Computer Misuse and Anomaly Detection - IV (11/96)

Steve Smaha

President
Haystack Labs, Inc.
10713 RR 620 North, Suite 512
Austin, Texas 78726
(512) 918-3555 (voice)
(512) 918-1265 (fax)
smaha@haystack.com
http://www.haystack.com

How To Form Your Very Own Silicon Valley Startup

by Laura Lemay

1. Go to Menlo Park. Find a tree.

2. Shake the tree. A venture capitalist will fall out.

3. Before the venture capitalist regains its wits, recite the following incantation: “Internet! Electronic Commerce! Distributed Enterprise-Enabled Applications! Java”

4. The venture capitalist will give you four million dollars.

5. In 18 (12? 6? 3?) months, go public.

6. After you receive your check, go back to Menlo Park. Find a tree.

7. Climb it. Wait.

Haystack Labs, Inc.

- Founded in 1989 & based in Austin, Texas
- 25 employees, 3 offices
- Current product development began in 1991
- R&D work for intelligence agencies
- University of Texas Technology Incubator Graduate
- Venture funded - Venrock, Trellis

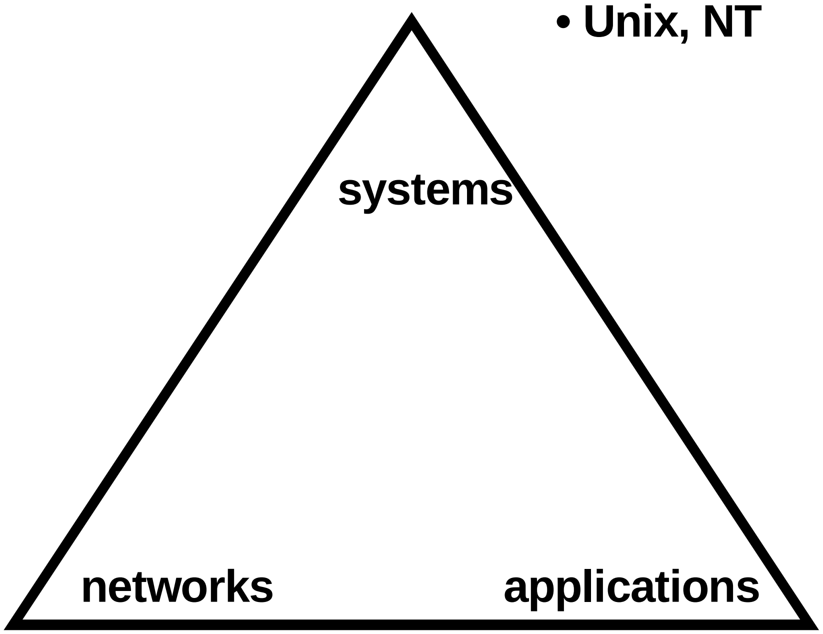
Partners

- Sun, IBM, Storage Technologies (Network Systems Corp.), AT&T, European VARs, Ascend
- Coming soon: firewall vendors, PC/NT vendors

Product Lines

Stalker

- Unix, NT



NetStalker

- NSC routers/switches
- Embedded in firewalls

Application Stalker

- WebStalker
- CommerceStalker
- More...

Underlying Technology

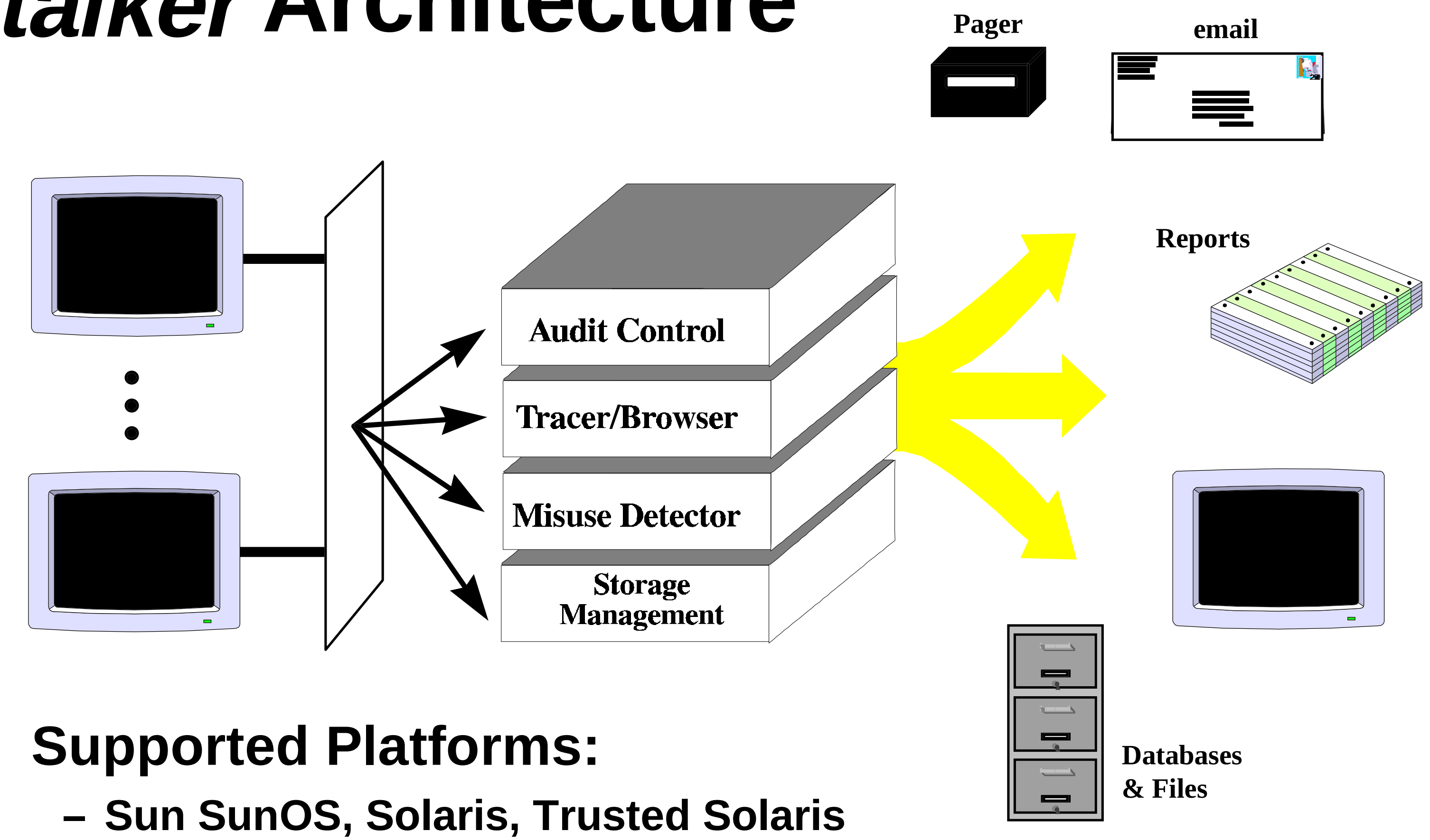
- **Generic signature recognition approach**
  - **Developed in 1992-93 after delivering and installing statistical and AI-based systems**
  - **Applying compiler/parser techniques to look for security-relevant patterns in audit trails, network event logs, and other security logs**
  - **U.S. patent #5,557,742 issued 17 Sep 96, other countries pending**
- **Engine + database model**
- **Significant use of outcomes analysis as “safety net”**

What’s In The Patent?

ABSTRACT

A processing system intrusion and misuse detection system and method utilizes instructions for and steps of processing system inputs into events and processing the events with reference to a set of selectable misuses in a misuse engine to produce one or more misuse outputs. The system and method convert processing system generated inputs to events by establishing an event data structure that stores the event. The event data structure includes authentication information, subject information, and object information. Processing system audit trail records, system log file data, and system security state data are extracted from the processing system to form the event data structure. A signature data structure stores signatures that the misuse engine compares and matches to selectable misuses. The signature data structure includes an initial state for each selectable misuse, an end state for each selectable misuse, one of more sets of transition functions for each selectable misuse, and one or more states for each selectable misuse, which can include the end state or the initial state. Furthermore, a misuse output and an index are utilized so that for each selectable misuse element there is a mechanism for loading the signature data structure.

Stalker Architecture



- **Supported Platforms:**
  - Sun SunOS, Solaris, Trusted Solaris
  - IBM AIX
  - HP- UX
  - NT 4.X Soon

Misuse Detector:
What *Stalker* Detects

Insider and outsider activities:

Known attacks

- **“doorknob rattling”**
- **rdist**
- **rlogin bin**
- **ICMP**
- **login trojan horses**
- **NFS mounts**
- **YP/NIS maps**
- **RPC portmapper**
- **Password “sniffer”**
- **SATAN**

Attempts to exploit known vulnerabilities

- **bugs in the code**
- **design flaws**
- **unexpected interactions with other system components**
- **affects operating systems, network protocols, applications**
- **example: “Internet worm” of 1988**
- **SATAN**

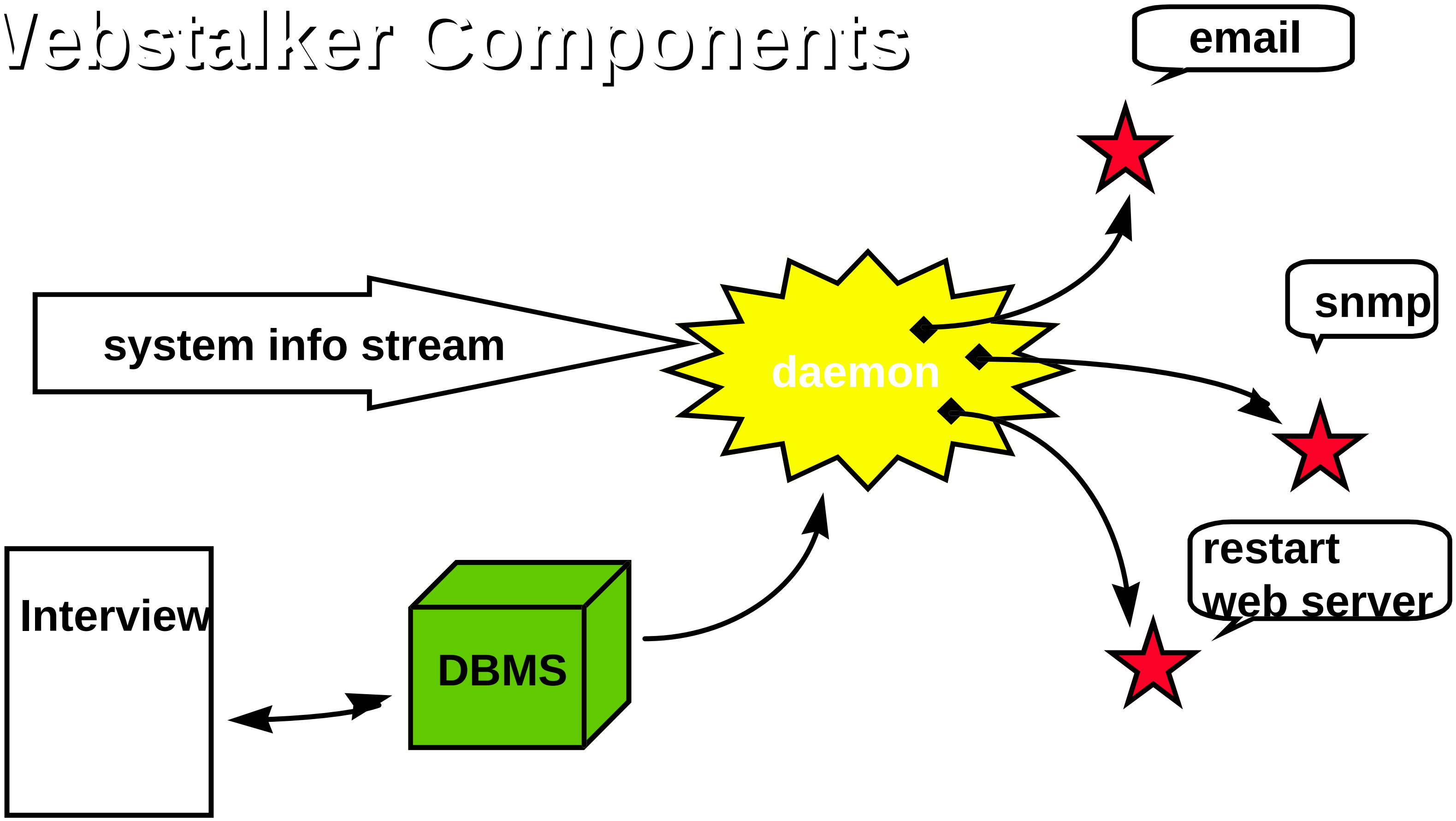
Known attack outcomes

- **Detecting these outcomes provides a “safety net” for trapping new hacker techniques.**
  - **Privilege escalation**
  - **Monitors disabled**
  - **Special files modified**

Introducing...

Real-time security monitoring for Web servers, ensuring 7 x 24 availability and integrity

Webstalker Components



email

snmp

restart
web server

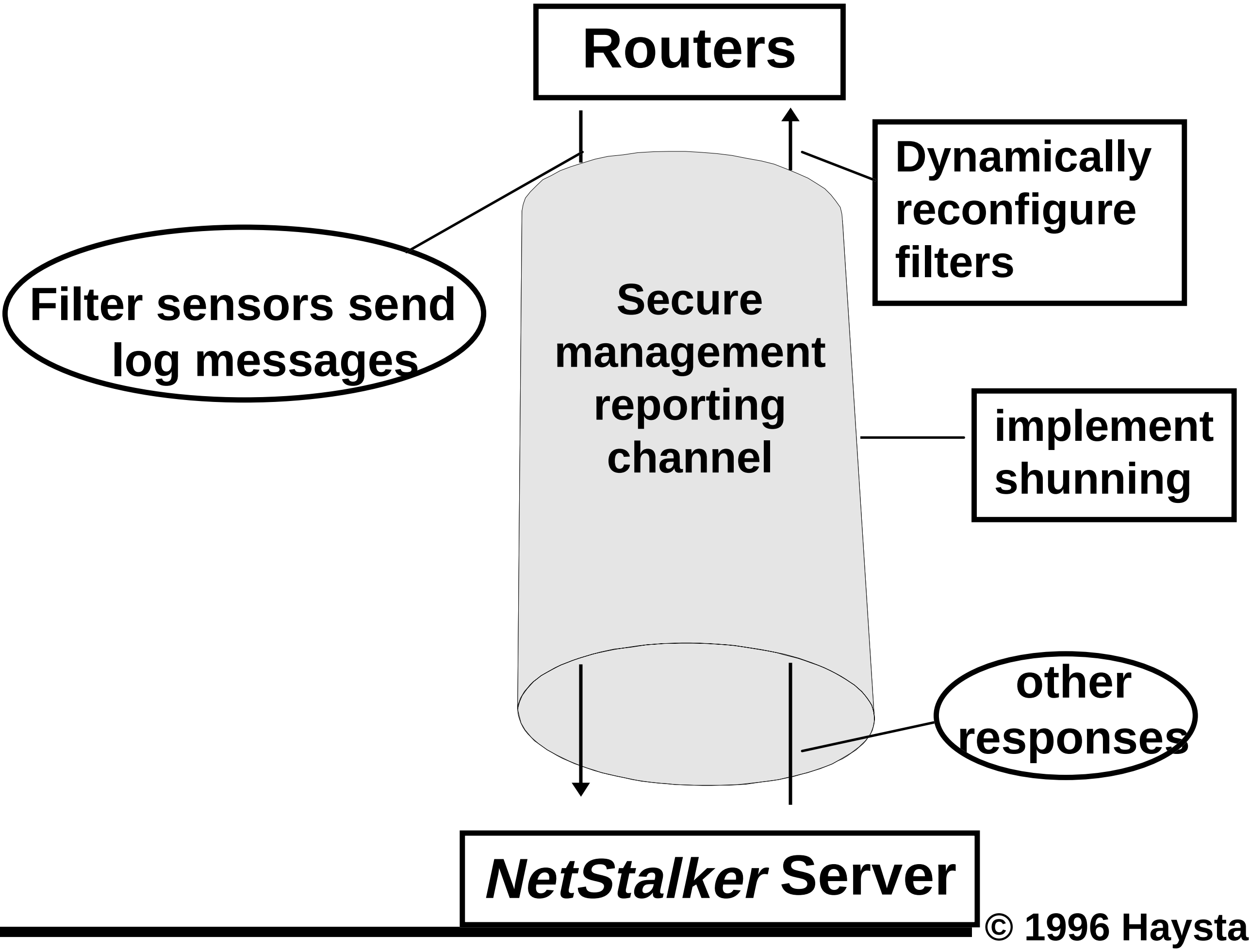
system info stream

daemon

Interview

DBMS

NetStalker for NSC: Architecture


Routers
Dynamically reconfigure filters
Filter sensors send log messages
Secure management reporting channel
implement shunning
other responses
NetStalker Server

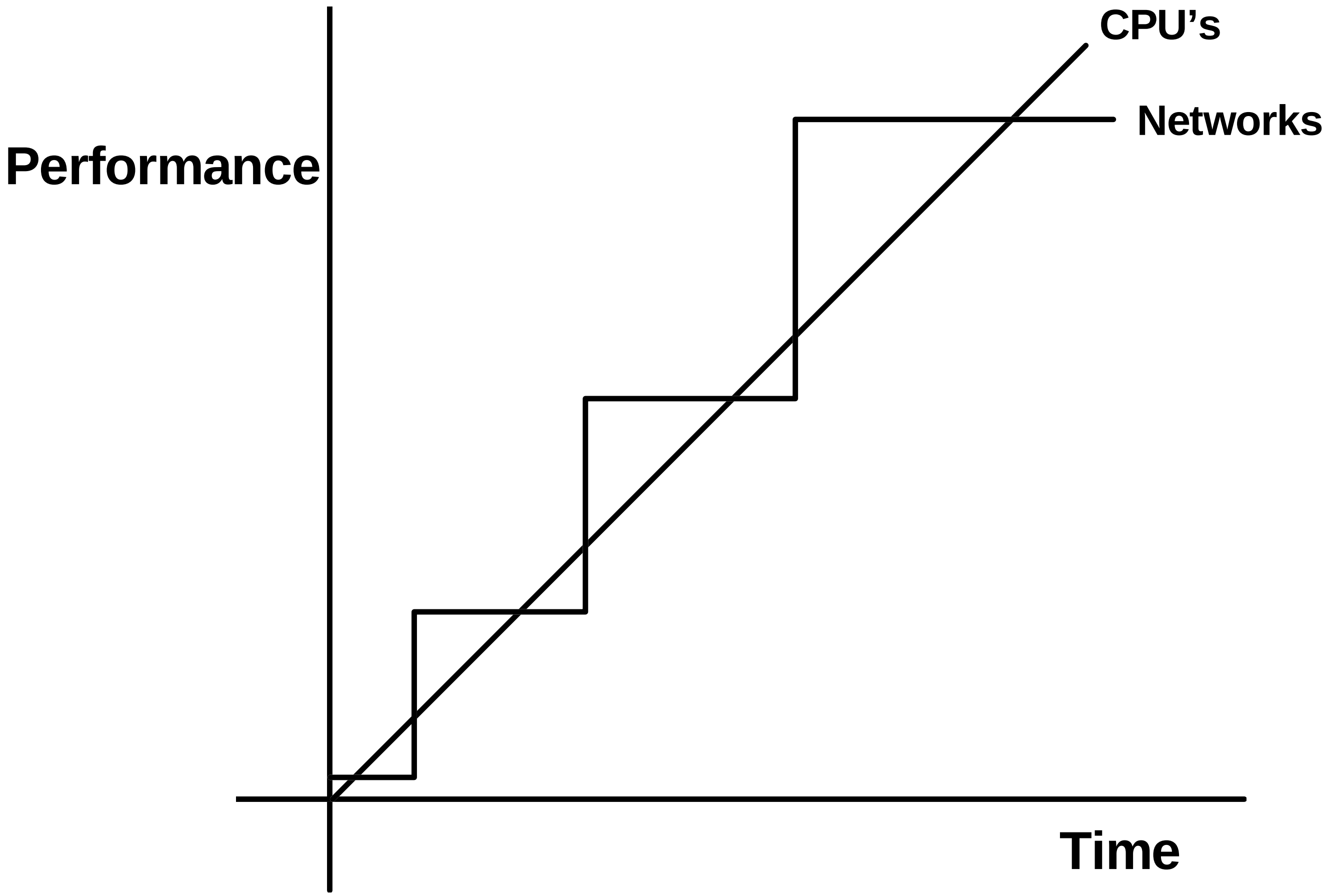
Overview

- The new threat
- Challenges of increased bandwidth
- Signs of hope: toasters
- Suggested roles

The Biggest Problem: Vendors

- Outsiders -> Insiders -> Vendors
- Mass-market software is designed to satisfy 80% of the market's needs, and to do so NOW!
- 3-4 major releases a year:
  - How much testing before your users download it?
  - Security flaws published in minutes on the Internet!
- Security products are mostly Band-Aids™.
- Large PC vendors don't give any special priority to security problems reported by governments.

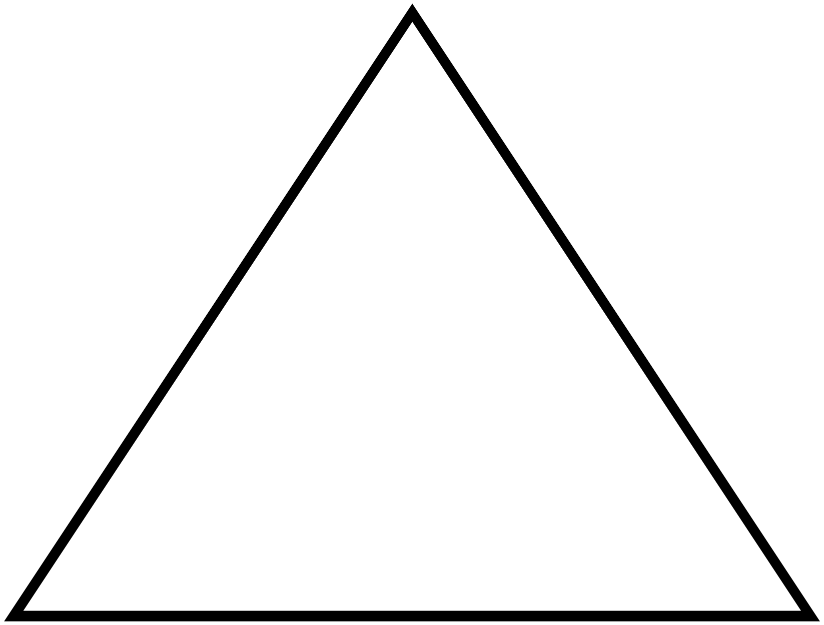
Fundamental Problem of Network Security Monitoring



Toasters Are A Good Thing.

- **Distributed computing with cheap boxes allow specialization of functions.**
  - **Divide and conquer … sounds object-oriented!**
  - **Fewer general purpose computers**
  - **Do one thing and do it well: e.g. serve Web pages.**
- ***SOME* may be built on a recycled MLS/CMW base, but not many!**
- **Major research issues:**
  - **How to state security attributes of components?**
  - **How to compose pieces into bigger systems?**

Active Security Needs



Availability

- 7 x 24
- Restart

Paranoia

- Confidentiality
- Integrity

Accountability

- Audit Requirements
- Reconstruction
- Traceability