CPSC 525: Access Control

“Deny by default.”

Michael E. Locasto

Department of Computer Science
UofC
CPSC 525/625

January 18, 2013
Announcements (2 minutes)

Learning Objectives for Today (1 minute)

→ Gain an understanding of some fundamental access control concepts

→ Appreciate just how much we rely on access control to provide a basis for a “secure” system
→ HW1 is released. Due 6 February.
→ More interaction on Piazza, please!
Is Access Control de facto “Security”?

Access Control often forms the foundation of protection in real systems.

When in doubt: sprinkle on “security”:

```html
<script type='text/javascript' src='includes/scripts/login.js'></script>

<form method="post" name="login_form" id="login_form">
  <div id="signon">
    <div id="uofc">University of Calgary</div>
    <div id="myuofc">UofC Access</div>
    <div id="alert"></div>
  </div>
  <h1>Sign In</h1>
  <div><label id="eid">eID</label> <input type="text" maxlength="32" name="username"></div>
  <div><label id="password">Password</label> <input type="password" maxlength="128"></div>
</form>
```
I ask you: is there a token we can take as belief that the party we allow access to is trustworthy and will not violate our confidentiality, integrity, or availability?

Does a label attest to the thing itself?
Terms

Access Control Matrix
Access Control List
Discretionary Access Control
Mandatory Access Control
Authentication (passwords, public key, etc.)
Authorization (permissions)
Authentication
You Can’t Get Away From It
You are changing the password for DB2Admin. If you do this, DB2Admin will lose all EFS-encrypted files, personal certificates, and stored passwords for Web sites or network resources.

To avoid losing data in the future, ask DB2Admin to make a password reset floppy disk.

New password
Confirm new password

If the password contains capital letters, they must be typed the same way every time.

How to create a strong password

Type a password hint

The password hint will be visible to everyone who uses this computer.

What is a password hint?

Change password  Cancel
Authentication
You Can’t Get Away From It

Sign In to Data.Gov

You must be logged in to access this page

Sign in with your Socrata ID

Use your Email and Password to sign into all Socrata powered sites.

Email

Password  Forgot?

Sign In  Don't have an account? Sign up now.

Or... Use one of these accounts to sign in. Take advantage of additional features these accounts provide and sign in with one click.

Connect with Facebook

Connect with Twitter

Sign in with Google

Sign in with OpenID
Examples of Authorization Mechanisms

firewall
Unix filesystem permissions
filesystem ACLs
SELinux MAC and TE labels
PTE bits in memory address translation (r/w/x, ?)
OO encapsulation, data hiding, visibility rules (gone?)
.htaccess
WebSOS (anti-DDoS: solve a CAPTCHA first)
Three Methods for the File system

[locaesto@csl demo]$ more /etc/sysconfig/iptables
/etc/sysconfig/iptables: Permission denied
[locaesto@csl demo]$ ll /etc/sysconfig/iptables
-rw-------. 1 root root 476 Aug 21 10:00 /etc/sysconfig/iptables
[locaesto@csl demo]$ ll -Z /etc/sysconfig/iptables
-rw-------. root root system_u:object_r:system_conf_t:s0 /etc/sysconfig/iptables
[locaesto@csl demo]$ getfacl /etc/sysconfig/iptables
getfacl: Removing leading '/' from absolute path names
# file: etc/sysconfig/iptables
# owner: root
# group: root
user::rw-
group::---
other::---

[locaesto@csl demo]$ exit
logout
Connection to csl.cpsc.ucalgary.ca closed.
To the terminal...
The readings listed for tonight in TCSS are a review of the protection services available in operating systems, based on the kinds of hardware primitives described in the first two papers.

If you read nothing else, you should read this class paper: “The Protection of Information in Computer Systems” by Jerome H. Saltzer and Michael D. Schroeder