ADEPTS: Automated Adaptive Intrusion Response
Yu-Sung Wu    Bingrui Foo    Matthew Glause    Saurabh Bagchi    Eugene Spafford

**Goal:** To design an automated intrusion response system that increases the survivability of distributed systems

**Key features**
- Adaptation in response decision algorithm
- Attack pattern matching for known attacks
- Ability to handle unanticipated attacks

---

**E-commerce testbed**

- **Client**
- **Load balancer**
- **Apache**
- **Warehouse**
- **MySQL**

**ADEPTS control center**

- **Detector alerts**
- **Unanticipated alerts**
- **Locality segmentation**
- **Subgraph creation/update**
- **Response feedback**
- **Response deployment/revocation**
- **I-GRAPH**
- **S-Net**
- **Petri dish**
- **Immunizer**
- **Distiller**

**Fragment of an attack scenario**

- A. Send Apache chunk buffer overflow packets
- B. Send Apache mod_ssl buffer overflow packets
- C. Stack-based buffer overflow Apache
- D. Heap-based buffer overflow Apache
- E. Inject malicious code into Apache
- F. IP/port scan to find SQL server
- G. Send SQL buffer overflow packets
- H. Guess SQL account password
- I. Stack-based buffer overflow SQL
- J. Login to SQL server
- K. Create malicious shell with SQL privileges
- L. Access SQL database directory

**Current work**

- Synthesize new responses at runtime
- Variable expiration periods of responses
- Optimality of responses

---

**Table of Attack Instances and Responses**

| Attack instance | (Responses deployed), after which step, (S|F) | Steps achieved before attack stopped | Response | Description |
|----------------|--------------------------------------------|--------------------------------------|----------|-------------|
| 1              | (R0,R1), L, (F)                           | A, C, E, F                           | R0       | Block attacker IP from port 80 of Apache server |
| 2              | (R4), F, (F)                              | B, D, E, F, H, J, L                 | R2, R3, R5, R6, R9 | Block attacker IP from accessing Apache server |
| 3              | (R7,R8), C, (S)                           | A, C                                 | R3, R7   | Restarting Apache server |
| 4              | (R9), F, (S)                              | B, D, E, F                           | R4       | Block attacker IP from port 443 of Apache server |
|                |                                            |                                      | R5       | Restart MySQL server |