

Automated Adaptive Intrusion Containment in Systems of Interacting Services

Yu-Sung Wu, Bingrui Foo, Yu-Chun Mao, Saurabh Bagchi, Eugene Spafford+
Dependable Computing System Lab (DCSL) & CERIAS
School of Electrical and Computer Engineering + School of Computer Science
Purdue University



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

Telecommunications Program
University of Pittsburgh

Motivation



- There're several causes of failure: natural failure or from malicious activities.
- Failure propagation can cause a lot of damage.
- To make our system tolerant to failures, it's necessary to contain the spread of failures once detected.
- In the face of failure we need our system to continue to provide partial functionality

Topic here

Telecommunications Program
Ph.D. Seminar Spring 2006

Slide: 2

Outline



- Overview of paper
- ADEPTS
 - I-Graph
 - Attack sub graph
 - How it works
- Implementation of ADEPTS
- Experiments and results
- Conclusion

Topic here

Telecommunications Program
Ph.D. Seminar Spring 2006

Slide: 3

Overview



- Present the design and implementation of a system named ADEPTS
 - *ADEPTS uses a directed graph representation to model the spread of the failure through the system*
 - *Presents algorithms for determining appropriate responses and monitoring their effectiveness*
 - *quantifies the effect of disruptions through a high level survivability metric*
- *Demonstrate it on a real e-com testbed*

Topic here

Telecommunications Program
Ph.D. Seminar Spring 2006

Slide: 4