-SERVICE ATTACK is traffic originating from multiple sources directed at a target. DDoS attacks are intended to cause a negative impact on the availability of servers, services, applications, and/or other functionality of an attack target.

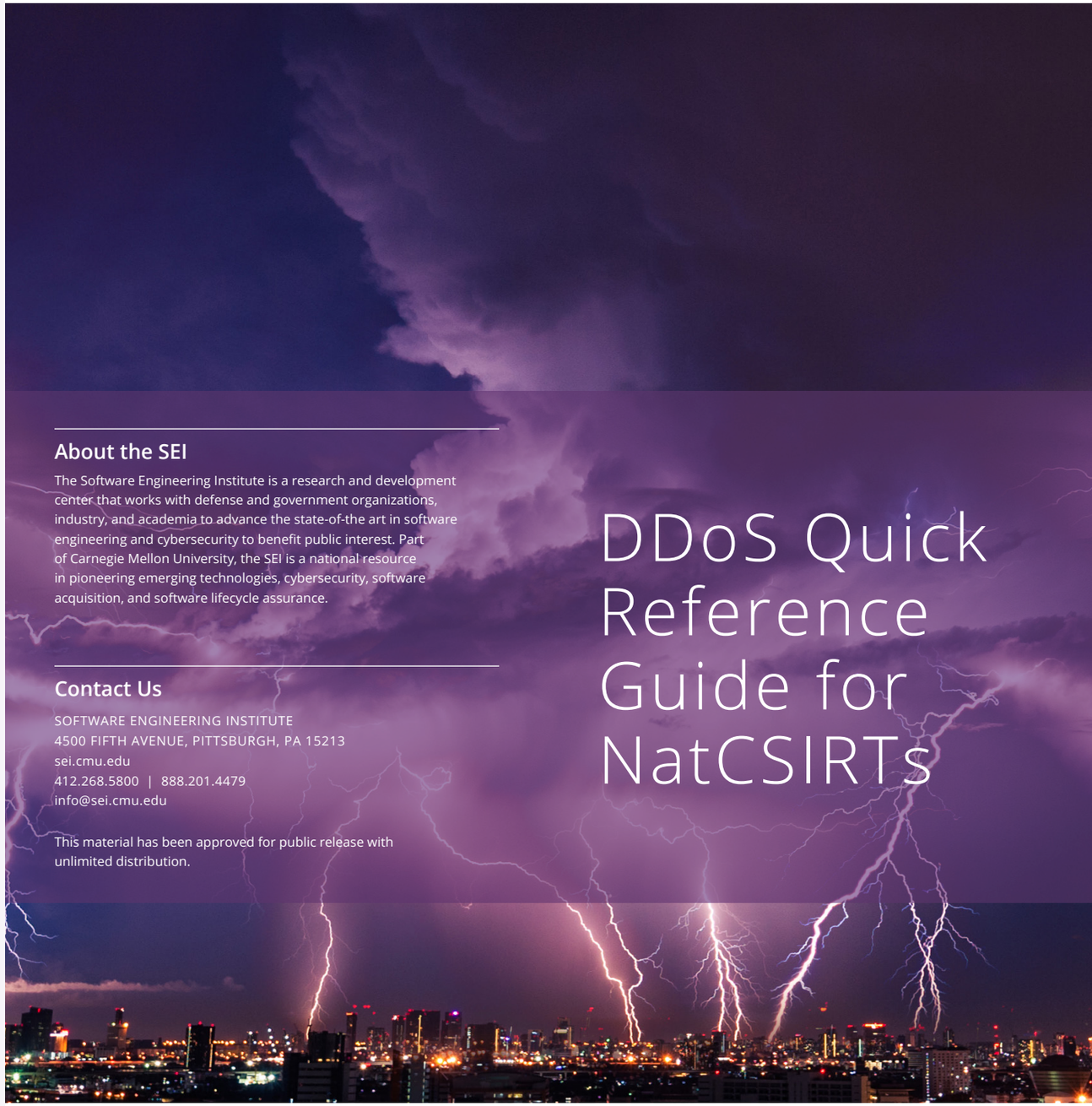
Types of DDoS

Volumetric	• UDP flood • DNS amplification • NTP amplification
Protocol	• SYN flood • ICMP flood • UDP fragments • DNS water-torture
Application	• GET/POST flood • Slowloris • STOMP flood • Apache killer

DDoS Defense

Bandwidth	• Increase bandwidth • Alternate routes • Filter unwanted traffic
Throttle/block	• Block unwanted protocol • Block unwanted source • Block unwanted destination • Blackhole upstream (RTBH)
Scrubbing	• BGP maneuver traffic (outsource) • Proxy application/CAPTCHA • Authenticate connection
Maneuver	• DNS re-allocate resources • BGP maneuver to partner

Carnegie Mellon University
Software Engineering Institute



About the SEI

The Software Engineering Institute is a research and development center that works with defense and government organizations, industry, and academia to advance the state-of-the art in software engineering and cybersecurity to benefit public interest. Part of Carnegie Mellon University, the SEI is a national resource in pioneering emerging technologies, cybersecurity, software acquisition, and software lifecycle assurance.

DDoS Quick Reference Guide for NatCSIRTs

Contact Us

SOFTWARE ENGINEERING INSTITUTE
4500 FIFTH AVENUE, PITTSBURGH, PA 15213
sei.cmu.edu
412.268.5800 | 888.201.4479
info@sei.cmu.edu

DDoS Prevention for NatCSIRTs

- Measure and increase bandwidth infrastructure
- Invest in hardware/fiber upgrades
- Connect with national peering networks
- Document contacts with network providers
- Participate in anti-spoofing efforts
- Partner with other national CSIRTS
- Support secure technology for ISP networks
- Increase transparency in reporting DDoS
- Provision bandwidth for emergency communications
- Sponsor events for collaboration and information sharing

Government

- Explore efforts to regulate digital device security
- Partner with commercial entities and NGOs on DDoS defense
- Adopt and validate best practices for digital services
- Sponsor innovative industry in DDoS defense
- Require DDoS security for critical services (medical, finance)
- Implement law and legal actions to prevent DDoS

DDoS Exercise and Evaluation

- Exercise annually for DDoS attack recovery
- Test all networks (metro, mobile, fiber) for capacity
- Evaluate critical communications for DDoS survival
- Practice DITL (Day in the Life) exercise to measure network devices, bandwidth, and usage
- Check QoS implementation

DDOS Prevention for Enterprises

- Implement source-validation and outgoing filtering
- Scan and remove open resolvers
- Implement DNS rate-limiting and NTP monlist

ISPs

- Harden perimeter (for example home routers, gateways, firewalls, etc.)
- Block/remediate infected Botnet clients
- Scan and remove open resolvers
- Implement DNS rate-limiting and NTP monlist
- Implement Quality of Service (QoS) where needed

Mobile

- Implement QoS and voice security
- Dedicate emergency traffic bandwidth
- Remediate infected phones

Vendors

- Practice secure coding
- PSIRT services to remediate devices
- Implement Over The Air (OTA) and live security updates

DDoS Operations and Training

- Measure and understand maximum bandwidth potential
- Measure ongoing bandwidth usage
- Document DDoS defense measures
- Educate Network Operations Center (NOC) on DDoS
- Validate communication with ISPs
- Commit to SLA on timelines for DDoS response
- Document takedown procedure for botnet infections
- Measure and increase efficiency in DDoS defense

DDOS Preparation Steps

TRACK	METHOD	DESCRIPTION
Capacity Planning	Physical	Fiber cable & hardware
	Logical	Protocols & logical failover
	Application	Software & application resources
Quality of Service	Audit critical application	Dedicate bandwidth for voice and emergency
RTBH	BGP	Implement upstream blackholing
Outsourcing/ Partnering	International partner	Host and co-host emergency apps
Anti-spoofing	CPE devices and major network links	Implement anti-spoofing at customer devices and at critical backbones
Device Security	Vulnerability management	VM for devices: home routers, access devices, and endpoints

DDOS Monitoring Tools

TYPE	SOFTWARE	DESCRIPTION
SNMP interface	• MRTG • Cacti	Bandwidth monitoring
Netflow	• nTop • nfsen • cflowd	Protocol and usage monitoring
	FastNetMon	high-speed netflow collection
SNMP & SNMP Trap	• NetXMS • OpenNMS	Resource usage and bandwidth usage
Log & APIs	Nagios/Zabbix	Generic monitoring of all resources (CPU/memory)

DDOS Monitoring Reports

REPORT NAME	TYPE	DESCRIPTION
Top Talkers	Netflow	Record top-talkers at metro-level network
Top Protocols & Applications	Netflow	Top-10 ports, protocols, and applications
Resource Usage	SNMP & SNMP Trap	Resource usage and bandwidth usage
Top Devices	Log & APIs	Generic monitoring of all resources (CPU/memory)
% Bandwidth	SNMP	Counters to measure logical and physical links at capacity
Resource & Capacity	SNMP	Resource usage of various backbone devices (distribution, core and hub layers)

DDOS Emergency Contacts

ENTITY/ISP	CONTACT	DATE