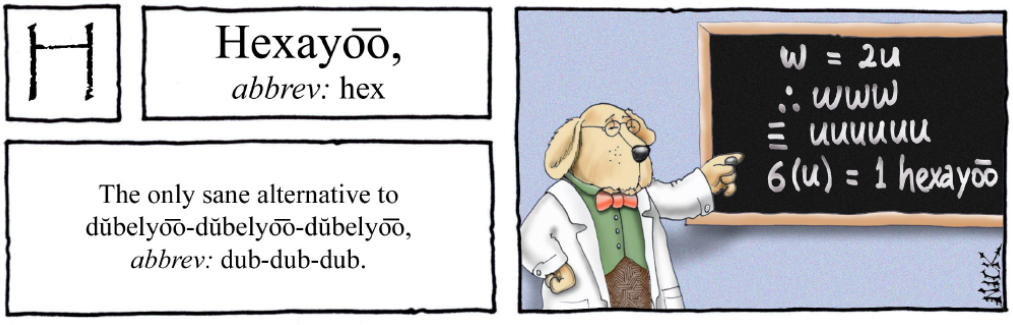



Chapter 11

Lecture 11 - Stack attack


World Wide Web...



Admin

- No tutorials next week (Hari Raya), instead...
  - I ask you to read Section 9 of the textbook: Ethics, CERT, NSA, C2.
- Last tutorial will be in week 13
- MCQ today at 5:05

Stranger danger...

*One of my sons was taught stranger-danger at his school. We were asked to quiz him afterwards, so we asked him if he should accept a lift in a car with a stranger. He immediately replied "**No way!**". We then asked: "**What if he offered you sweets?**", but he still replied "**No way!**". Finally we asked: "**Why not?**", to which he replied "**Because you might not get any!**"*

Ethics

Moral development stages:

Stage 1: *Obedience and punishment*

...

Stage 6: *Individual principles of conscience* - an orientation not only toward existing social rules, but also toward the conscience as a directing agent, mutual trust and respect, and principles of moral choice involving logical universalities and consistency. If one acts otherwise, self-condemnation and guilt result.

Ethics and computing

No new ethical dilemmas... Perhaps the only significant difference is that the computer crimes are so easy.

Software duplication: = *theft*.

Using information: = *insider trading.*

E-mail abuse: = *abuse.*

Network administrator's dilemma

- Network administrators often come to learn things about their 'clients'
- Without asking the client, they should not make use of that information.
- The network administrator's dilemma: How to control bad-guys without trampling over rights.

Professional codes of ethics

- Most professional bodies[18] have formal written codes of ethics
- The computer industry has yet to develop a standard code of conduct
- If computer crime continues to rise, codes may be imposed on it.

[18] For example: Medical boards.

ACS code of ethics

1. I will serve the interests of my clients and employers, my employees and students, and the community generally, as matters of no less priority than the interests of myself or my colleagues.
   ...

Within a general framework of ethical and moral responsibility, codes such as this one can help clarify *grey* areas of concern.

Insecurity - threats are real

For example:

- Pentagon machines were repeatedly corrupted by unknown intruders during the Gulf war. The intruders appeared to be doing it as part of a contest.

- German hackers demonstrated on TV a method of transferring money into their own accounts using ActiveX controls downloaded to an unsuspecting person's machine.

Taxonomy of insecurity?

Each new attack adds new levels to the structure:

- physical insecurity, and
- password insecurity

Some of the security of modern systems is provided through cryptographic techniques (particularly password storage), the subject today.

Non-cryptographic cracking

Misconfiguration: If excessive permissions exist on certain directories and files, these can lead to gaining higher levels of access. For example, on a UNIX system, if /dev/kmem is writable it is possible to rewrite your UID to match root's.

Poor SUID: Sometimes there are scripts (shell or Perl) that perform certain tasks and run as root. If the scripts are writable by you, you can edit it and run it.

Non-cryptographic cracking

Buffer overflow: Buffer overflows are typically used to spawn root shells from a (server) process running as root.

Race conditions: A race condition is when a program creates a short opportunity for attack by opening a small window of vulnerability. For example, a program that alters a sensitive file might use a temporary backup copy of the file during its alteration.

Non-cryptographic cracking

Poor temporary_files: Many programs create temporary files while they run. If a program runs as root and is not careful about where it puts its temporary files and what permissions these files have, it might be possible to use links to create root-owned files.

Attacks using these methods can be launched locally on the target machine, or often remotely, by exploiting *services* with loopholes.

Protection

Can you protect yourself against attacks?

- **Hack/crack yourself:**
- **Be vigilant:**
- **Reduce reliance:**
- **Use more secure systems:**
- **Update systems:**

Finally: "*Its not the end of the world!*"

Computer Emergency Response Team

The CERT Coordination Center is the organization that grew from the computer emergency response team formed by the Defense Advanced Research Projects Agency (DARPA) in November 1988 in response to the needs identified during the Internet worm incident. The CERT charter is to work with the Internet community to facilitate its response to computer security events involving Internet hosts, to take proactive steps to raise the community's awareness of computer security issues, and to conduct research targeted at improving the security of existing systems.

CERT

- ✘ If you are ever involved in a computer security incident it is useful to get in touch with CERT.
- ✹ They provide incident reports and advisories, and can liaise with other system administration people if the attack on your system comes from outside your organization.

CERT Incident Note IN-99-04

Here is an excerpt from an incident report:

Similar Attacks Using Various RPC Services

Thursday, July 22, 1999

Overview

We have recently received an increasing number of reports that intruders are using similar methods to compromise systems. We have seen intruders exploit three different RPC service vulnerabilities; however, similar artifacts have been found on compromised systems.

…

SIGINT

- *Signals Intelligence* (SIGINT) broke the Japanese military code and learned of plans to invade Midway Island.
- In 1943 they began the VENONA project to examine encrypted Soviet diplomatic communications.
- The messages were double-encrypted and were extremely difficult to crack.
- Almost all of the US KGB messages in 1944 and 1945 were broken between 1947 and 1952.

NSA - National Security Agency

- Successor of SIGINT
- *The National Security Agency is the USA's cryptologic organization.*
- *It coordinates, directs, and performs highly specialized activities to protect U.S. information systems and produce foreign intelligence information.*

NSA - National Security Agency

- *NSA employs the country's premier codemakers and codebreakers.*
- *It is said to be the largest employer of mathematicians in the United States and perhaps the world.*

Rainbow documents

- The NSA created various documents describing the criteria for evaluating the security behaviour of machines.
- These criteria were published in a series of documents with brightly coloured covers, and hence became known as the *Rainbow* series. (red book, yellow book...)

C2 security

DOD 5200.28-STD - “Department of Defense Trusted Computer System Evaluation Criteria”:

- To provide a standard to manufacturers (for security features related to confidentiality)...
- To provide DoD components with a metric with which to evaluate the degree of trust...
- To provide a basis for specifying security requirements in acquisition specifications.

C2 security example

- *The TCB[19] shall require users to identify themselves to it before beginning to perform any other actions that the TCB is expected to mediate.*
- *Furthermore, the TCB shall use a protected mechanism (e.g., passwords) to authenticate the user’s identity.*

[19] Trusted Computing Base.

Microsoft and C2

Windows NT Workstation vs 3.5 with U.S. Service Pack 3 was the first Microsoft product that has completed C2 testing, and is only certified if using the same hardware, and installed software, and does not include any network connection. The NT utility ***c2config.exe*** sets up an NT system to pass the C2 tests.

The 1998 attacks on the Pentagon involved theft and modification of data, as well as denial-of-service. The attacked machines were C2-secure Windows NT machines.

UNIX and C2

Many UNIX systems have also got C2 certification, and come configured this way from the manufacturer.

> *There are numerous examples of hacked UNIX systems found on the Internet. In 1996, a site I managed in New Zealand was the target of a malicious attack by intruders from Australia and Belgium.*

Given all this, C2 certification is probably not a good guide as to the security of your system.

DVD security

- Content Scrambling System - data encryption scheme
- Developed by commercial interests to stop copying... but
  - Easy to copy a DVD, but CSS prevents decrypting, changing and re-recording.
- Details are trade secret.
- Master set of 400 keys is stored on every DVD, and the DVD player uses these to generate a key needed to decrypt data from the disc.

DVD security

- Linux users were excluded from access to CSS licenses because of the open-source nature of Linux.
- In October 1999, hobbyists/hackers in Europe cracked the CSS algorithm
- DVD industry players have been trying to prevent distribution of any software
- The source code for decoding DVD is available on a T-shirt.

DVD security

The lesson to learn from this is that once-again *security-through-obscurity* is a very poor strategy.

The source code and detailed descriptions for a CSS descrambler is available at:

http://www-2.cs.cmu.edu/~dst/DeCSS/Gallery/

DVD security

Description of the key/descrambling process:

First one must have a master key, which is unique to the DVD player manufacturer. It is also known as a player key. The player reads an encrypted disk key from the DVD, and uses its player key to decrypt the disk key. Then the player reads the encrypted title key for the file to be played. (The DVD will likely contain multiple files, typically 4 to 8, each with its own title key.) It uses the decrypted disk key (DK) to decrypt the title key. Finally, the decrypted title key, TK, is used to descramble the actual content.

DVD security

Confusion and diffusion...

```
#define m(i)(x[i]^s[i+84])<<
unsigned char x[5],y,s[2048];main(n){for(read(0,x,5);read(0,s,n=2048);
write(1,s ,n))if(s[y=s[13]%8+20]/16%4==1){int i=m(1)17^256+m(0)8,k=m(2)
0,j=m(4)17^m(3)9^k *2-k%8^8,a=0,c=26;for(s[y]-=16;--c;j*=2)
a=a*2^i&1,i=i/2^j&1<<24;for(j=127;++j<n ;c=c>y)c+=y=i^i/8^i>>4^
i>>12,i=i>>8^y<<17,a^=a>>14,y=a^a*8^a<<6,a=a>>8^y<<9,k=s [j],k="7
Wo~'G_\216"[k&7]+2^"cr3sfw6v;*k+>/n."[k>>4]*2^k*257/8,s[j]=k^(k&k
*2&34) *6^c+~y;}}
```