Resilient and Survivable Networking
The University of Kansas EECS 983
Traffic Tolerance

James P.G. Sterbenz

Department of Electrical Engineering & Computer Science
Information Technology & Telecommunications Research Center
The University of Kansas

jpgs@eecs.ku.edu

http://www.ittc.ku.edu/~jpgs/courses/rsnets

09 March 2010
Resilient and Survivable Networking
Traffic Tolerance

TT.1 Overview and definitions
TT.2 Techniques and mechanisms
Traffic Tolerance

TT.1 Overview and Definitions

TT.1 Overview and definitions
   TT1.1 Definition
   TT1.3 Relationship to other disciplines

TT.2 Techniques and mechanisms
Traffic Tolerance

Definition

- Traffic tolerance
  - ability to avoid service failures
    - significant drop in carried load including congestion collapse
  - in the presence of traffic
    - beyond design specification of network
    - expected for normal operation
Traffic Tolerance

Challenges: Legitimate Flash Crowd

• Flash crowd
  - legitimate traffic beyond expected for normal operation

• Occurs in response to a triggering event
  - disaster or significant news event
    • can overwhelm new Web sites
    • can overwhelm mobile telephone networks
  - publicity for an obscure Web site called slash-dotting
    • article on slashdot.org frequently brings down Web servers
Traffic Tolerance

Challenges: Malicious DoS

- **DoS**: denial of service attack
  - injection of information or traffic
    - traffic competing with legitimate users
    - signalling messages that prevent normal access
    - jamming of RF signals
  - intended to deny access to a resource
    - reduce availability or cause total failure of a system
  - can frequently be traced to source
    - throttled or shut down
Traffic Tolerance
Challenges: Malicious DDoS

- **DDoS**: distributed denial of service attack
  - distributed DoS
    - intended to deny access to a resource as with DoS
  - injection of traffic from *many* sources
    - far more difficult to shut down than single-source DoS
    - sufficiently sophisticated DDoS attack indistinguishable from legitimate traffic
Fault Tolerance

Relationship to Other Disciplines

- Trustworthiness
  - Dependability
    - reliability
    - maintainability
    - safety
  - availability
    - integrity
  - confidentiality
  - nonrepudiability
  - Security
    - audibility
    - authorisability
    - authenticity
  - Performability
    - QoS measures

- Robustness Complexity
- Challenge Tolerance
  - Survivability
    - many \( \land \) targeted failures
  - Disruption Tolerance
    - environmental delay
    - mobility
    - connectivity
    - energy
  - Fault Tolerance (few \( \land \) random)
  - Traffic Tolerance
    - legitimate flash crowd
    - attack DDoS

- Dependability
- Maintainability
- Safety
- Availability
- Integrity
- Confidentiality
- Nonrepudiability
- Audibility
- Authorisability
- Authenticity
- QoS Measures
Traffic Tolerance

TT.2 Techniques and Mechanisms

TT.1 Overview and definitions

TT.2 Techniques and mechanisms
   TT2.1 Attack detection
   TT2.2 Mitigation
TT Techniques and Mechanisms

TT.2.1 Attack Detection

TT.1 Overview and definitions

TT.2 Techniques and mechanisms
   TT2.1 Attack detection
   TT2.2 Mitigation
Traffic Tolerance

Attack Detection

• **Attack detection techniques**
  - attempt to distinguish malicious from legitimate traffic
  - cat-and-mouse game
    • as detection improves…
      …attackers become more sophisticated
  - sufficiently sophisticated DDoS attack
    indistinguishable from legitimate traffic
    • motivates need for mitigation techniques
TT Techniques and Mechanisms

TT.2.2 Mitigation

TT.1 Overview and definitions

TT.2 Techniques and mechanisms
  TT2.1 Attack detection
  TT2.2 Mitigation
Traffic Tolerance
Mitigation Techniques

• Traffic mitigation
  - defend and remediate against traffic challenges
  - malicious (DDoS) and legitimate (e.g. flash crowds)

• Goals
  - protect target of traffic challenge (e.g. Web server)
  - isolate from other flows
Traffic Tolerance

References and Further Reading

References on
wiki.ittc.ku.edu/resilinets/Traffic_Tolerance

[JRK2002] J. Jung, B. Krishnamurthy, and M. Rabonovich,
"Flash Crowds and Denial of Service Attacks:
Characterization and Implications for CDNs and Web Sites",
ACM 11th WWWC, May 2002, pp. 532–569

[XPH+2008] L. Xie, P. Smith, D. Hutchison, M. Banfield, H.
Leopold, A. Jabbar, and J.P.G. Sterbenz,
"From Detection to Remediation: A Self-Organized System for
Addressing Flash Crowd Problems",
IEEE ICC'08, May 2008, pp. 5809–5814
End of Foils