

WebSOS: an overlay-based system for protecting
web servers from denial of service attacks

A. Stavrou, D. L. Cook,
W. G. Morein, A. D. Keromytis, V. Misra, D. Rubenstein
Computer Networks 48 (2005)



Presented by
Yuttasart Nitipaichit
IS 3957 (Ph.D. Seminar 2006)

Telecommunications Program
University of Pittsburgh

Motivation

- Internet & E-commerce gain more popularity
- Web Servers is a target of DoS
- Many vulnerable hosts being used as DDoS
- DDoS attack is difficult to prevent
- Traditional approaches: Monitoring and blocking malicious traffic once detected via traffic pattern & packet header analysis
- Require more effective way

Topic here

Telecommunications Program
Ph.D. Seminar Spring 2006

Slide: 2

Outline



- WebSOS Architecture
- Simulation
- Implementation
- Evaluation
- Conclusion

Topic here

Telecommunications Program
Ph.D. Seminar Spring 2006

Slide: 3

Overview



- WebSOS, an adaptation of the Secure Overlay Services (SOS) architecture Intended to prevent congestion-based DDoS attacks from denying any users access to web servers targeted
 - Use strong client authentication to identify legitimate traffic
 - Make use of Graphic Turing Tests to distinguish between human users and automated attack zombies
 - transparency to browsers and servers
 - WebSOS itself protects only web traffic but can be used to enable routing of other types of traffic by establishing IPsec tunnels through the overlay

Topic here

Telecommunications Program
Ph.D. Seminar Spring 2006

Slide: 4