FCoE Threat Model Objectives Discussion

David Black, EMC
Landon Noll, Cisco

T11 Document: 08-338v0

Context: Bottom-up vs. Top-down

- Bottom-up: Extensive security scenario analysis – ACLs and rules
  - Scenario 1g, 3b, etc.
  - ACLs, more ACLs, and yet more ACLs ...
  - This could go on for a long time ...
- Top-down: How do we know when we're done?
  - Set goals to "Define what is important and what is out of scope" (08-212v0)
  - Purpose of this presentation
- Goal: Discussion
  - Will take notes on these slides and post result

Four High-level Objectives (Informal)

1. Virtual FCoE link (Vx_Port to Vx_Port) is like a physical FC link
   - FCoE is a form of FC, link behavior should be common
   - Reuse existing FC technology (FC-SP)
2. Configuration is as expected
   - Links are where they are supposed to be (FIP and afterwards)
3. Keep-alive mechanisms have desired behavior (link lifetime)
   - Link doesn't die too early or too late
   - Diverges from item 1 in presence of Ethernet-only switches (bridges)
4. Underlying Ethernet assumptions are not violated
   - Solid foundation for FCoE-level security analysis (e.g., duplicate MAC issues)
   - Reuse existing Ethernet technology (e.g., 802.1x)

- Are these the right high level objectives?
- Anything obvious missing?

1. FCoE: Virtual link is like a physical FC link

- Security properties no worse than physical FC link (FC-0 + FC-1)
  - Do not hold FCoE to a higher standard than native FC
- Confidentiality: None
  - See FC-SP for confidentiality
- Integrity: Non-cryptographic (CRC-grade)
  - See FC-SP for cryptographic integrity
- Availability: Frame delivery as reliable as physical FC
  - Ethernet switches (bridges) provide new opportunities for non-delivery

2. Configuration is as Expected

- FIP creations of virtual links
  - FIP Protocol operates from configuration data
  - FIP is responsible for doing what it's told
  - FIP is not responsible for bad instructions producing bad results
- Virtual link configuration
  - Links stay where they are supposed to be (no hijacking)
  - Link lifetime is mostly item 3 (next slide)

3. Keep alive mechanisms (virtual link lifetime)

- Virtual link stays alive as long as endpoints are alive
- Virtual link is terminated promptly when intended

4. Underlying Ethernet assumptions

- Ethernet assumptions made in working on the previous 3 items
  - Things that have to be “right” for FCoE level analysis to “make sense”
- MAC address duplication (absence of)
- Learning behavior issues (e.g., per-VLAN learning)