

# CS530L – lab component of Security Systems course

January 13, 2012

## Correlation

### lab component << >> main course

- loosely coupled
- contributes to course grade
  - directly: via grading of individual labs
  - indirectly: subject matter may appear in exams
- cumulative lab results are reported to Professor Mirkovic who considers them in determining course grade

## Lab sessions per week

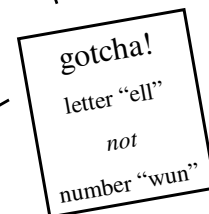
- a 50-minute lab lecture
  - Friday 4:00 pm, in RTH105
  - addresses the theory that the exercise demonstrates
  - explains the exercise procedurally
- an 80-minute lab exercise
  - at a time the following week
  - performed hands-on
  - per specific instructions
  - assisted by grader – Simon Woo

## Lab website

<http://www-scf.usc.edu/~csci530l/>

or equivalently

<http://ccss.usc.edu/530l>



## 3 candidate timeslots for scheduling

Wednesday    Thursday    Friday

9:30a-10:50a

1:00p - 2:20p

2:20p - 3:40p\*

Location: OHE406 - fourth floor Olin Hall

\* lab lecture follows at 4pm

## Lab mechanics

- sign up for a lab session (non-DEN students)
- by filling out a form

Edit record	
Wed1300-1420:	<input type="text" value="2"/>
Thu0930-1050:	<input type="text" value="0"/>
Fri1420-1540:	<input type="text" value="1"/>
ID:	<b>morgan</b>
<input type="button" value="[ save ]"/> <input type="button" value="[ cancel ]"/>	

## Lab mechanics

- form is at <http://unexgate.dmorgan.us/cgi-bin/csvupdate.pl>
- express a preference (1, 2, or 3) or conflict (0) for each of the three timeslots  
(non-correct, non-complete forms will be discarded and receive later lower priority scheduling; 1=most preferred, 3=least preferred, 0=conflict)
- first give 0's to all conflicting timeslots
- then give 1, 2, 3 to any remaining timeslots
  - if you had three conflicts, you're done
  - if you had two conflicts, give 1 to the other slot
  - if you had one conflict, give 1 & 2 to the other two slots
  - if you had no conflicts, give 1, 2, & 3 to the other three slots
- I will seek to follow preferences
- response deadline – end of Tuesday 1/17/2011

## An acceptably filled form

- 0 for any conflicts (there's one of them in this example)
- preference rankings for any and all remaining (indicated by 1, 2, 3 in decreasing order of preference)
- no blanks/omissions

Edit record	
Wed1300-1420:	<input type="text" value="2"/>
Thu0930-1050:	<input type="text" value="0"/>
Fri1420-1540:	<input type="text" value="1"/>
ID:	<b>morgan</b>
<input type="button" value="[ save ]"/> <input type="button" value="[ cancel ]"/>	

## Lab exercise mechanics

- before: preview website's posted instructions
- attend your chosen/assigned lab session
- lab will be attended by assisting lab grader
- recover and install your removable hard drive
- perform the week's prescribed lab
- after: turn in requested result electronically
  - email it to [csci530l@usc.edu](mailto:csci530l@usc.edu)
  - use prescribed email title for each lab
  - deadline: by start of following week's lab

## Lab mechanics

- there are 10 lab exercises
- each is followed by a few questions
- every question must be answered
- each lab graded
- overall average will influence course grade  
(per methodology determined by Professor Mirkovic)
- contributes 20% of course grade

## Lab workstation installations

- operating platform is Windows 7
- hosting virtual (VMware) operating systems
  - Centos (linux)
  - Fedora 7 (linux)
  - Windows XP

## DETER

cyber-DEfense Technology Experimental Research

- a computer network testbed
- some exercises done on DETER, instead of in the lab



## Policies

- no late submissions
- submissions not accepted without attendance
- follow course online homes
  - lab website at  
<http://www-scf.usc.edu/~csci530l/>  
(different from professor's main site for the course)
  - lab lectures webcast and archived on DEN

## Representative lab topics<sup>1</sup>

- Cryptography
- Authentication
- Authorization
- Application security
- Packet sniffing
- Firewalls (DETER)<sup>2</sup>
- Intrusion detection
- ARP spoofing (DETER)
- Tunnels & VPNs (DETER)
- Computer forensics (DETER)

<sup>1</sup>subject to adjustment – changes might be made (but unlikely)

<sup>2</sup>labs done on the DETER system are performed remotely

## Calendar schedule

<u>Fri lecture</u>	<u>Topic</u>	<u>lab performed week of:</u>
1/20	Cryptography	1/23 –
1/27	no lecture	
2/3	Authentication	2/6 -
2/10	Authorization	2/13 -
2/17	Application security	2/20 -
2/24	Packet sniffing	2/27 -
3/2	Firewalls	(remote)
3/9	Intrusion detection	3/12 –
3/16	no lecture – spring break	
3/23	arp spoofing	(remote)
4/30	Tunnels and VPNs	(remote)
4/6	Computer forensics	(remote)

Prof Mirkovic's lectures vs our labs – note 15 weeks vs only 10  
we conclude *before* end-of-semester

## DEN students

- lab exercises are performed in VMware virtual machines
- vm's run under VMware Player
  - free from [www.vmware.com](http://www.vmware.com)
  - please install (or use other VMware you may have)
- same vm's as in lab will be made available to you via download (details forthcoming)
- these are not for the consumption of non-DEN students

## Today's take-away for your to-do list

- Non-DEN students
  - please make your timeslot choices per earlier instructions
- DEN students
  - please install VMware Server on a computer available to you

## Contacts and support

- discussion forum (preferred)
  - “Labs” subsection of forum at CS530 DEN site
- email
  - csci5301@usc.edu lab grader, me, course TA, prof collectively
  - davidmor@usc.edu me individually
- office hours
  - I am part-time, no office, no fixed office hours
  - case-by-case, by appointment, possible before Friday lecture (email a request)

# Thank you

- for sharing an interest in the subject matter
- for your kind attention today