DDoS & TDoS – Defending Against the Great Threats

Dan Zeiler CISSP, CISA, CISM, CRISC, CGEIT, CCFP, CHFI, CEH
Director, Cybersecurity Motorola Solutions

Caveats

- This presentation presents my personal and/or professional opinions and does not necessarily reflect the opinion of my employer, APCO, or any other person, living or dead.
- I am not an attorney, please do not take anything within this presentation as legal advice.

Next Generation 9-1-1 Transition

- Next Gen 9-1-1 involves a fundamental shift to IP based technologies, which opens up the scope of attacks that are able to target a PSAP.

- There is a great deal of concern, but also a lack of clear understanding about what this new attack surface looks like, how vulnerable PSAPs really are, and what PSAPs can do to mitigate these threats.

- We'll decompose how these attacks work, what defenses work at which points in the ecology, what defenses can't help, and what we have to do going forward to minimize the attack surfaces exposed to these attacks.

Definitions… What's what?

- **DDoS**
  - Distributed Denial of Service
    - … Lots of IP / network traffic from lots of sources
    - … Might be legit, might be bogus, typically some of both
    - … Always ask if the path for this attack exists or not
    - … Useful directly, also useful to disguise another attack
- **TDoS**
  - Telephony Denial of Service
    - … Lots of phone calls to a PSAP, either on 9-1-1 or on an administrative line
    - … Doesn't matter of it's TDM or SIP or what, it all hurts the same
    - … There are some special use cases around Wireless, VoIP, etc., but don't get lost in those cases, spend your worry where it belongs… the phone is ringing.. ringing… ringing
    - … Remember, everyone knows your main line phone number 9-1-1!
- **Mechanism of Action**
  - How it hurts first, second, and third
    - … Critical for understanding which impact is felt where
    - … Greatly helps determine what defenses can actually help, and where they need to be placed

Common Elements

- All Denial of Service attacks deplete the target resources causing normal traffic to not be responded to properly. This is the universal mechanism of action.

- Optimally, an attacker can deplete these resources asymmetrically (more expensive to defend than attack), but this is not a requirement for a successful attack at all.

- **Example – DNS amplification attack.**
  - In this sort of attack, a DNS query is sent to a third party, with the response from that third party hitting the defender. A small query is sent to the third party with a return path set to the defender. When the third party responds to the "sender", they're actually attacking the defender by sending a large amount of data to them.

- **This can amplify the attacker's striking power by a factor of 10 or more.**

Variable Elements

What the attacker is trying to deplete varies. Typical targets:

- Ingress connectivity
  - … Flood the pipe
  - … Hang sessions (half-pipe)
- Infrastructure impacts
  - … Internal Amplification
  - … Disruption of internal authentication systems
- Human impact
  - … TDoS attacks in particular can hit calltakers
  - … Lower confidence in all systems during an attack
- Service Provider targeted attacks
  - … Effective
  - … Difficult for the defender to engage (standing issues)

DDoS Attacks

DDoS Attack Characteristics

- IP based attack

- Some variation of “lots of junk traffic” or “lots of looks real traffic”
  - TCP / UDP (rarely ICMP)
  - Typically spoofed (false) return address

- Average sized attacks are in the 13-16 gbps range without amplification
  - Note that means ingress is almost certainly saturated
  - Obviously, with amplification, this number can go up very quickly

- Largest attack on record is just over 700 gbps
  - At this magnitude you impact cloud service and cloud based cyber defense service providers without very careful pre-planning

- DDoS attacks grow naturally once initiated

TDoS Attacks

TDoS Attack Characteristics

- Call based attack
  - Doesn't much matter how the call gets to you, SIP, TDM, VoIP, wireline, wireless, etc.
- Calls might present as:
  - Dead air
  - Some sort of sound or DTMF tones on the line
  - Some form of pre-recorded noise, talking, screaming, etc.
- Impacts can vary widely depending on attack sourcing / pattern
  - All lines busy
  - Call taker confusion / distress
  - Caller anger

- Example of a persistent anonymous attack: Converting normal phones into NSI phones, attacking, then re-establishing normal service, or just raiding the dump bin at the local electronics store, charging them up, and turning them loose.
- TDoS attacks grow naturally once initiated

Traffic Path

How do communications get to a PSAP?

Call Traffic

- Originating Service Provider
- Router Operator
  - IPSR
  - ESRP
- ESInet Operator
- Call Handling Solution

Non-call Traffic

- Through a direct internet access (DIA) circuit –or – through an ESInet
- Begs the question of how traffic enters the ESInet (hint, DIA)
- ESInets carry more than just calls: GIS, patching, monitoring, etc.

DDoS attacks as they walk the path

Call Traffic

1. **Originating Service Provider**
2. **Router Operator**
   A. IPSR
   B. ESRP
3. **ESInet Operator**
4. **Call Handling Solution**

Non-call Traffic

1. **Through a direct internet access (DIA) circuit –or – through an ESInet**
2. **Begs the question of how traffic enters the ESInet (hint, DIA)**
3. **Used for GIS, patching, monitoring, etc.**

Call Traffic

1. Should always be delivered as point to point circuits, so no attack surface which can be targeted.
2. Same as #1
3. Only exposed at the edge, proper design can control for the risk.
4. Only exposed to internally generated attacks with proper architecture.

Non-call Traffic

1. DIA is directly targetable, or the provider might be attacked as part of a snowshoe attack.
2. ESInet DIA is targetable as above, but if properly designed, the attack can be contained to the loss of DIA
3. These functions will not work properly for the duration of the attack. Note that the *other end* of these functions may be targeted as well.

TDoS attacks as they walk the path

Call Traffic

1. Originating Service Provider
2. Router Operator
   A. IPSR
   B. ESRP
3. ESInet Operator
4. Call Handling Solution

Non-call Traffic

1. Through a direct internet access (DIA) circuit –or – through an ESInet
2. Begs the question of how traffic enters the ESInet (hint, DIA)
3. Used for GIS, patching, monitoring, etc.

Call Traffic

1. Tandem saturation is the most likely outcome.
   A. E9-1-1 is terribly vulnerable to this
   B. NG9-1-1 is less vulnerable conceptually
2. Routers are vulnerable to being saturated.
3. Most likely other things will break before the ESInet
4. On a small attack, the call takers will be flattened by the workload. On a larger attack, crushed.

Non-call Traffic

Not targeted. Shouldn't be impacted as the paths for call and non-call traffic are physically isolated from one another.

ESInet sizing / saturation is a concern on larger attacks, reproducing the Tandem issues above but for normal IP traffic.

DDoS defenses on the path

Call Traffic

1. Originating Service Provider
2. Router Operator
   A. IPSR
   B. ESRP
3. ESInet Operator
4. Call Handling Solution

Non-call Traffic

1. Through a direct internet access (DIA) circuit –or – through an ESInet
2. Begs the question of how traffic enters the ESInet (hint, DIA)
3. Used for GIS, patching, monitoring, etc.

Call Traffic

1. Shouldn't be able to be targeted. (Agencies, require point to points!)
2. See #1… **BUT** CLECs are required to deliver all 9-1-1 calls, so if targeted successfully…
3. Depends on who operates, but since the ESInet doesn't ever terminate calls, "how" becomes a major question.
4. Has broad authority to address all problems, but it's usually too late if there's an impact.

Non-call Traffic

1. Must have dedicated and purpose built equipment in place in order to mitigate successfully.
2. Worst case, this has to fail at the edge and not come into the ESInet proper.

TDoS defenses on the path

Call Traffic

1. Originating Service Provider
2. Router Operator
   A. IPSR
   B. ESRP
3. ESInet Operator
4. Call Handling Solution

Non-call Traffic

1. Through a direct internet access (DIA) circuit –or – through an ESInet
2. Begs the question of how traffic enters the ESInet (hint, DIA)
3. Used for GIS, patching, monitoring, etc.

Call Traffic

1. Not legally allowed to delete traffic? FCC rule is that the OSP must deliver all 9-1-1 calls. Hamstrung.
2. CLECs are also required to deliver all 9-1-1 calls. Could assign confidence levels.
3. Depends on who it is, but since the ESInet doesn't ever terminate calls, "how" becomes a major question.
4. Has broad authority to address all the problems, but...

Non-call Traffic

Not targeted. Shouldn't be impacted as the paths for call and non-call traffic are physically isolated from one another.

ESInet sizing / saturation is a concern on larger attacks, reproducing the Tandem issues above but for normal IP traffic.

So how do we defend?

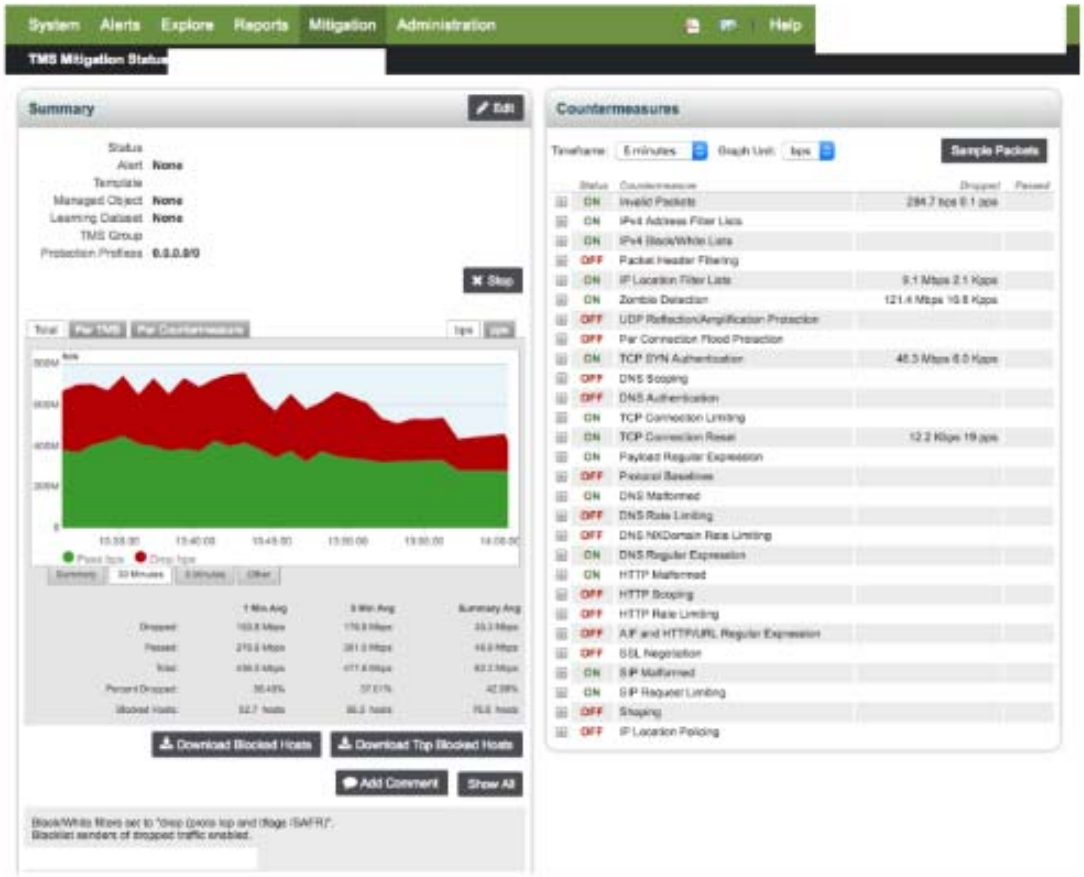
- DDoS defense require dedicated equipment which can play “protocol games”
  - Interacting with the syn / syn-ack / ack process
  - Real time automated creation of blacklists
  - Real time updates of known zombie systems
  - Removal of non-compliant traffic

- Thousands or more packets per second, most of which is attack traffic.

- Note, this is simply not a clean process. It starts “clean” with the removal of anything that can’t ever succeed at proper communications, but you quickly get into a judgment based messy situation.

Anything is better than down!

Specific Cyberthreats for NG deployments



Note that this kind of solution requires trained personnel to manage the events. It helps a great deal if they're experienced in DDoS defense.

Can you achieve similar protections without a dedicated, purpose designed system?

MOTOROLA SOLUTIONS

DDoS Defense Myths

- "We have XYZ amazing routers and they…"
- "Our firewalls are next generation and they…"
- "Our firewalls are layer 7 and they…"
- "Our system sits at the PSAP it protects by…"
- "We can hide you so well nobody will ever find you and…"

Any defense at the PSAP makes the assumption that the inbound paths are not impacted.

At thousands of packets per second, without proper tools and automation assistance, odds of a good outcome are quite low. Pulling thousands of pages of logs from a firewall / router and then trying to read them to determine what *might* be happening *may* have *some* positive impact *maybe*… *sometimes*.

It's just too many asterisks. If you've not built to defend, when the time comes, your options are *extremely* limited.

TDoS Defense Systems

The Originating Service Providers can police / filter somewhat within their areas using a mix of normal validation technologies and proprietary technologies.

The Router Operators (E9-1-1 or NG9-1-1) are largely prevented from taking any meaningful actions by FCC rule. Especially given that defense is not a “clean” thing, the authority to defend, if it’s meaningful, may be unpalatably broad. Note that the Routing functions of NG9-1-1 *if* delivered as IP are going to be a lot more tolerant than the old TDM handoffs because they’re larger and more flexible. Router operators can (and should) assign confidence levels.

The ESInet Operator may architect to be able to take meaningful actions, but must do so in advance. This would consist of being able to adjust traffic flows to a scrubbing solution.

The Call Handling operations can use confidence levels to direct suspect traffic to lower priority queues, or enable automated call back features, or an automated answer + proof of life feature. Significantly not perfect, but these features can have a very positive effect.

Summary

- DDoS and TDoS are related functions, but quite different in how they impact.
- DDoS should never impact calls assuming the routing / route path structures are built to not be exposed to such attacks.
- DDoS typically saturates the connection, and the victim will not have standing to fight until after they're impacted. (If the upstream is offline, what's the PSAP going to do?)
- DDoS requires specialty equipment and specific architectures to fight and engage. Other things can "help" point out who's kicking you around, but you'll need more than that when the time comes.

- TDoS is not currently a cleanly solved problem.
- E9-1-1 is MORE vulnerable than NG9-1-1
- NG9-1-1 is significantly less vulnerable if the OSP delivers as IP (future state)
- Confidence levels should be assigned at the ESRP / SBC / BCF
- PSAPs should be ready with auto-answer / auto call back functionality and queue controls.

Thank You!

For more information, contact:
dan.zeiler@motorolasolutions.com

MOTOROLA SOLUTIONS