CS530L – lab component of Security Systems course

August 28, 2015

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 Neuman who considers them in determining course grade
Lab sessions per week

- a 50-minute lab lecture
  - Friday 4:30 pm, in OHE122
  - 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 graders - Xuanni Du and Gautam Bhatnagar

Lab website

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

or equivalently

http://ccss.usc.edu/530l
7 candidate timeslots for scheduling

<table>
<thead>
<tr>
<th>Mon</th>
<th>Tue</th>
<th>Wed</th>
<th>Thu</th>
<th>Fri</th>
</tr>
</thead>
<tbody>
<tr>
<td>10:30a-11:50a</td>
<td>12:30p-1:50p</td>
<td>12:30p-1:50p</td>
<td>10:30a-11:50a</td>
<td>3:00p-4:20p</td>
</tr>
<tr>
<td>1:00p-2:20p</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2:30p-3:50p</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Location: OHE406 - fourth floor Olin Hall

Lab mechanics

- sign up for a lab session
- by filling out a form
Lab mechanics

- form is at http://dmorgan.us/cgi-bin/csvupdate.pl
- express a preference 1-2, 5, or 0, for each of the 7 timeslots
  (non-correct, non-complete forms will get discarded and receive later lower priority scheduling; first choice, 2=second choice, 5=lesser choices, 0=conflict)
- give a single 1 and single 2, to your top 2 timeslots
- give 5’s to all non-conflicting but unpreferred timeslots
- give 0’s to all conflicting timeslots
- I will seek to follow preferences
- response deadline – end of Tuesday 9/1/2015

An acceptably filled form

For the 7 timeslots:
- a single “1”
- a single “2”
- exactly five “5 or 0”s
- no blanks/omissions

Note: web form does not dynamically validate user input up front. But at the backend incorrect records get filtered out before processing. Please enter your preferences carefully to make sure they receive consideration.
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
  - use prescribed email title for each lab
  - deadline: start of following week’s lab timeslot
  regardless whether a lab is then actually performed (or is remote)

Lab mechanics

- there are 10 lab exercises
- each is followed by a few questions
- every question must be answered
- each lab graded fail/lo-pass/pass/hi-pass

\[
\begin{array}{cccc}
0 & 1 & 2 & 3 \\
\end{array}
\]

- 9 highest grades averaged (i.e., lowest discarded)
- average will influence course grade
  - average > 2 raises/enhances
  - average < 2 lowers/damages
  - average = 2 no effect
Lab workstation installations

- operating platform is Windows 7
- hosting virtual (vmware) operating systems
  - CentOS 6.4 linux
  - CentOS 4.3 with Snort and overflowable stack
  - Kali linux with hashcat pw cracker and heartbleed attacker
  - Fedora 19 with heartbleed-vulnerable openSSL

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 on DEN
Representative lab topics

- Cryptography/key mgmt
- Authentication
- Authorization
- Application security
- Packet sniffing
- Firewalls
- Intrusion detection
- ARP spoofing
- Tunnels & VPNs
- Computer forensics

subject to adjustment – some changes might be made

Which labs use which VMs?

- Cryptography/key mgmt – CentOS-6.4
- Authentication – kali linux
- Authorization – CentOS-6.4
- Application security
  - Stack overflow uses CentOS 4.3 min-gdb
  - Heartbleed uses kali linux
  - c sign extension bug uses CentOS-6.4
- Packet sniffing – CentOS-6.4
- Intrusion detection – CentOS 4.3 min-gdb
- the other 4 – DETER/remote  n/a
Calendar schedule

<table>
<thead>
<tr>
<th>Fri lecture</th>
<th>Topic</th>
<th>lab meeting week of:</th>
<th>due:</th>
</tr>
</thead>
<tbody>
<tr>
<td>9/4</td>
<td>Cryptography</td>
<td>9/7</td>
<td></td>
</tr>
<tr>
<td>9/11</td>
<td>Authentication</td>
<td>9/14</td>
<td></td>
</tr>
<tr>
<td>9/18</td>
<td>Authorization</td>
<td>9/21</td>
<td></td>
</tr>
<tr>
<td>9/25</td>
<td>Application security</td>
<td>9/28</td>
<td></td>
</tr>
<tr>
<td>10/2</td>
<td>Packet sniffing</td>
<td>10/5</td>
<td></td>
</tr>
<tr>
<td>10/9</td>
<td>Firewalls</td>
<td>(remote)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- 10/16 Midterm – assumed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10/23</td>
<td>Intrusion detection</td>
<td>10/26</td>
<td>10/23 Fri</td>
</tr>
<tr>
<td>10:30</td>
<td>arp spoofing</td>
<td>(remote)</td>
<td>11/13 Fri</td>
</tr>
<tr>
<td>11/6</td>
<td>Tunnels and VPNs</td>
<td>(remote)</td>
<td>11/20 Fri</td>
</tr>
<tr>
<td>11/13</td>
<td>Computer forensics</td>
<td>(remote)</td>
<td>11/29 Sun</td>
</tr>
</tbody>
</table>

- Prof Neuman’s lectures vs our labs – note 15 weeks vs only 10
  - we conclude by around mid-November

DEN students

next Friday expect announcement of a URL (or posted earlier on lab website) where you can download VMware virtual machines identical to those in the lab (please install VMware player v6 in order to use them)
Today’s take-away for your to-do list

- Non-DEN students
  - please make your timeslot choices per earlier instructions
- DEN students
  - install VMware player if you don’t already have some version of VMware

Email contacts

- csci530l@usc.edu
  - lab graders, me, course TA, prof collectively
- davidmor@usc.edu
  - me individually
Thank you

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