Computer Science @ CI

Michael Soltys
Professor and Chair of Computer Science

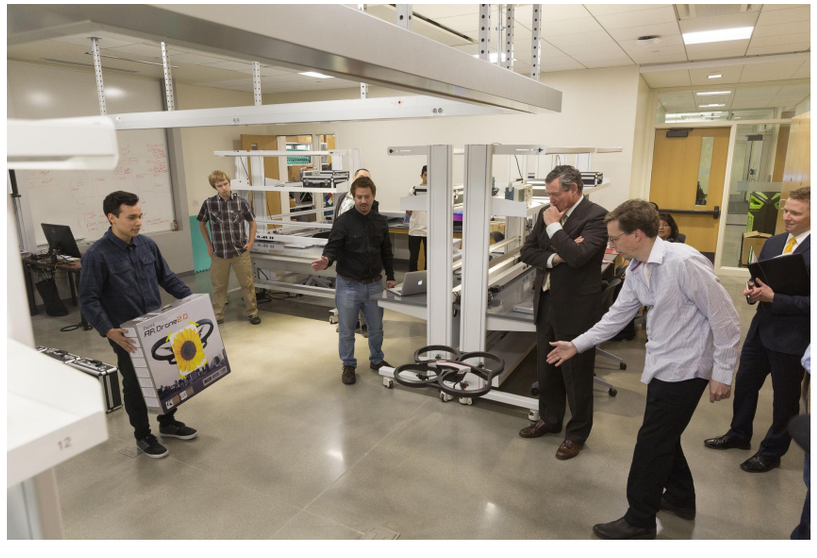
November 6, 2018

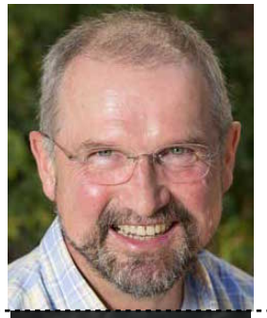
Regional Defense Partnership
For the 21st Century
(RDP-21)

Computer Science @ CI

Best kept secret in Ventura County

California State University at Channel Islands: Department of Computer Science



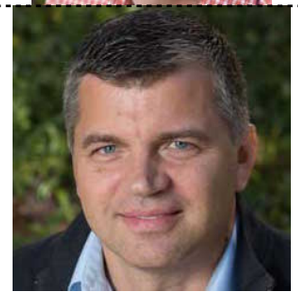


AJ Bieszczad
CI Rainbow Project

Houman Dallali
Mechatronics

Jason Isaacs
Embedded Systems & UAVs

Brian Thoms
Social Media, online teaching



Michael Soltys
Algorithms & Security

ACM Regional Competitions 2018

ACM Regional Competitions 2018

The 2018 World Finals

ACM Regional Competitions 2018

The 2018 World Finals

1. Moscow State University
2. Moscow Institute of Physics and Technology
3. Peking University
4. The University of Tokyo
5. Seoul National University
6. University of New South Wales
7. Tsinghua University
8. Shanghai Jiao Tong University
9. St. Petersburg ITMO University
10. University of Central Florida

https://icpc.baylor.edu/regionals/finder/world-finals-2018

Sobering Stats

- NSB: engineering degrees dropped 20% since 1985
- ACT: less than 6% high school seniors plan to take engineering
- AFS: 0.8% students plan to major in math
- Intel Science Fair: 6million Chinese students applied; 65K US students did (~100:1)
- 50% of US Engineering PhDs go to foreign students
- In next decade, 90% of world scientists & engineers will reside in Asia

COMPUTER SCIENCE PROGRAM

Computer Science and Information Technology is a fast-growing and vibrant program at CSU Channel Islands. Our faculty specialize in algorithms, artificial intelligence, security, social media, and robotics.
Learn more »

NEWS & EVENTS MORE »

Prof. Soltys will be giving an invited talk at LDS&LAW2016 in London, February 2-4, 2016.

Prof. Thoms' co-authored paper, "Task Oriented Reading of Instructional Materials and Its Relationship to Message Scores in Online Learning Conversations," to be presented at the Hawaiian Conference on System Sciences on January 6, 2016.

Prof. Claveau to present his paper, "System of 3-D Printed Components for the Rapid Prototyping of Legged Robots," at the 4th International Conference on Robot Intelligence, Technology and Applications in Bucheon, Korea on December 12-15, 2015.

Prof. Thoms' co-authored paper, "Instructor versus Peer Attention Guidance in Online Learning Conversations," was published in *AIS Transactions on Human-Computer Interaction*, Volume 7, Issue 4.

Meet our faculty and staff

Course Listings

Apply Now

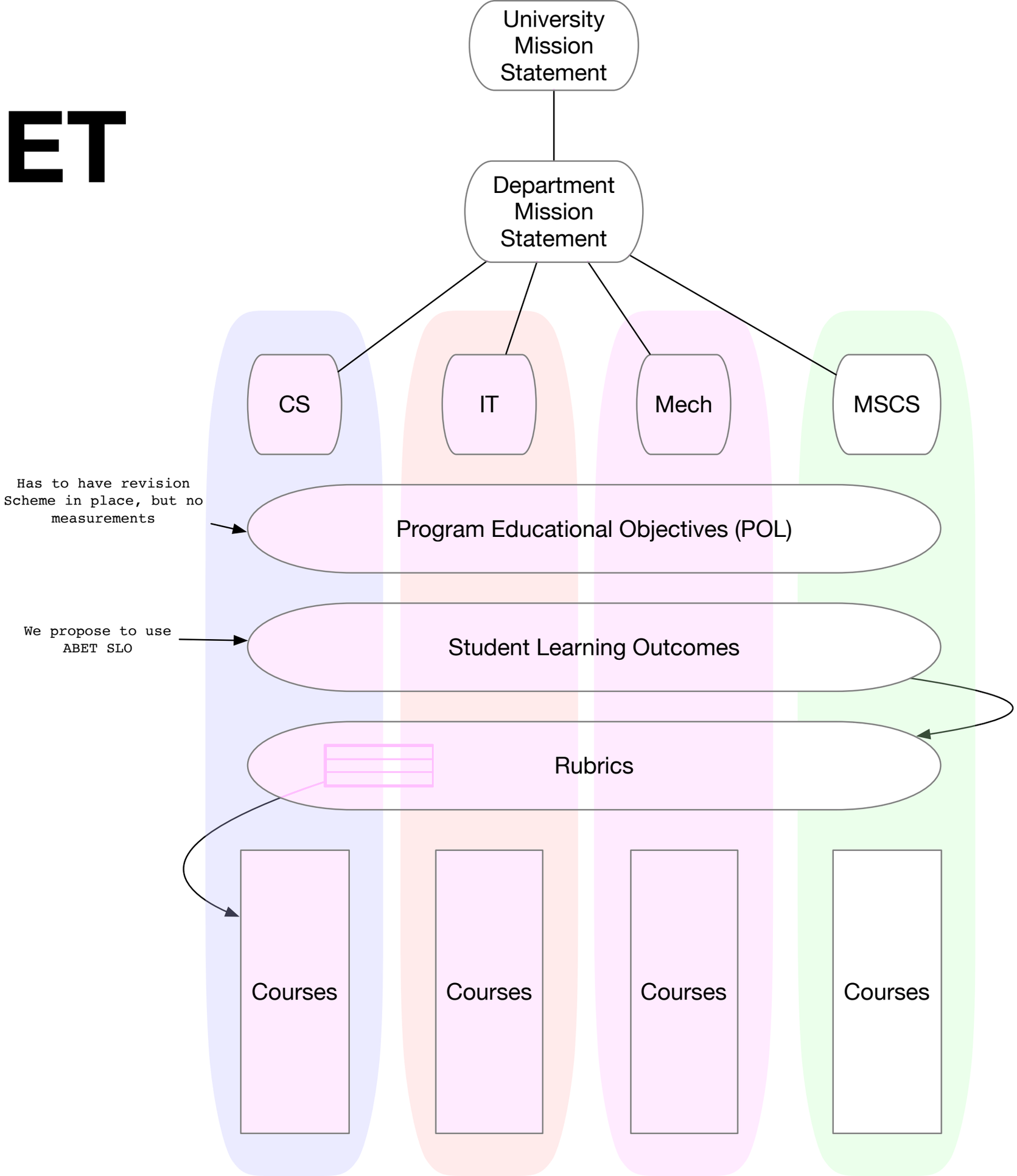
Seminars

compsci.csuci.edu

We collaborate with

- Local Companies: Advisory Board
- Navy
- HTTF
- VCCC
- VCOE

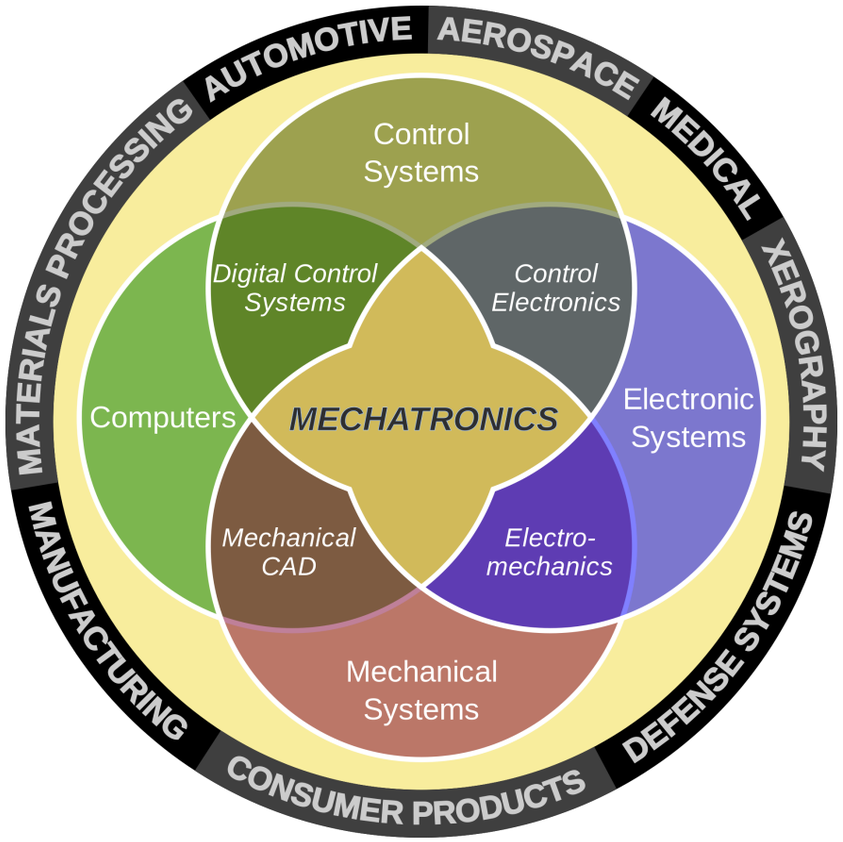
ABET

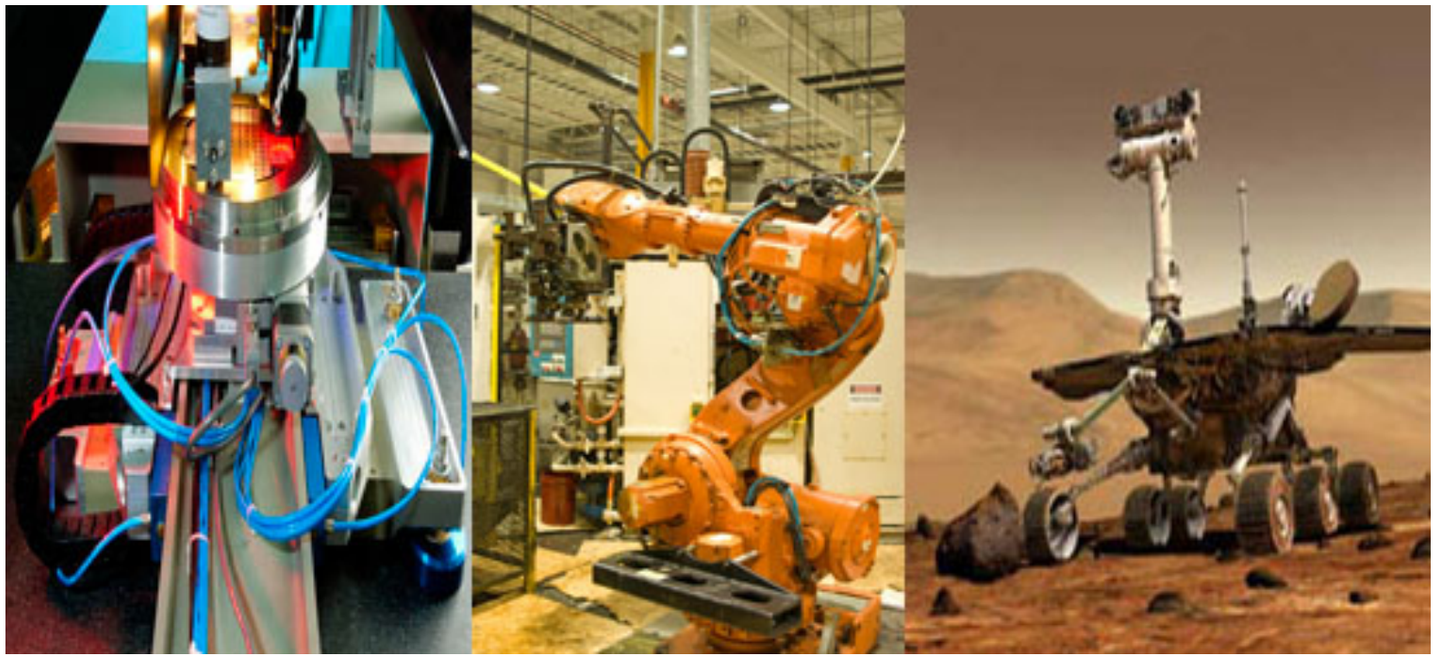

University Mission Statement
Department Mission Statement
CS
IT
Mech
MSCS
Has to have revision Scheme in place, but no measurements
Program Educational Objectives (POL)
We propose to use ABET SLO
Student Learning Outcomes
Rubrics
Courses
Courses
Courses
Courses

Mechatronics =

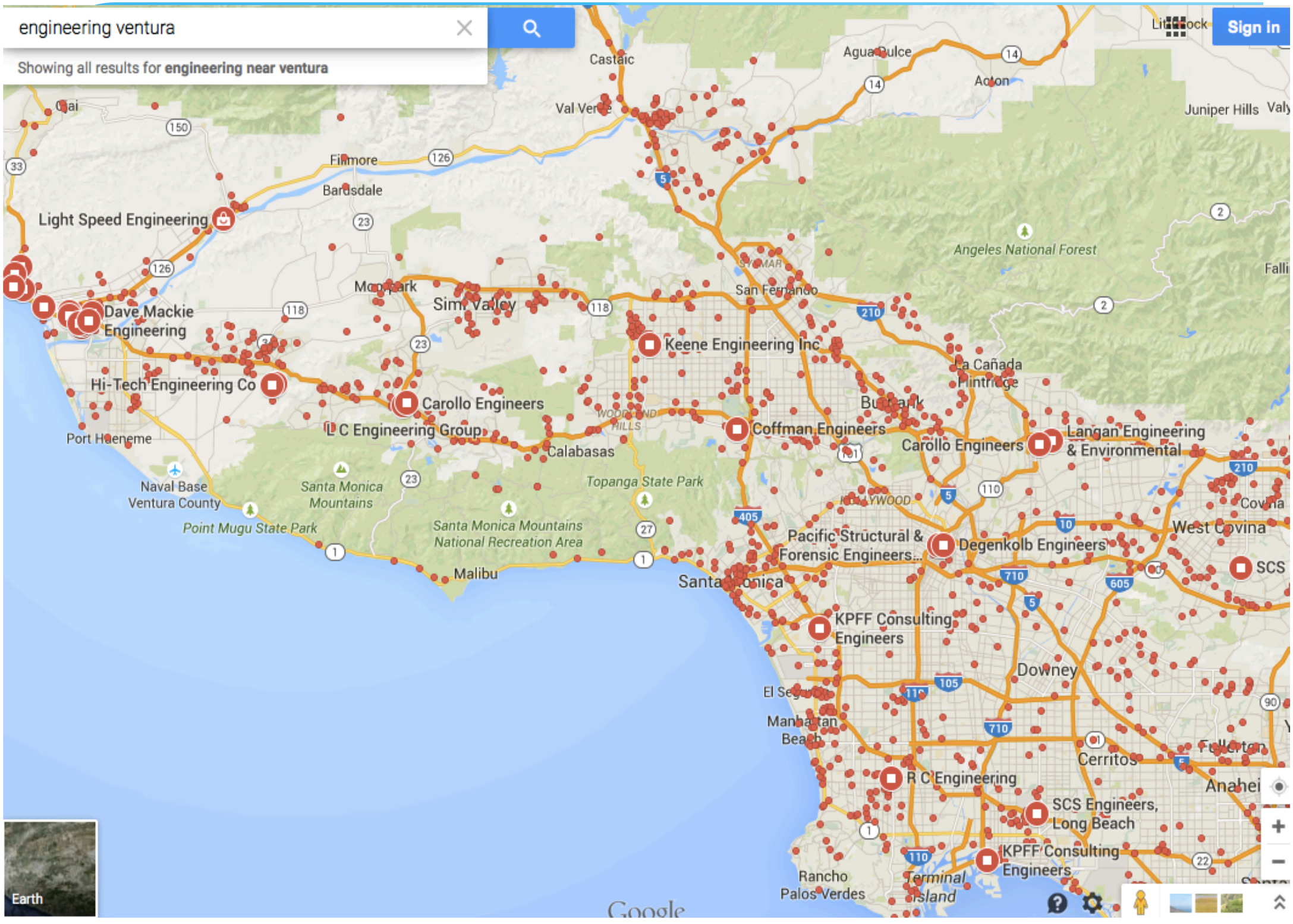
Mechanics + Electronics

- Mechatronics is a modern multi-disciplinary field of Engineering, combining Computer Hardware, Electronics and Mechanical Engineering in one.





A lot of Employment Opportunities!


engineering ventura
Showing all results for engineering near ventura
Sign in
Light Speed Engineering
Dave Mackie Engineering
Hi-Tech Engineering Co
Carollo Engineers
L C Engineering Group
Keene Engineering Inc
Coffman Engineers
Carollo Engineers
Langan Engineering & Environmental
Pacific Structural & Forensic Engineers...
Degenkolb Engineers
SCS
KPFF Consulting Engineers
R C Engineering
SCS Engineers, Long Beach
KPFF Consulting Engineers
Angeles National Forest
Topanga State Park
Santa Monica Mountains National Recreation Area
Point Mugu State Park
Naval Base Ventura County
Port Hueneme
Malibu
Calabasas
Simi Valley
Moorpark
Fillmore
Bardsdale
Castaic
Agua Dulce
Acton
Juniper Hills
San Fernando
Burbank
La Cañada Flintridge
West Covina
Downey
Cerritos
Manhattan Beach
Rancho Palos Verdes
Earth
Google

Engineers Get Top Pay

Industry	Median Entry-Level Salary[1]	Mean Annual Salary[2]
Geological and Mining Engineering and Sciences National Labor Stats	Data Not Provided	$100,970
Materials Science and Engineering National Labor Stats	$65,979	$91,150
Mechanical Engineering National Labor Stats	$61,523	$87,140

6 more rows, 1 more column

2015 Engineering Salary Statistics | College of Engineering

www.mtu.edu/**engineering**/.../**salary**/ Michigan Technological University

Our Focus: *Small Robotics*

Cybersecurity

Outline

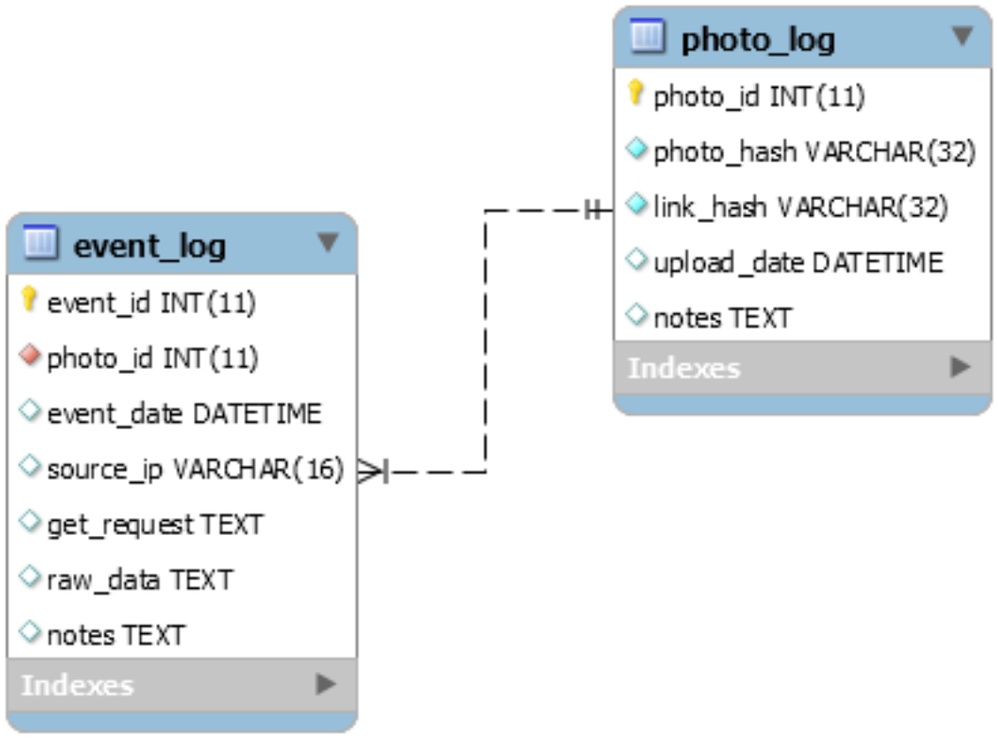
Cybersecurity at CI

Digital Forensics
Collaboration with HTTF

Penetration Testing

SEAKER

Voyager


photo_log
photo_id INT(11)
photo_hash VARCHAR(32)
link_hash VARCHAR(32)
upload_date DATETIME
notes TEXT
Indexes
event_log
event_id INT(11)
photo_id INT(11)
event_date DATETIME
source_ip VARCHAR(16)
get_request TEXT
raw_data TEXT
notes TEXT
Indexes

Password Beast

Virus Total

COMP 424/524

3 Klein's attack on RC4

Suppose w key streams were generated by RC4 using packet keys with a fixed root key and different initialization vectors. Denote by $\mathsf{K}_u = (\mathsf{K}_u[0], \ldots, \mathsf{K}_u[m]) = (\mathsf{IV}_u \| \mathsf{Rk})$ the uth packet key and by $\mathsf{X}_u = (\mathsf{X}_u[0], \ldots, \mathsf{X}_u[m-1])$ the first m bytes of the uth key stream, where $1 \le u \le w$. Assume that an attacker knows the pairs $(\mathsf{IV}_u, \mathsf{X}_u)$ – we shall refer to them as *samples* – and tries to find Rk.

In [5], Klein showed that there is a map $\mathcal{F}_i \colon (\mathbb{Z}/n\mathbb{Z})^i \to \mathbb{Z}/n\mathbb{Z}$ with $1 \le i \le m$ such that

$$\mathcal{F}_i(K[0], \ldots, \mathsf{K}[i-1], \mathsf{X}[i-1]) = \begin{cases} \mathsf{K}[i], & \text{with Prob} \approx \frac{1.36}{n} \\ a \neq \mathsf{K}[i], & \text{with Prob} < \frac{1}{n} \text{ for all } a \end{cases}$$

If the first i bytes of a packet key are known, then the internal permutation S_{i-1} and the index j at the $(i-1)$th step of the RC4 key setup algorithm can be found. We have

$$\mathcal{F}_i(\mathsf{K}[0], \ldots, \mathsf{K}[i-1], \mathsf{X}[i-1]) = \mathsf{S}_{i-1}^{-1}[i - \mathsf{X}[i-1]] - (j_{i-1} + \mathsf{S}_{i-1}[i]) \bmod n$$

The attack is based on the following properties of permutations.

Theorem 1 *For a random permutation* P*, and random number* $j \in \{0, \ldots, n-1\}$*, we have*

$$\text{Prob}(\mathsf{P}[j] + \mathsf{P}[\mathsf{P}[i] + \mathsf{P}[j] \bmod n] = i \bmod n) = \frac{2}{n}$$

$$\text{Prob}(\mathsf{P}[j] + \mathsf{P}[\mathsf{P}[i] + \mathsf{P}[j] \bmod n] = c \bmod n) = \frac{n-2}{n(n-1)}$$

where $i, c \in \{0, \ldots, n-1\}$ *are fixed, and* $c \neq i$.

AWUS 036 ACH

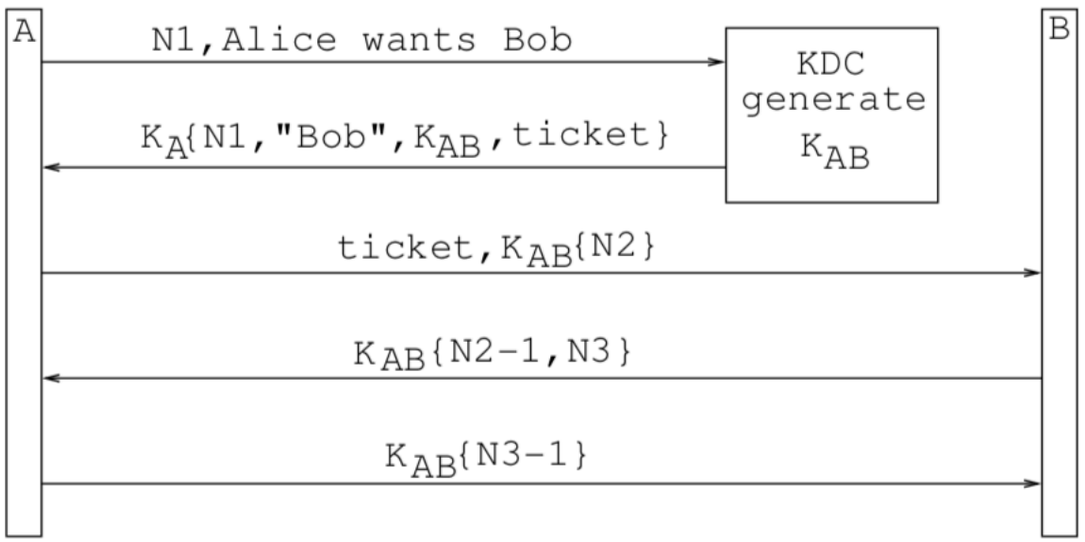
Course Outline

1. Crypto: basics
2. Crypto: symmetric ciphers, Assignment: break a MAC
3. Crypto: DES, IDEA, AES, htpasswd; case study: break WEP
4. Crypto: blocks & hashes
5. Crypto: public key: D-H, ElGamal, RSA, elliptic curves
6. Authentication: kerberos
7. Tools:
   I. OpenSSL & GnuPG
   II. Hashcat & John Ripper
   III. Kali Linux, Wireshark & Palo Alto Firewalls
   IV. Malware

Cryptoanalysis
How to break a code
Encoding vs Encryption

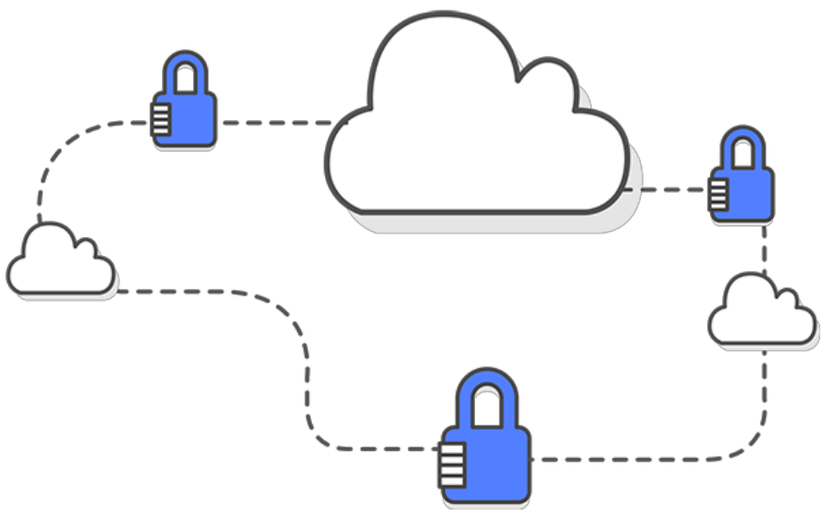
```
Base 64 Encrypted String:
oZ04bYkMsJoFV3csbYwcmXEcjnHzj3EUlHndV4kMsJoFbYkMsJ
oFeVU1wqcBtpM6bZcFtpw7wVDzV34Bbak7slU5uKc4vKkGbZQ5
bak7slUBtpw7wW/zV4w7rqjztpIAuKcHrpDztZYBsVUCv1U4xp
n/bT8WuKo/sVU5v5YAslUHta3zs5o0v5sIuVUGxpIAsqkFxmPz
Vz8cu1UKtZYHbZk8vKk0u6jzsZo4vafzuKbzvJA8sqfBbT8Vwq
cBwVUHtZnzs54FslUCs1UHtZ4BslU4xpoGiFTdmJLzwJ00wVUK
tpM6vFU3rqc4bZ04bZYGvZ4FsmPzV4w7rqjzwZ04bZ00u5j/bZ
k0v5nzvJo8x5nzwZ04bZs8v5nSbT7djpM3baw7rqjzvJ0CwpE3
sqb/bVrzwJ00wVU0v6j/bT8WuKo/sVUHwJ4GwVUHtZnzvJ4Bsq
wGbZQ5bak7xlU7spYFwWPzV3YBsVUKtZoBbak7xlU7spYFwVU1
spw0u1UHuFU1spYHeVTdoJ00wVU3v5o0sVU7rpM3iFT5baw7rq
jzsac4rpjzs5o4wWPzVz8qtZYHbak7slU7rpIAsqbSbaw7rqjz
wZ04bZg7rp4BeVTdlpLzwJ00wVU5wqcBrpg4baw0vFUHta3zr6
c0tpLSbT8qtZYHbak7slU0u6s8uWPzwJ00wVU3v5o0sVU6v5YG
vVDzV3k0v5nztqkGbZk4rpk/xlUHsqcFuKcGbZg/rqgDblTdV4
w7spLzwZ04bagHrqcGbak7v5oKbZkCwJLzwZ04tqbzvKU4rqcG
bT8Uu5jzwJYHsqb6sVU7spYJspLzwJ4HtVUHtZo8v1UHspYFvG
7zV3k8sVU7slUGup4/slU7tqfzwJQFtFUHuFUGspnSbT8Xtpjz
tZnzwJ0CbZI0sZnzwZ04bXE0upbzupY+slUHtZo4iFTdV4kMsJ
oFbYkMsJoFbZcIv5M8u5vzr6c8sJ0HeVTdlpLzwZ04bZsCv5oG
wafzuJrzwZ04bZM8sJ0Hh1TdoJ00wVU8upICv6k0uVU7rpM3bZ
QFbZoMslDzV3k0v5nzs6c0upnzwZ0MbZs4rqc5wpDzvK4AupoH
v63SVz==
```

Needham-Schroeder Protocol



8. CompTIA Security+

9. AWS security



10. Another assignment, usually coding in Python

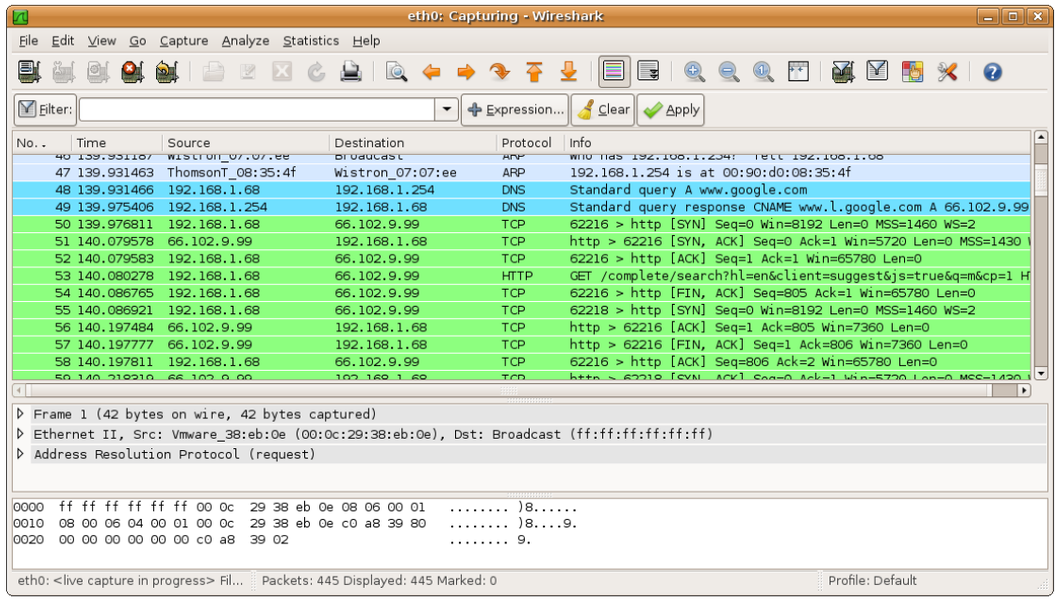
11. Presentations

    I. Long list of articles (articles more current than textbooks)

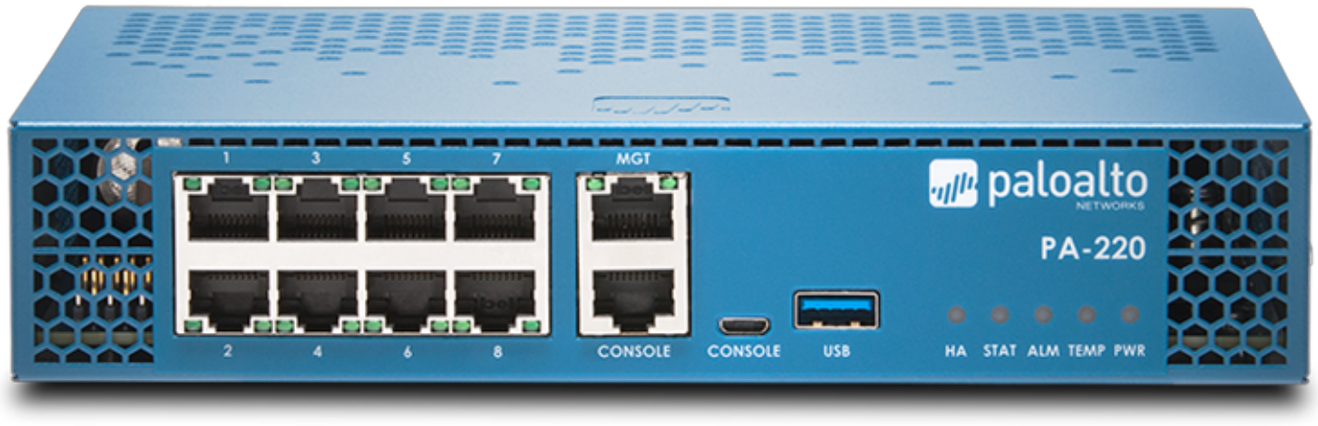
    II. Ability to articulate ideas about security

Penetration Testing

Kali Linux



Wireshark



Palo Alto Firewall

Capstone Showcase

November 29, 2018
3:00 - 5:00

Sierra Hall

Questions?

Michael Soltys

michael.soltys@csuci.ed
www.msoltys.com
@MichaelMSoltys

www.msoltys.com/mechatronics
www.msoltys.com/cybersecurity
www.msoltys.com/aws