Process Control Systems
Industry Conference

When Good Packets Go Bad — How Much Application Traffic Is Too Much?

Reliability / Availability / Security for Industrial Control Systems Networks

Introductions

- **Kevin McGrath**
  - Scientist
    ABB
- **Daniel Peck**
  - Analyst
    Digital Bond
- **Thomas Maufer**
  - Dir., Tech. Mktg.
    Mu Dynamics

What is DoS?

- **Not (only) an operating system**
- **A DoS definition: When the load on a system impairs the system's ability to do its job.**
  - Note: DoS does not imply malice!
  - Note: Systems are often showing signs of impairment at traffic levels far less than wire speed
    - Control vs. forwarding plane aspects
- **DoS is reduced reliability and/or availability**
  - DoS may be a security issue as well

Why do DoS attacks occur?

- **A range of causes result in DoS conditions**
  - Generic Internet threats
  - Insider attack
  - Monetary gain (criminal extortion)
  - Political activism and cyber terrorism
  - Just plain too much traffic
- **DoS is the effect, not the cause**
  - Even when the source of the attack is unintentional and non-malicious, the effect is what's important

Why is DoS a Problem?

- **Vendors lack qualitative metrics showing how independent system components may affect each other**
  - Opportunity to excel in new benchmarks
  - Ensure that these metrics are developed and tracked across the software development life cycle (SDLC)
- **Asset owners lack insight into the reliability and availability of control system networks when the control plane is stressed**
  - Look beyond the forwarding plane to the real sources of performance impairments by measuring live or lab systems

DoS Is Real

- **Brown's Ferry Cyber Incident**
  - ARP broadcast storm?
    - From the NRC report: "***…PLC failure was a likely symptom of the excessive network traffic…***"
- **Amazon S3 Outage**
  - Cloud computing data centers are managed much more like a control system than a traditional IP network
- **Massive DDoS attacks target Estonia**
  - Cyber attacks paralyze government servers

DoS Is Real

- **Brown's Ferry Cyber Incident**
  - ARP broadcast storm?
    - From the NRC report: "...information received from the PLC vendor indicated that the ***PLC failure was a likely symptom of the excessive network traffic***…"
- **Amazon S3 Outage**
  - Cloud computing data centers are managed much more like a control system than a traditional IP network
  - Not industrial control systems, but isn't reliability and availability important here, too?
    - What can we learn from this?

DoS Is Real

- **OPC Security Checker**
  - Langner at S4 2007
  - Resource/Memory Exhaustion

Mitigation (vendors)

- **Technique samples**
  - Syn Cookies
  - Source filtering
  - Rate limiting

- **Logging/Reporting**
  - Best way to keep a minor incident from turning into a major one

Mitigation (owners)

- **What else can asset owners do to prevent another Brown's Ferry type incident?**
  - QoS limits in networks
  - Load balancing & redundant systems (round robin)
- **In any case, though, must test proposed mitigation techniques to ensure they don't themselves degrade service performance**
  - However, these controls may have their own failure modes!

What's Being Done?

- **Vendors**
  - Testing reliability, availability and security throughout SDLC
    - Recognizing the control plane's affect on overall system performance
- **Asset owners**
  - Procurement requirements
  - Factory Acceptance Tests
  - Other testing through the deployment life cycle
    - Documenting hidden performance requirements or scaling limits

Driving Improved Reliability and Availability

- **Improved security helps**
  - Standards efforts
    - ISA99-WG4
    - ISCI
  - Pre-standard testing
- **Other drivers**
  - Industry collaboration
  - Insurance industry
  - Government regulations

How Do We Test Reliability and Availability?

- **Testing DoS involves two aspects**
  - Load + Monitors
    - Generating traffic at precise levels
    - Monitoring something in the network
      - Correlate what effect (if any) arises from the traffic
  - Variations on valid service traffic
    - Discover software defects before they undermine reliability, availability or security
    - Malformed packets — even a small number of them — can cause service degradation or a complete outage
      - Cascading effects within highly interdependent systems

Does Security = Reliability = Availability?

- **Not quite, but it's hard to improve one without improving the others**
- **Industry efforts to improve security are a good first step**
  - It's the hardest problem, so it's good to tackle it first
- **Reliability and Availability can be improved by Asset Owners and Vendors *now***
  - Elimination of software weaknesses or weak system configurations may eliminate some security issues

Demo

- Traffic: TCP SYN Flood against firewall's web-based HTTP management interface
- Monitor: DHCP service in the firewall
- Observe: DHCP stops working as the TCP SYN flood ramps up

- Conclusions?

Q&A

Thanks for attending!