2110413 Computer Security

Lecture 4

Auditing, IDS, IPS

Introduction to buffer overflow

Krerk Piromsopa, Ph.D.
Department of Computer Engineering
Chulalongkorn University

Outline

- Definition
- Audit Trials
- Log Analysis
- Put it all together
- IDS & IPS
- Firewall & DMZ
- Introduction to Integrity

Auditing

To sway an audience, you must watch them as you speak.
C. Kent Wright

- The easiest component to implement and is the fundamental of secure system.
- Continuous Quality Improvement (CQI).
- Historically, a soldier guards a gate.
- Definition
  - a systematic review or assessment of something
  - a report or description of an event or experience (account)

How to Audit?

- Audit Trails
  - Physical trails
  - Log files
- Analysis Tools
  - Statistic
  - Data Mining

S.No.	Table	Column Name	Type of Changes	Old Value	New Value	Updated By	Date Log
1	LEADPARTNER	LEADPARTNER NAME	INSERT	-	Testing Lead Partner	Wilson Sim	02/05/2006 09:28:32am
2	LEADPARTNER	LEADPARTNER NAME	INSERT	-	scstester	STEVEN THAME	04/05/2006 10:04:26am
3	LEADPARTNER	LEADPARTNER NAME	INSERT	-	Singapore Computer Systems	WILSON SIM	05/05/2006 02:00:21pm
4	LEADPARTNER	LP_ID	INSERT	-	291	ADMIN	07/04/2006 08:41:00am
5	LEADPARTNER	NAME	UPDATE	Test Triggers	Test Triggers 1	ADMIN	07/04/2006 08:45:05am
6	LEADPARTNER	NAME	UPDATE	Lokesh Co Ltd	Lokesh Co Ltd 1	Wilson Sim	07/04/2006 08:57:22am
7	LEADPARTNER	NAME	UPDATE	Lokesh Pandey155	345	SCS	07/04/2006 11:27:47am
8	LEADPARTNER	NAME	UPDATE	Lokesh Pandey155	345	SCS	07/04/2006 11:27:47am
9	LEADPARTNER	NAME	UPDATE	Lokesh Pandey155	345	SCS	07/04/2006 11:27:47am
10	LEADPARTNER	NAME	UPDATE	Lokesh Pandey155	345	SCS	07/04/2006 11:27:47am
11	LEADPARTNER	NAME	UPDATE	Lokesh Pandey155	345	SCS	07/04/2006 11:27:47am

Traditional Log

- No standard in formatting
  - Unix Syslog (defacto-standard)
  - Windows System, Security, Application Event Logs
  - Standard Java Logging (log4j)
  - Novell, Etc...

Modern Auditing Services

- OpenGroup Distributed Auditing Server (OpenXDAS)
  - Start in 1998 (preliminary). Reestablished in Mar 2007
  - Standardized API for event submission and management
- Okay, we stay with Syslog.
- Others?
  - (e.g. common log, extended log)

Analysis Tools

- Statistical Analysis
- Anomaly Detection
- Association Analysis
- AI (Genetic Algorithm, Neural Net, etc)

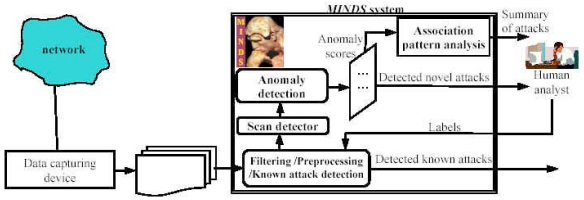
Auditing in Action

- Intrusion Detection System (passive system)
  - detects unwanted manipulations of computer systems
  - Network Intrusion Detection System (NIDS) ... e.g. snort
  - protocol-based intrusion detection system
  - application protocol-based intrusion detection system
  - host-based intrusion detection system ... e.g. OSSEC
  - hybrid intrusion detection system ... e.g. Prelude

MINDS

- Minnesota INtrusion Detection System (MINDS)
  - unsupervised anomaly detection
  - association pattern analysis

Capturing
SQL SLAMMER



http://www.cs.umn.edu/research/MINDS/

Auditing in Action

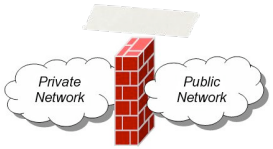
- Intrusion Prevention System (active system)
  - react to suspicious activity (by resetting connection or reprogramming the firewall to block suspected malicious source)
  - a form of application layer firewall

Pop Quiz

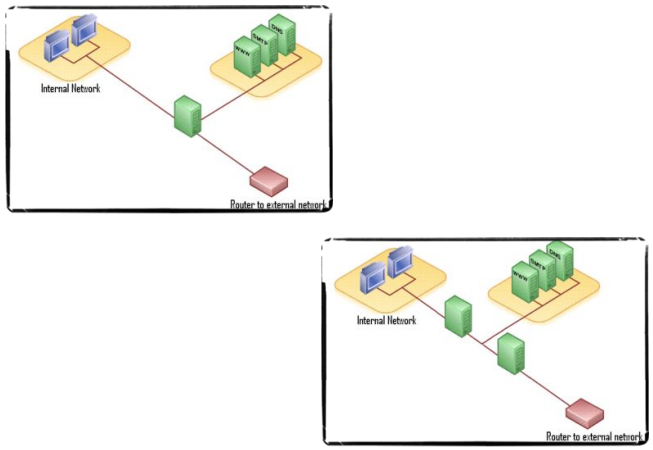
- What is the different between IDS, IPS and firewall?
- Is it possible to evade IDS and IPS?
  - If yes, HOW?

Firewall

- Separate public network and private network (inside and outside)
  - 1st generation - packet filters
  - 2nd generation - stageful filters
  - 3rd generation - application layer
- Personal Firewall, NAT



Demilitarized Zone (DMZ)



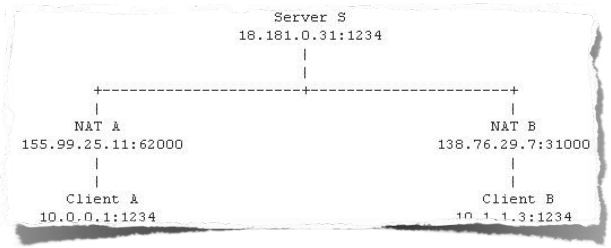
Firewall pinhole

- Connection initializes from internal network.
- (sometimes) automatically close after a period of time.
- Can we create a hole between two systems behind firewall?

Punch Hole

How to block this?

- Firewall & Admin nightmare
- used by P2P, VoIP (Skype), VPNs



Introduction to Buffer Overflow

Memory Organization

Stack (growing down) Heap (growing up)
BSS
Data
Text

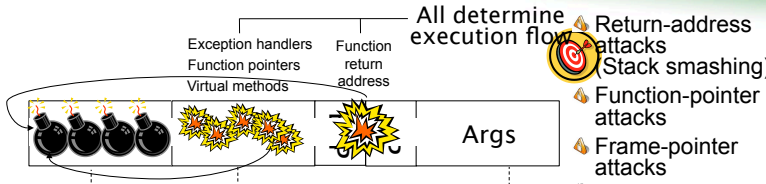
Simple Buffer Overflow

```
#include <stdio.h>
int main(char argc,char *argv[]) {
        int age;
        char name[8];
        char tmp[20];
        printf("Enter your age:");
        gets(tmp);
        age=atoi(tmp);
        printf("Enter your name:");
        gets(name);
        printf("----------\n%s is %d
years old\n"
                ,name,age);
}
```

```
$./a.out
Enter your age:15
Enter your name: Dr.Krerk1
----------
Dr.Krerk1 is 49 years old
```

What's wrong?

Stack Buffer Overflows at Work



- Return-address attacks (Stack smashing)
- Function-pointer attacks
- Frame-pointer attacks

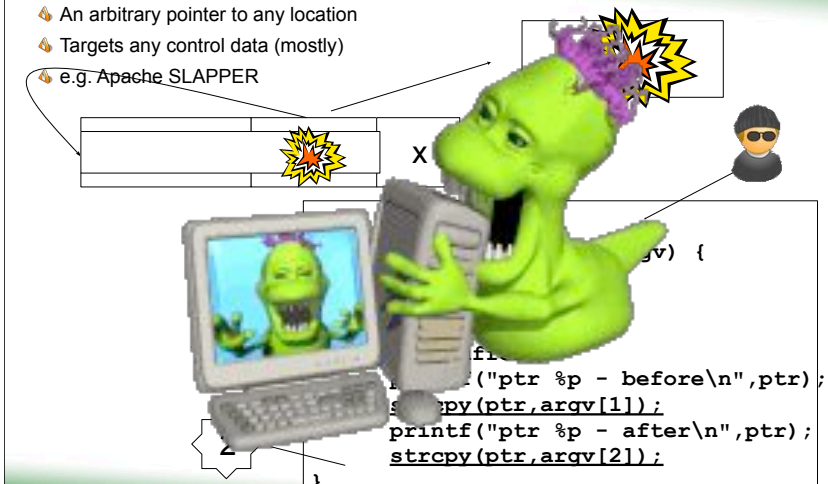

```
void func(char *p, int i) {
  int j = 0;
  CFoo foo;
  int (*fp)(int) = &func;
  char b[128];
  strcpy(b,p);
}
```

Bad things happen if *p points to data longer than b

Michael Howard, Microsoft.

Sample Buffer-Overflow Attack

- An arbitrary pointer to any location
- Targets any control data (mostly)
- e.g. Apache SLAPPER




```
printf("ptr %p - before\n",ptr);
strcpy(ptr,argv[1]);
printf("ptr %p - after\n",ptr);
strcpy(ptr,argv[2]);
}
```

The (almost) End

Homework II

- 2 weeks (due December 5, 2007)
- In this homework, you will master the technique to render buffer-overflow attacks. The exercises will walk you through stack smashing.
- Your platform is cygwin.
- Details will be posted on the web.

about term projects.

- Send me a topic before December 5
- A presentation shows how it works
  - 25 minutes for presentation + 5 minutes for question
- a report (write up)
- Which team will present first? Let's play a roulette.
  - Available time slots (8*3)
  - Jan 9, Jan 16, Jan 23, Jan 30, Feb 6, Feb 13, Feb 20, Feb 27

Grading

- Submit the materials to me one week before your presentation. I will post it on the web for you.
- presentation 20%
- question 5%
- report 15%