

Shifting the Focus of Survivability: Back to the Basics

A. Krings, S. Harrison,

Computer Science Department

University of Idaho

M. McQueen, S. Matthews

Idaho National Engineering & Environmental Laboratory
(INEEL)

What is Survivability?

◆ Network and Computer Survivability

– Definition:

“Survivability is the capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents”

[Ellison1997]

“Survivability is the ability of a computer-communication system-based application to satisfy and to continue to satisfy certain critical requirements (e.g., specific requirements for security, reliability, real-time responsiveness, and correctness) in the face of adverse conditions.”

[Neumann 2000]

Partitioning the Problem

The “Three R’s” [Ellison 1997]

Resist

- » intrusion prevention

Recognize

- » intrusion detection

Recover

- » “take a lick’n and keep on tick’n”

Our Focus

Adaptation

- » adapt, learn, ...

Key Question

“What is the lowest level of complexity at which attacks exhibit distinct, observable characteristics?”

◆ Two key Issues

- Level of complexity
 - » Low complexity solutions promise higher real-time potential

- Characteristics of attack class
 - » e.g. low level attack
 - DDoS attacks may be detected
 - Stealth attacks unlikely to show distinctive characteristics

Standard User Environment

◆ Target System

- Typical desktop computer, e.g. Pentium 1GHz
- Mostly operated by single individual
- Standard applications
 - » browser, email, ftp, telnet, multi-media, text processor, etc.

◆ System Characteristics

- Low utilization!
 - » linux `top` command
- “Idle Profile” of system is surprisingly clean

Passive and Active Survivability

- ◆ Similar to passive and active redundancy in fault-tolerance

- ◆ Passive Survivability
 - Employs implicit techniques
 - » e.g. authentication, fault masking using redundancy

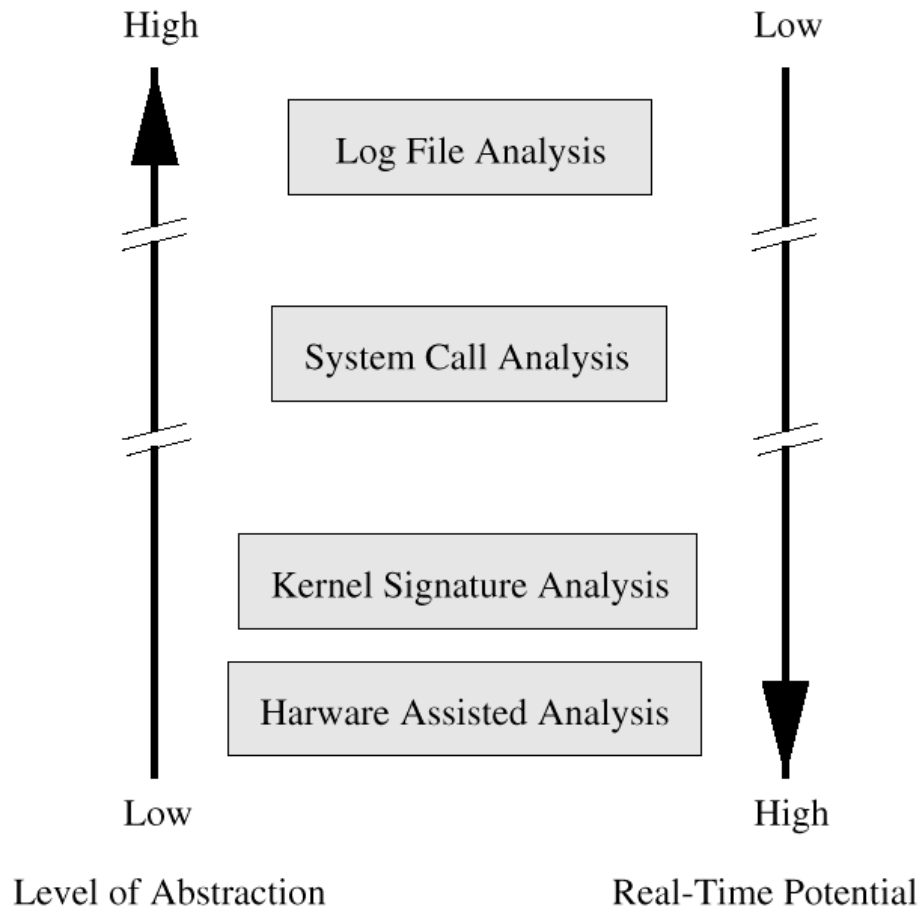
- ◆ Active Redundancy
 - requires recognition of event, e.g. malicious attack, as first step in sequence leading to recovery

Attack Recognition

- ◆ Attack Signature Detection
 - ideally requires a priori knowledge of *all* attack scenarios
- ◆ Anomaly Detection
 - requires full knowledge of expected system behavior
- ◆ Neither strategy can achieve complete realistic detection coverage

Levels of Abstraction

◆ Real-time Potential



Off-line and On-line Survivability

◆ Off-line Design Process

- clean system environment (off-line, no applications)
- creation of attack signature database
- attack signatures aid in identification of critical functions
- implementation of reactionary mechanisms
 - » low level (kernel handlers) -- high level (migratory agents)
 - » a priori matching of critical functionalities with critical functions

◆ On-line (real-time) Protective Capabilities

- real-time attack recognition
- at kernel level
 - » survivability handlers get invoked (independent of attack recognition)
- at high level
 - » recognition triggers response agents

Profiles

- ◆ We view a system as a collection of profiles of its functionalities P_i

$$P_{sys}(\Delta t) = \sum_{i=1}^k P_i(\Delta t)$$

k is the number of functionalities active during Δt

- ◆ Functionality Profile

$$P_i(\Delta t) = (f_1(\Delta t), f_2(\Delta t), \dots, f_n(\Delta t))$$

$f_j(\Delta t)$ is the number of times identity F_j has been invoked during Δt

Attack Signatures

- ◆ Atomic Attacks A_i
 - the smallest attack technology unit
 - e.g. a port sweep, sequence of unsuccessful login attempts
- ◆ Attack Signature S_i
 - the portion of a profile that is attributable to A_i

$$S_i(\Delta t) = (f_{\alpha(1)}(\Delta t), f_{\alpha(2)}(\Delta t), \dots, f_{\alpha(s_i)}(\Delta t))$$

α is a one-to-one mapping from indices of S_i to indices of the identities F_j profiled

Real-Time Attack Recognition

◆ Vector Analysis

- Profile $P_i(\Delta t)$, Idle Signature $S_0(\Delta t)$, and Attack Signature $S_i(\Delta t)$ are vectors

◆ “Strictly Speaking”

- there are three possible scenarios

$P_{sys}(\Delta t) \geq S_i(\Delta t)$ possible attack

$P_{sys}(\Delta t) \neq S_i(\Delta t)$ attack not possible

$P_{sys}(\Delta t) < S_i(\Delta t)$ attack not possible

How related are Attacks?

- Limitation of Signatures
 - » reactionary, e.g. similar to virus definitions
 - » always one step behind attacker
- however:
 - » are we always one step behind?

“How related are attacks?”

Signature Analysis

- Relationship between Signatures

$$\mathbf{S}_i \subseteq \mathbf{S}_j$$

- Common functions

$$\mathbf{S}_i \cap \mathbf{S}_j$$

- Signature Correlation

$$C(i, j) = \frac{|\mathbf{S}_i \cap \mathbf{S}_j|}{\min(|\mathbf{S}_i|, |\mathbf{S}_j|)}$$

Correlation

◆ “Some things seem too good to be true”

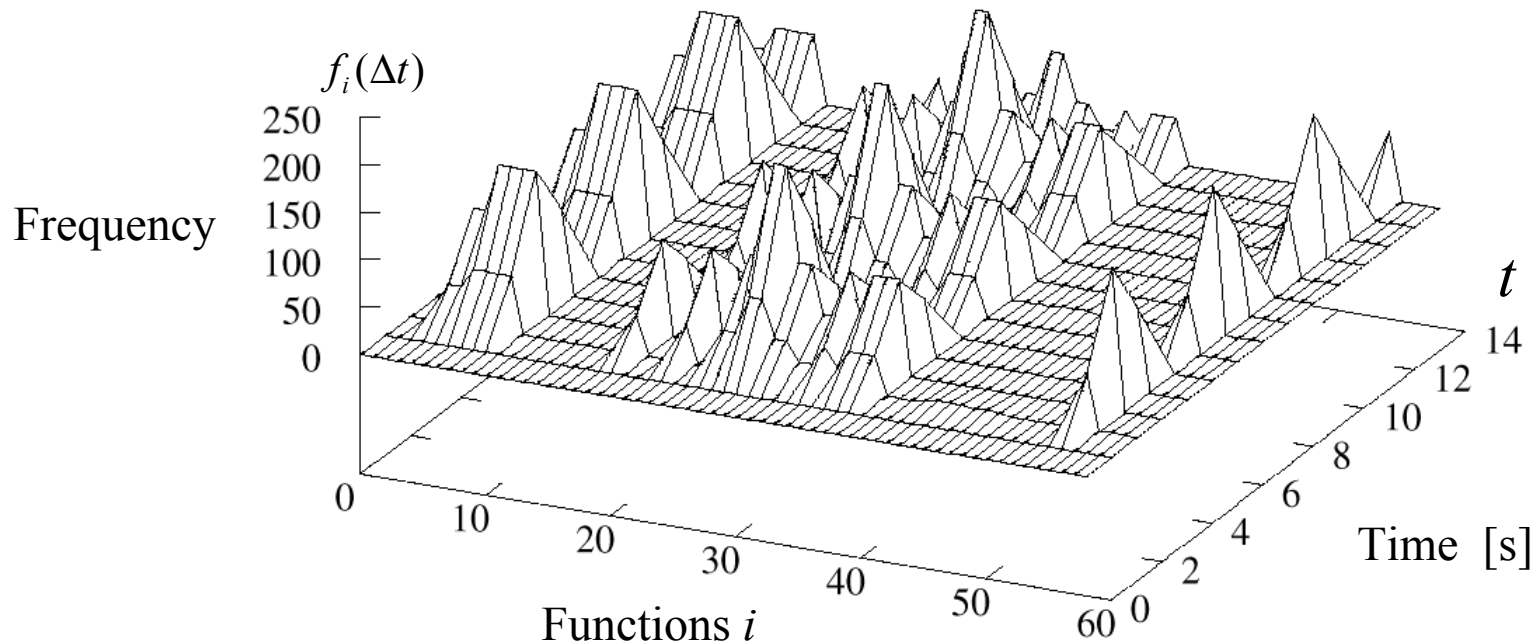
		13	13	18	18	18	18	20	20	21	21	21	21	21	21	22	22	24	35	35	37	42	45	51	57	135	164	194
		conseal	misfrag	fawx	jolt	pimp2	ssping	flushot	trash	boink	bonk	newtear	syndrop	teardrop	nestea	smack	dcd3c	beer	spiffit	biffit	synhose	land	pepsi	trash2	gewse	gewse5	hiperbomb2	
13	conseal	1.00	0.85	0.85	0.85	0.85	0.85	0.85	0.85	0.85	0.85	0.85	0.85	0.85	0.85	0.85	0.85	0.85	0.92	0.92	0.92	0.85	0.92	0.92	0.85	0.85	0.85	0.85
13	misfrag	0.85	1.00	0.85	0.85	0.85	0.85	0.85	0.85	0.85	0.85	0.85	0.85	0.85	0.85	0.92	0.92	1.00	0.85	0.85	1.00	0.77	0.85	0.85	1.00	1.00	1.00	1.00
18	faw x	0.85	0.85	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.61	0.61	0.61	0.61	0.61	0.61	0.61	0.67	0.61	1.00	0.61	0.61	0.61
18	jolt	0.85	0.85	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.61	0.61	0.61	0.61	0.61	0.61	0.61	0.67	0.61	1.00	0.61	0.61	0.61
18	pimp2	0.85	0.85	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.61	0.61	0.61	0.61	0.61	0.61	0.61	0.67	0.61	1.00	0.61	0.61	0.61
18	ssping	0.85	0.85	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.61	0.61	0.61	0.61	0.61	0.61	0.61	0.67	0.61	1.00	0.61	0.61	0.61
20	flushot	0.85	0.85	1.00	1.00	1.00	1.00	1.00	1.00	0.90	0.90	0.90	0.90	0.90	0.90	0.55	0.55	0.55	0.55	0.55	0.55	0.65	0.60	0.55	1.00	0.65	0.60	0.55
20	trash	0.85	0.85	1.00	1.00	1.00	1.00	1.00	1.00	0.90	0.90	0.90	0.90	0.90	0.90	0.55	0.55	0.55	0.55	0.55	0.55	0.65	0.60	0.55	1.00	0.65	0.60	0.55
21	boink	0.85	0.85	1.00	1.00	1.00	1.00	0.90	0.90	1.00	1.00	1.00	1.00	1.00	1.00	0.52	0.52	0.52	0.52	0.52	0.52	0.52	0.62	0.52	1.00	0.52	0.52	0.52
21	bonk	0.85	0.85	1.00	1.00	1.00	1.00	0.90	0.90	1.00	1.00	1.00	1.00	1.00	1.00	0.52	0.52	0.52	0.52	0.52	0.52	0.52	0.62	0.52	1.00	0.52	0.52	0.52
21	new tear	0.85	0.85	1.00	1.00	1.00	1.00	0.90	0.90	1.00	1.00	1.00	1.00	1.00	1.00	0.52	0.52	0.52	0.52	0.52	0.52	0.52	0.62	0.52	1.00	0.52	0.52	0.52
21	syndrop	0.85	0.85	1.00	1.00	1.00	1.00	0.90	0.90	1.00	1.00	1.00	1.00	1.00	1.00	0.52	0.52	0.52	0.52	0.52	0.52	0.52	0.62	0.52	1.00	0.52	0.52	0.52
21	teardrop	0.85	0.85	1.00	1.00	1.00	1.00	0.90	0.90	1.00	1.00	1.00	1.00	1.00	1.00	0.52	0.52	0.52	0.52	0.52	0.52	0.52	0.62	0.52	1.00	0.52	0.52	0.52
22	nestea	0.85	0.85	1.00	1.00	1.00	1.00	0.90	0.90	1.00	1.00	1.00	1.00	1.00	1.00	0.50	0.50	0.50	0.50	0.50	0.50	0.50	0.59	0.50	0.95	0.50	0.50	0.50
22	smack	0.85	0.92	0.61	0.61	0.61	0.61	0.55	0.55	0.52	0.52	0.52	0.52	0.52	0.50	1.00	1.00	0.55	0.59	0.59	0.73	0.64	0.77	0.68	0.55	0.55	0.55	
24	dcd3c	0.85	0.92	0.61	0.61	0.61	0.61	0.55	0.55	0.52	0.52	0.52	0.52	0.52	0.50	1.00	1.00	0.50	0.54	0.54	0.75	0.63	0.75	0.67	0.50	0.50	0.50	
35	beer	0.85	1.00	0.61	0.61	0.61	0.61	0.55	0.55	0.52	0.52	0.52	0.52	0.52	0.50	0.55	0.50	1.00	0.77	0.77	0.57	0.71	0.77	0.77	0.80	0.74	0.80	
35	spiffit	0.92	0.85	0.61	0.61	0.61	0.61	0.55	0.55	0.52	0.52	0.52	0.52	0.52	0.50	0.59	0.54	0.77	1.00	1.00	0.43	0.86	1.00	0.91	0.66	0.60	0.66	
37	biffit	0.92	0.85	0.61	0.61	0.61	0.61	0.55	0.55	0.52	0.52	0.52	0.52	0.52	0.50	0.59	0.54	0.77	1.00	1.00	0.41	0.86	1.00	0.92	0.62	0.57	0.62	
42	synhose	0.92	1.00	0.61	0.61	0.61	0.61	0.65	0.65	0.52	0.52	0.52	0.52	0.52	0.50	0.73	0.75	0.57	0.43	0.41	1.00	0.50	0.50	0.57	0.67	0.64	0.62	
45	land	0.85	0.77	0.67	0.67	0.67	0.67	0.60	0.60	0.62	0.62	0.62	0.62	0.62	0.59	0.64	0.63	0.71	0.86	0.86	0.50	1.00	0.87	0.96	0.47	0.42	0.47	
51	pepsi	0.92	0.85	0.61	0.61	0.61	0.61	0.55	0.55	0.52	0.52	0.52	0.52	0.52	0.50	0.77	0.75	0.77	1.00	1.00	0.50	0.87	1.00	0.86	0.45	0.41	0.45	
57	trash2	0.92	0.85	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	0.95	0.68	0.67	0.77	0.91	0.92	0.57	0.96	0.86	1.00	0.44	0.39	0.40	
135	gew se	0.85	1.00	0.61	0.61	0.61	0.61	0.65	0.65	0.52	0.52	0.52	0.52	0.52	0.50	0.55	0.50	0.80	0.66	0.62	0.67	0.47	0.45	0.44	1.00	0.99	0.95	
164	gew se5	0.85	1.00	0.61	0.61	0.61	0.61	0.60	0.60	0.52	0.52	0.52	0.52	0.52	0.50	0.55	0.50	0.74	0.60	0.57	0.64	0.42	0.41	0.39	0.99	1.00	0.96	
194	hiperbomb2	0.85	1.00	0.61	0.61	0.61	0.61	0.55	0.55	0.52	0.52	0.52	0.52	0.52	0.50	0.55	0.50	0.80	0.66	0.62	0.62	0.47	0.45	0.40	0.95	0.96	1.00	

Attack Signature

◆ Attack Signature over Time

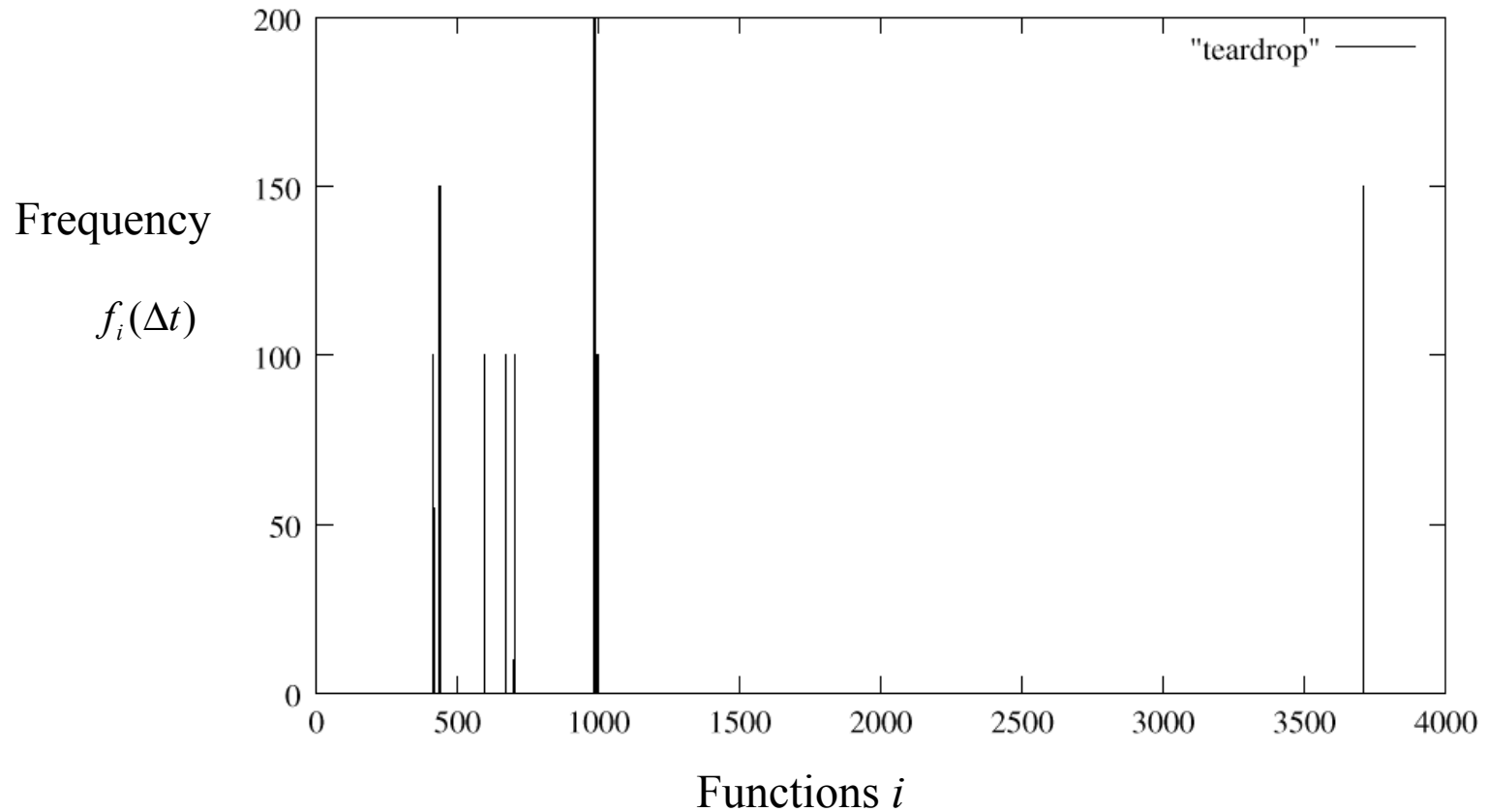
- Example: “teardrop”

(overlapping IP(TCP) fragments are formatted to cause reassembly crashes)



Attack Signature

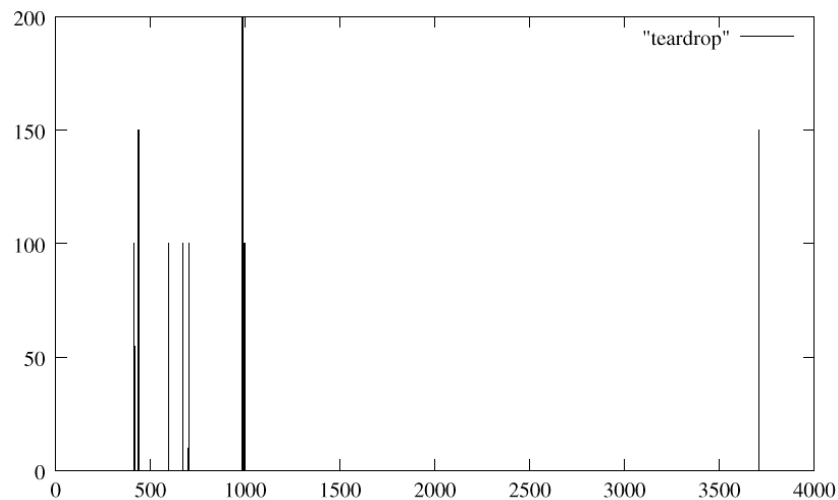
◆ Example “teardrop”



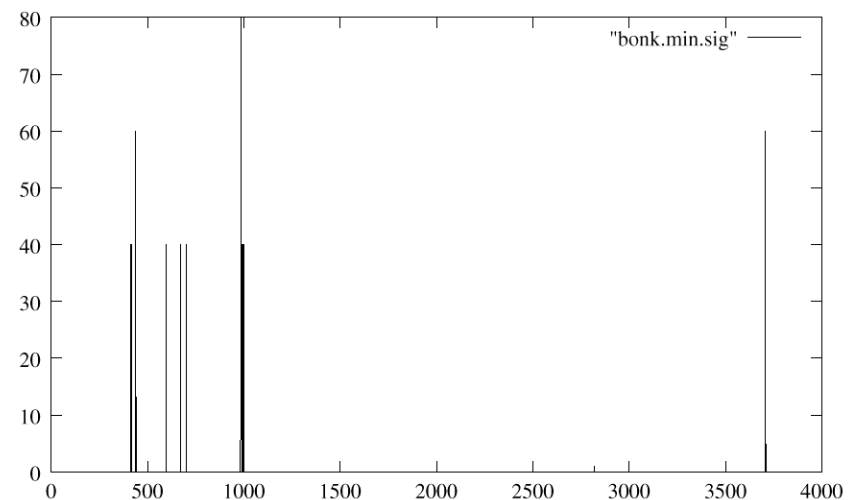
Attack Signature

◆ Example “teardrop” vs. “bonk”

- bonk: malformed IP header causes packet size violation upon reassembly
- Note: scales differ
- Correlation is 1.0



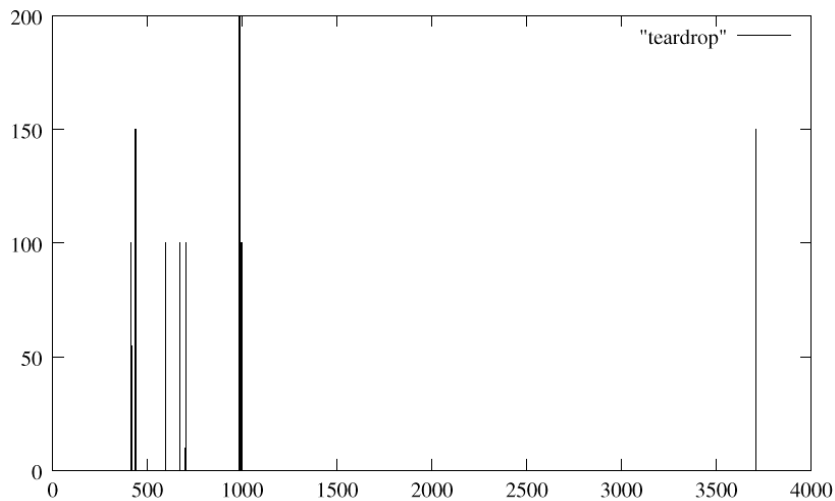
teardrop attack



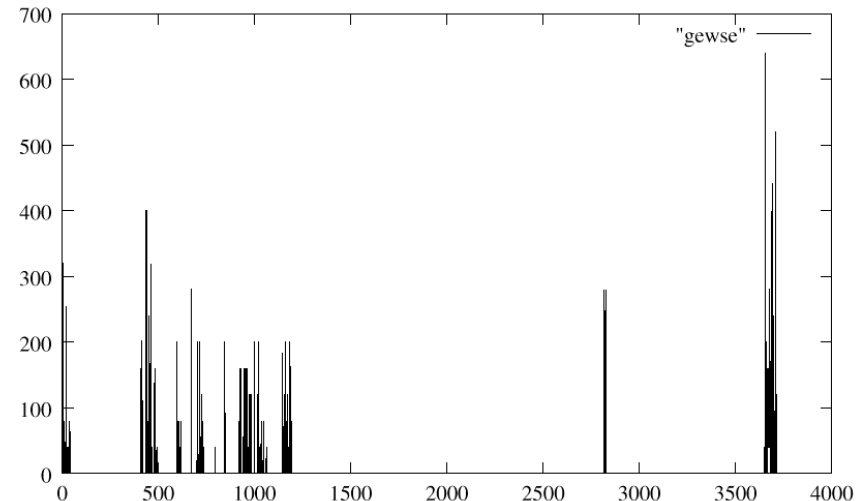
bonk attack

Attack Signature

- ◆ Example “teardrop” vs. “gewse”
 - Gewse: (DoS - attack) floods identd on port 139
 - Note: scales differ
 - Correlation is 0.54



teardrop attack



gewse attack

Two Layers of the Architecture

◆ Low-level Event Handlers

- Survivability handlers
- Currently used for kernel instrumentation

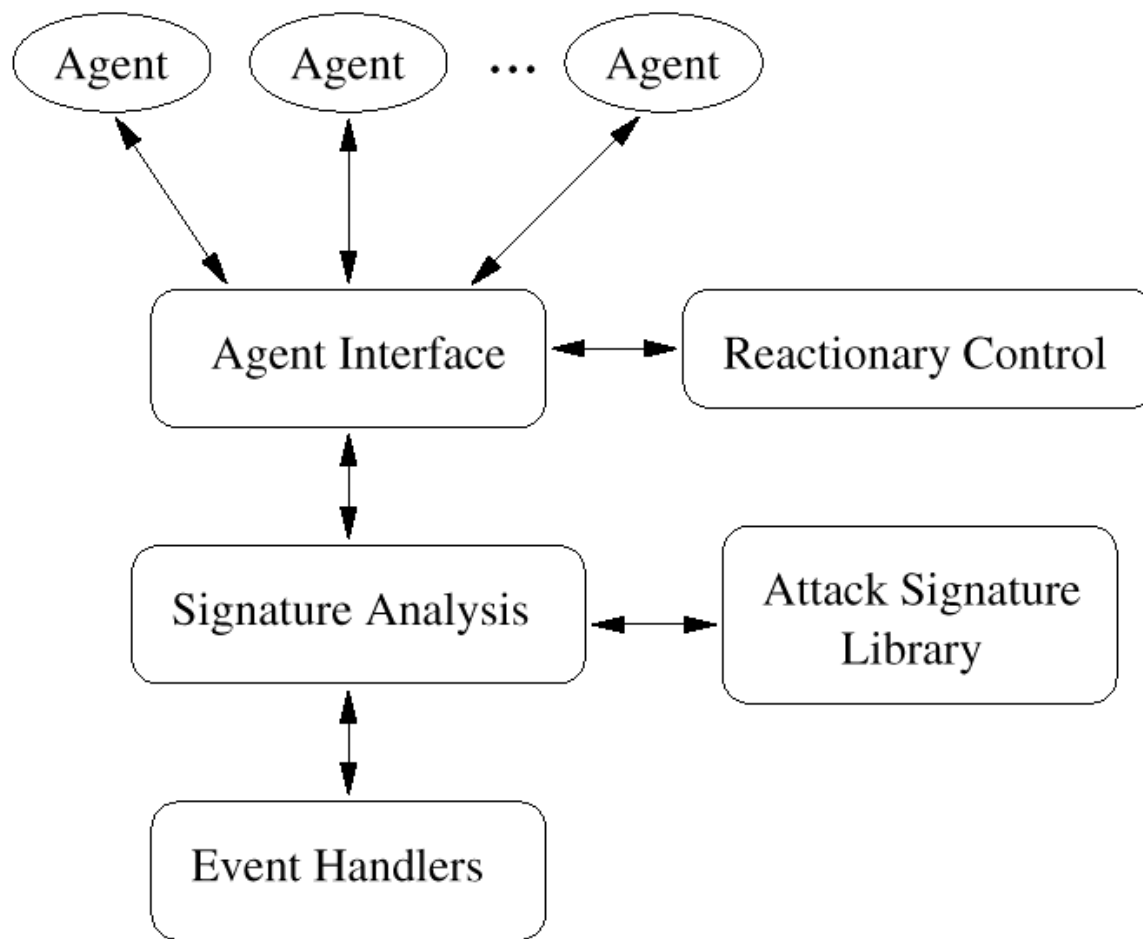
◆ High-level Reactionary Control

- Implements high-level survivability features
 - » e.g. filtering, patching, early warning
- Migratory Autonomous Agent System
 - » Small specialized program to perform specific task
 - » Off the shelf technology, (Aglets)

Survivability Architecture Overview

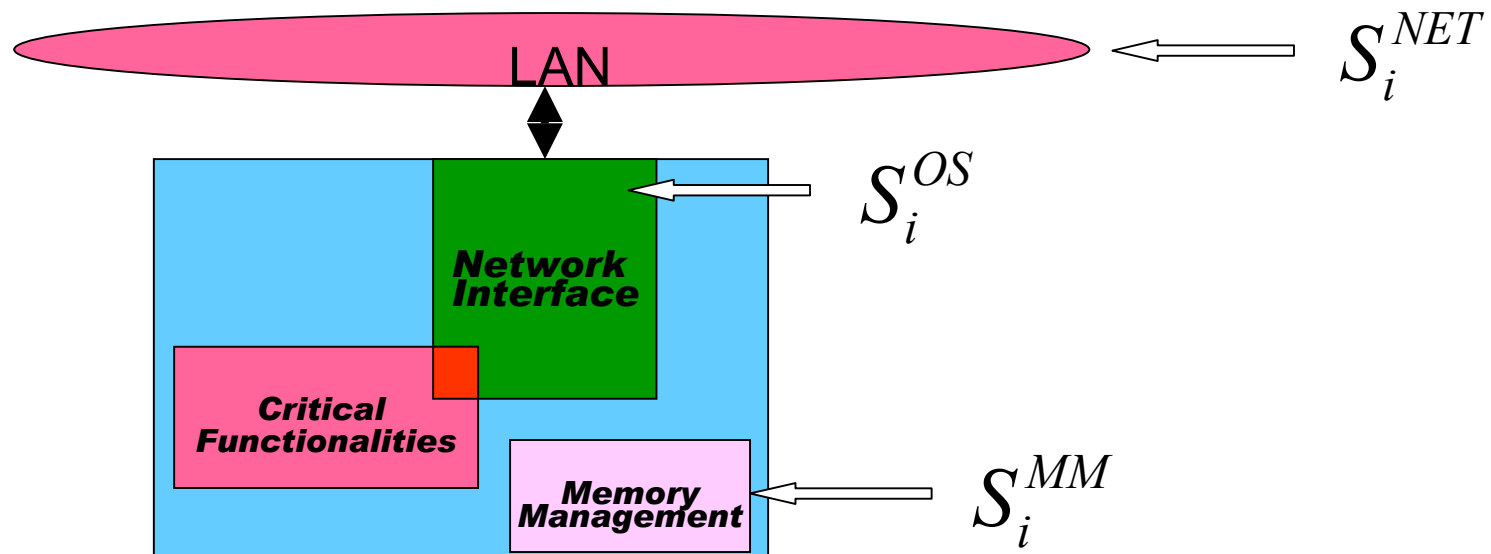
Reactionary Mechanism

◆ System Components



Extending the Model

- ◆ Signatures and N-Version dissimilarity
 - signatures based on Network portion of OS
 - signatures based on IP protocol flags



Conclusions

- ◆ Address survivability with respect to different levels of complexity
- ◆ Recognize specific attacks at lowest suitable level
- ◆ Survivability Architecture:

Layered approach to Survivability

Questions?

2001+ Project related Publications

- ◆ A.W. Krings, W.S. Harrison, M.H. Azadmanesh, and M. McQueen, "Scheduling Issues in Survivability Applications Using Hybrid Fault Models", Submitted: Parallel Processing Letters
- ◆ Taylor, C, A.W. Krings, W.S. Harrison, N. Hanebutte, and M. McQueen, "Considering Attack Complexity: Layered Intrusion Tolerance", Submitted: DSN 2002 Workshop on Intrusion Tolerance
- ◆ Harrison W.S., A.W. Krings, N. Hanebutte, and M. McQueen, "On the Performance of a Survivability Architecture for Networked Computing Systems", Procs. 35th Hawaii International Conference on System Sciences, January 2002.
- ◆ Krings A.W., Harrison W.S., M. McQueen, and S. Matthews, "Shifting the Focus of Survivability: Back to the Basics", Information Survivability Workshop, (ISW-2001), Vancouver, BC Canada, March, 2002.
- ◆ Krings A.W., Harrison W.S., M.H. Azadmanesh, and M. McQueen, "Scheduling Issues in a Computer and Network Survivability Application", New Trends in Scheduling Parallel and Distributed Systems, Book of Abstracts, Lunimy-Marseille, October 1-5, 2001.
- ◆ Taylor C., W. Harrison, A. Krings, N. Hanebutte, and M. McQueen, "Low-Level Network Attack Recognition: A Signature-Based Approach", 13th International Conference on Parallel and Distributed Computing and Systems, (PDCS'2001), Anaheim, California, Aug 21-24, pp. 570-574, 2001.
- ◆ Krings A.W, W.S. Harrison, N. Hanebutte, C. Taylor, and M. McQueen, "A Two-Layer Approach to Survivability of Networked Computing Systems", International Conference on Advances in Infrastructure for Electronic Business, Science, and Education on the Internet, (SSGRR'2001), L'Aquila, Italy, Aug 06 - Aug 12, pp. 1-12, 2001.
- ◆ Krings A.W, W.S. Harrison, N. Hanebutte, C.S. Taylor, M. McQueen, and S. Matthews, "An Agent Supported Bottom-Up Approach to Computer and Network Survivability", Supplement of the 2001 International Conference on Dependable Systems and Networks (DSN-2001), Goteborg, Sweden, pp. B70-71, July 1-4, 2001.
- ◆ Krings, A.W., and M.H. Azadmanesh, "The Impact of Hybrid Fault Models on Scheduling for Survivability", The European Operational Research Conference, (EURO 2001), Rotterdam, Netherlands, July 9-11, pg. 206, 2001.
- ◆ Krings, A.W., S. Harrison, N. Hanebutte, C. Taylor, and M. McQueen, "Attack Recognition Based on Kernel Attack Signatures", Proc. of the International Symposium on Information Systems and Engineering, (ISE'2001), Las Vegas, June 25-28, pp. 413-419, 2001.