CERIAS

ADEPTS

Adaptive Intrusion Response using Attack Graphs in an E-commerce Environment

Dependable Computing Systems Lab
Secure & Dependable Distributed Systems

Department of Electrical and Computer Engineering
Purdue University

Members

Faculty: Saurabh Bagchi
Students: Yu-Sung Wu
Bingrui Foo
Yu-Chun Mao

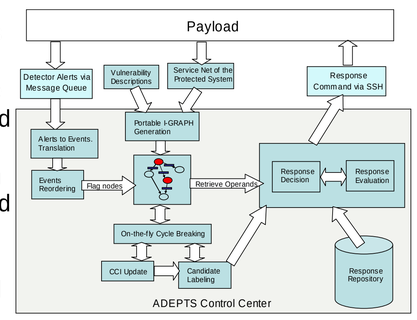
URL: http://shay.ecn.purdue.edu/~dcsl/

Motivation

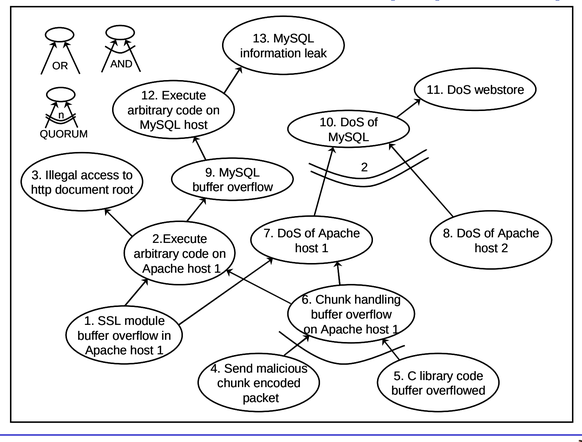
- E-commerce characterized by distributed systems with complex interacting services
- E-commerce systems are prime candidates for intrusions due to huge financial stakes
- Only rudimentary response mechanisms available within present anti-virus products and intrusion detection systems
- Absence of comprehensive automated intrusion response systems

Process Flow

1. Detection framework flags alerts
2. I-GRAPH parameters updated
3. Best locations to take responses determined
4. Available responses determined based on attack parameters and I-GRAPH
5. Best responses chosen and deployed
6. Evaluation of active responses



Partial View of Intrusion Graph (I-GRAPH)



Determining how likely a node is compromised

- The *Compromised Confidence Index* (CCI) of a node in the I-GRAPH is the measure of the likelihood that an attacker has reached that node

$$CCI = \begin{cases} \text{alert confidence} & \text{, nodes with no children} \\ f'(CCI_i) & \text{, nodes with no detectors} \\ f(f'(CCI_i), \text{alert confidence}) & \text{, otherwise} \end{cases} \qquad f' = \begin{cases} \max(CCI_i) & \text{, OR edges} \\ \min(CCI_i) & \text{, AND edges} \\ \begin{cases} \text{Mean}(CCI_i \mid CCI_i > \tau N) & \text{, quorum met} \\ 0 & \text{, quorum not met} \end{cases} \end{cases}$$

where CCI_i corresponds to the CCI of the i^{th} child and τN is a per node threshold

Picking Resposes

- After determining a set of likely-compromised nodes, the response decision module will search the response repository for the responses whose opcodes and operands are applicable to the intrusions on these compromised nodes.

Feedback Mechanism

- After responses are deployed, we can judge whether the deployed responses are effective or not by checking if intrusions are still propagating (higher level nodes in the I-GRAPH keep getting flagged). ADEPTS will then adjust the EI values of the responses so that effective responses will be more preferable in a future run.

Survivability Metric

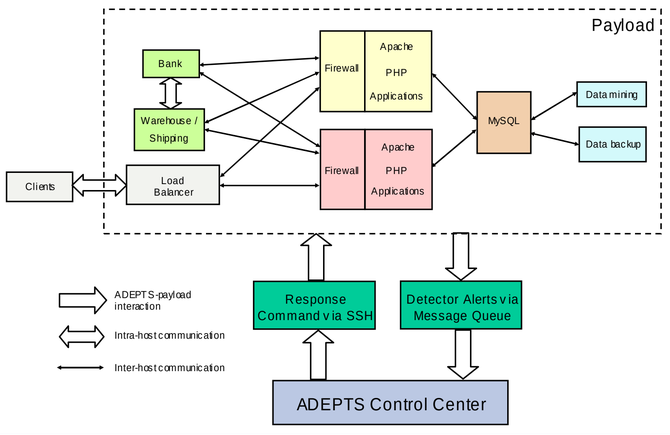
- We define a set of transactions (ex: browsing the webstore and buying products) and a set of security goals (ex: confidentiality of customer's information). We use the survivability metric in the experiment to demonstrate the benefit of adopting ADEPTS in terms of maintaining the survivability of the underlying E-Commerce system.

$$\text{Survivability} = 1000 - \sum \text{unavailable transactions} - \sum \text{failed security goals}$$

Response Repository

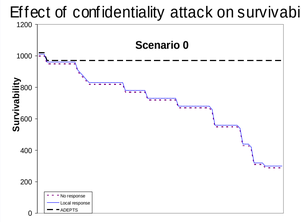
Command type	Commands		Explanation
	Opcode	Operands (oprl And opr2 And ...)	
General	KILL_PROCESS	PROCESS_ID	Kill process
	SHUT_DOWN	SERVICE_NAME / HOST	Shutdown/restart a service/host
	RESTART/REBOOT	SERVICE_NAME / HOST	
	DISABLE	USER_ACCOUNT	Freeze a user account
File	DENY_FILE_ACESS	FILE_NAME	Disable read, write, and execute access to a file, valid for the super user.
	DISABLE_READ	FILE_NAME	Disable read/write access to a file, valid for the super user.
	DISABLE_WRITE	FILE_NAME	
Network	BLOCK_INPUT	REMOTE_IP	Blocking incoming packets associated with the command operands.
		REMOTE_IP/LOCAL_PORT	
		REMOTE_PORT PROTOCOL	
		LOCAL_PORT	
	BLOCK_OUPUT	REMOTE_IP	Blocking outgoing packets associated with the command operands.
		REMOTE_IP/LOCAL_PORT	
		REMOTE_PORT PROTOCOL	
		LOCAL_PORT	
	BLOCK_FORWARD	SOURCE_IP/DESTINATION_IP	Blocking forwarding packets associated with command operands.
DoS	LIMIT_RATE	SYN	Limiting rates of a type of packets
		ICMP_ECHO	
		ICMP_HOST_UNREACHABLE	
		SYN_ACK	
		UDP_PACKET	

Testbed

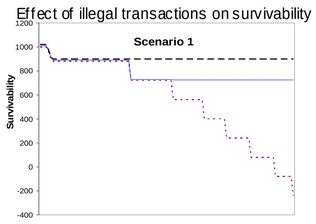


Experimental Results

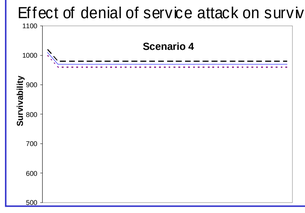
Effect of confidentiality attack on survivability



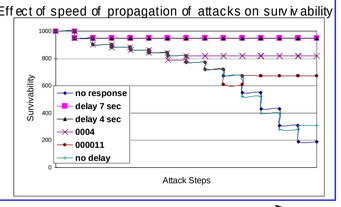
Effect of illegal transactions on survivability



Effect of denial of service attack on survivability



Effect of speed of propagation of attacks on survivability



PURDUE UNIVERSITY

CERIAS®

Discovery Park e-Enterprise Center