OS Security Basics

CS642: Computer Security

Professor Ristenpart

http://www.cs.wisc.edu/~rist/

rist at cs dot wisc dot edu
Arizona Botnet Controller Draws 30-Month Federal Sentence

Posted by timothy on Sunday September 09, @05:35PM from the such-a-sweet-boy dept.

dgharmon writes with word from the BBC that

"A U.S. hacker who sold access to thousands of hijacked home computers has been jailed for 30 months. Joshua Schichtel of Phoenix, Arizona, was sentenced for renting out more than 72,000 PCs that he had taken over using computer viruses."

Time is cheap: Schichtel admitted to giving access to those 72,000 computers for $1500.
We start with some basics about operating system security:

- Multics
- Multi-level security
- Security policies
- Access controls
- UNIX permissions
Take yourself back to the 1960’s

http://fyeahhippies.tumblr.com/post/135907376
Take yourself back to the 1960’s

Time-share multiuser computers coming into use

GE-645
36 bit address space
Up to 4 processors
Magnetic tape drives
Supported virtual memory in hardware

Courtesy of
http://aficionadous.blogspot.com/
MulEplexed Information and Computing Service (Multics)

Project to develop operating system for time-shared systems

- MIT project MAC, Bell Labs, and GE
- ~100 installations at greatest extent
- Last one shut down in 2000 (Canadian department of defense)

“"A small but useful hardware complement would be 2 CPU units, 128K of core, 4 million words of high speed drum, 16 million words of disc, 8 tapes, 2 card readers, 2 line printers, 1 card punch and 30 consoles.”

[Vyssotsky, Corbato, Graham 1965]
Multics: ancestor to many OS’s

Lots of innovations in design

• Use of segmentation and virtual memory with hardware support
• SMP (shared memory multiprocessor)
• Written in PL/1 (high level language)

Significant attention paid to security
Multi-level security

• Military and other government entities want to use time-sharing too

Top secret data

Unclassified data
Classification levels

- Top secret
- Secret
- Confidential
- Unclassified
Classification levels and compartmentalization

- Top secret
- Secret
- Confidential
- Unclassified

European

Special intelligence
Classification levels and compartmentalization

• Security level (L,C)
  – L is classification level (Top secret, secret, ...)
  – C is compartment (Europe, Special intelligence...)

Dominance relationship:

\[(L_1, C_1) \leq (L_2, C_2)\]

\[L_1 < L_2\]

\[C_1 \text{ subset of } C_2\]

Example:

\[(\text{Secret, \{European\}} ) \leq (\text{Top Secret, \{European,Special Intel\}})\]
Bell-Lapadula Confidentiality Model

“no reads up”, “no writes down”

- Top secret
- Secret
- Confidential
- Unclassified

European

Special intelligence
Bell-Lapadula Confidentiality Model

“no reads up”, “no writes down”

Simple security condition

User with \((L_1,C_1)\) can read file with \((L_2,C_2)\) if?

\((L_1,C_1) \leq (L_2,C_2)\) or \((L_1,C_1) \geq (L_2,C_2)\)

*-property

User with \((L_1,C_1)\) can write file with \((L_2,C_2)\) if?

\((L_1,C_1) \leq (L_2,C_2)\) or \((L_1,C_1) \geq (L_2,C_2)\)
Say we have just Bell-Lapadula in effect... what could go wrong?
Biba integrity model

“no read down”, “no writes up”

Top secret
Read should fail

Secret

Confidential
Write should fail

Unclassified

European

Special intelligence
Biba integrity model

“no read down”, “no writes up”

Simple integrity condition

User with \((L1,C1)\) can read file with \((L2,C2)\) if?

\[(L1,C1) \leq (L2,C2) \quad \text{or} \quad (L1,C1) \geq (L2,C2)\]

*-property

User with \((L1,C1)\) can write file with \((L2,C2)\) if

\[(L1,C1) \leq (L2,C2) \quad \text{or} \quad (L1,C1) \geq (L2,C2)\]
If we combine them… one can only communicate in same classification
Other policy models

- Take-grant protection model
- Chinese wall
- Clarke-Wilson integrity model
- etc.

A good reference is:
Bishop, Computer Security: Art and Science
Multics: ancestor to many OS’s

Lots of innovations in design

• Use of segmentation and virtual memory with hardware support
• SMP (shared memory multiprocessor)
• Written in PL/1 (high level language)

Significant attention paid to security
Multics: security mechanisms

Protection rings 0-7 in which processes execute

- Lower number = higher privilege
- Ring 0 is “hardcore” supervisor
- Inherit privileges over higher levels

Protection rings included in all typical CPUs today and used by all operating systems
Multics: security mechanisms

Segments

- Virtual memory
- Program and data items stored in a segment
- Descriptor control field (read only, write only, execute only, ...)
- Segments access controlled
Multics: security mechanisms

Enciphered passwords

- Couldn’t find the algorithm
- Later ones used DES, but Multics predates DES

\[ pw = 12345 \]

\[ pw \rightarrow h(pw) \]
The password bitstrengths allow us to determine the length of the password and the number of character types it includes. By tabulating all possible password lengths from w to qv, considering passwords shorter than length w generate entries in the PPLl and the realtime locator FIFO is length qvh and all combinations of the t different types we find a unique mapping between the quantized password strength and length typen. This allows us to analyze not merely the strengths of passwords but also the types.

Figure z shows the percent of passwords that are of a particular type as a function of length gaveraged across all sites. The strength appears to be a function of the users' perceived importance of the site. New York Times subscription passwords have an average bitstrength tyozwi which are noticeable weaker than the average over all sites haverage bitstrength uqovuim while PayPal and Fidelity haverage bitstrengths usoqu and t909si are stronger. Microsoft OWA, which mandates strong password rules, has the highest haverage bitstrength vrotwio.

From reading:
A Large-Scale Study of Web Password Habits, by Florencio and Herley
Karger and Schell: security analysis of Multics

• Classic red teaming example

We have concluded that AFDSC cannot run an open multi-level secure system on Multics at this time. As we have seen above, a malicious user can penetrate the system at will with relatively minimal effort. However, Multics does provide AFDSC with a basis for a benign multi-level system in which all users are determined to be trustworthy to some degree. For example, with certain enhancements, Multics could serve AFDSC in a two-level security mode with both Secret and Top Secret cleared users simultaneously accessing the system. Such a system, of course, would depend on the administrative determination that since all users are cleared at least to Secret, there would be no malicious users attempting to penetrate the security controls.
Karger and Schell: security analysis of Multics

In the long term, it is felt that Multics can be developed into an open secure multi-level system by restructuring the operating system to include a security kernel. Such restructuring is essential since malicious users cannot be ruled out in an open system. The
Reference monitors / security kernels

• System component that monitors (hopefully all) accesses to data for security violations
• Reference monitors may be:
  – kernel
  – hypervisor
  – within applications (Apache)
Circumventing access controls: covert channels

\[(L_1,C_1) \geq (L_2,C_2)\]
Circumventing access controls: covert channels

\[(L_1, C_1) \geq (L_2, C_2)\]

Process 1

\(\text{Process 1 sends a 1 bit to Process 2 by writing lots of bits to files it controls on hard disk}\)

Process 2

\(\text{Process 2 measures time to read from its files on disk}\)

\(\text{Hard disk}\)

\(\text{Longer read time} = 1 \text{ bit sent}\)

\(\text{Shorter read time} = 0 \text{ bit sent}\)
Covert channels one reason shared MLS systems unsolved problem
Access controls
## Access control matrix

User $i$ has permissions for file $j$ as indicated in cell $[i,j]$.

Due originally to Lampson in 1971.

<table>
<thead>
<tr>
<th>Subjects</th>
<th>file 1</th>
<th>file 2</th>
<th>...</th>
<th>file n</th>
</tr>
</thead>
<tbody>
<tr>
<td>user 1</td>
<td>read, write</td>
<td>read, write, own</td>
<td></td>
<td>read</td>
</tr>
<tr>
<td>user 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>user m</td>
<td>append</td>
<td>read, execute</td>
<td></td>
<td>read, write, own</td>
</tr>
</tbody>
</table>
Two common implementation paradigms

<table>
<thead>
<tr>
<th></th>
<th>file 1</th>
<th>file 2</th>
<th>...</th>
<th>file n</th>
</tr>
</thead>
<tbody>
<tr>
<td>user 1</td>
<td>read, write</td>
<td>read, write, own</td>
<td>read</td>
<td></td>
</tr>
<tr>
<td>user 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>user m</td>
<td>append</td>
<td>read, execute</td>
<td>read,write,own</td>
<td></td>
</tr>
</tbody>
</table>

(1) Access control lists

Column stored with file

(2)Capabilities

Row stored for each user

Unforgeable tickets given to user
ACLs compared to Capabilities

ACLs requires authenticating user

Processes must be given permissions

Reference monitor must protect permission setting

Token-based approach avoids need for auth

Tokens can be passed around

Reference monitor must manage tokens
UNIX-style file system
UNIX-style file system ACLs

Permissions:
- Directory?
- Owner (r,w,x), group (r,w,x), all (r, w, x)

Owner (rist)
Group (staff)
Who uses capabilities?

- Amoeba: distributed operating system (1990’s)
- Eros (extremely reliable operating system)

- IBM System 38
- Intel iAPX 432

Capabilities are used in various ways inside modern systems all over

(From Wikipedia)
Delegation

Need to give a process, other user access

In ACL, process run by user inherits user’s permissions

In Cap, process can pass around token
Revocation

Take away access from user or process

In ACL, remove user from list

In Cap, more difficult

Reference monitor must know where tokens are

Using pointer indirection
UNIX-style file system ACLs

Permissions:
- Directory?
- Owner (r,w,x), group (r,w,x), all (r, w, x)

Owner (rist)
Group (staff)
Roles (groups)

Group is a set of users

Administrator  User  Guest

Simplifies assignment of permissions at scale

User 1 -> Administrator -> /etc/passwd
User 2 -> User -> /usr/local/
User 3 -> Guest -> /tmp/
UNIX file permissions

- Owner, group
- Permissions set by owner / root
- Resolving permissions:
  - If user=owner, then owner privileges
  - If user in group, then group privileges
  - Otherwise, all privileges
UNIX Process permissions

• Process (normally) runs with permissions of user that invoked process

/etc/shadow is owned by root

Users shouldn’t be able to write to it generally
How do you reset your password?
Process permissions continued

UID 0 is root

Real user ID (RUID) --
same as UID of parent (who started process)

Effective user ID (EUID) --
from set user ID bit of file being executed or due to sys call

Saved user ID (SUID) --
place to save the previous UID if one temporarily changes it

Also SGID, EGID, etc..
Executable files have 3 setuid bits

- Setuid bit – set EUID of process to owner’s ID
- Setgid bit – set EGID of process to group’s ID
- sticky bit:
  - 0 means user with write on directory can rename/remove file
  - 1 means only file owner, directory owner, root can do so

So passwd is a setuid program

program runs at permission level of owner, not user that runs it
How do you reset your password?
seteuid system call

uid = getuid();
eid = geteuid();
seteuid(uid);  // Drop privileges
...
seteuid(eid);  // Raise privileges
file = fopen( "/etc/shadow", "w" );
...
seteuid(uid);  // drop privileges

seteuid can:
- go to SUID or RUID always
- any ID if EUID is 0
Details of setuid more complicated

Chen, Wagner, Dean “Setuid Demystified”

(a) An FSA describing setuid in Linux 2.4.18
Setuid allows necessarily privilege escalation but...

• Source of many privilege escalation vulnerabilities

Control-flow hijacking vulnerability (next lecture) in local setuid program gives privilege escalation

Race conditions
Race conditions

Time-of-check-to-time-of-use (TOCTTOU)

```c
if( access("/tmp/myfile", R_OK) != 0 ) {
    exit(-1);
}

file = open( "/tmp/myfile", "r" );
read( file, buf, 100 );
close( file );
print( "%s\n", buf );
```
Say program is setuid root: access checks RUID, but open only checks EUID

access("/tmp/myfile", R_OK)

In –s /home/root/.ssh/id_rsa /tmp/myfile

open( "/tmp/myfile", "r" );

print( "%s\n", buf );

Prints out the root’s secret key...
euid = geteuid();
ruid = getuid();
seteuid(ruid);        // drop privileges
file = open("/tmp/myfile", "r");
read( file, buf, 100 );
close( file );
print("%s\n", buf );
Summary

• Multics: seminal multi-user operating system
  – many security features
  – significant auditing performed, achieved high security certifications

• MLS security principles
  – covert channels

• Access controls (matrices, ACLs, capabilities)
• UNIX style file and process permissions