Design Guidelines for Robust Internet Protocols

Tom Anderson, Scott Shenker, Ion Stoica, David Wetherall

Ankit Singla

CS 598

Oct. 27, 2009

Complete vs. Arbitrary Failure

- Internet protocols were designed assuming fail-stop systems
- Robustness to such failures is founded on a set of design principles
  - End-host recovery
  - Refresh critical state regularly
  - Assume failures are common
- But arbitrary failures are different - syntactic vs. semantic correctness

Broad Ideas

- Arbitrary failures occur often enough in the Internet
- Other methods fail against these
  - Cryptographic authentication
  - Fault-tolerance via consensus
  - Formal verification of protocols
- Long term solution - formulate design guidelines (Require RFC section addressing these?)
- Focus on *defensive design*

Guideline #1: Value Conceptual Simplicity

- Multiple parties implementing complex functions can break things
- Example: Persistent route oscillations in BGP

Guideline #2: Minimize Your Dependencies

- Trust is often misplaced
  - Variety of agents with different motives
- TCP send-receive co-ordination and fast recovery

Guideline #3: Verify When Possible

- When dependencies are necessary, try verification
  - Actively test node responses
  - Compare information from other sources
- Verification need conflicts with KISS paradigm
- But often, there are simple solutions
  - ECN modification

Guideline #4: Protect Your Resources

- Unsolicited requests can lead to resource exhaustion
- Example: DoS attacks based on SYN-Floods
- The conserving resources approach does well against SYN-Floods

Guideline #5: Limit the Scope of Vulnerability

- Damage control is also important
- Route flapping in BGP
- The damping based solution limits propagation of updates
- Another Example: BGP error processing

Guideline #6: Expose Errors

- Actively seek out and expose errors
  - TCP checksum failure discovery
  - Flaw in BGP configuration strategy

Discussion

- How good an idea is an RFC 'Robustness Considerations' section?
- Any more design principles ideas?

Thank You!