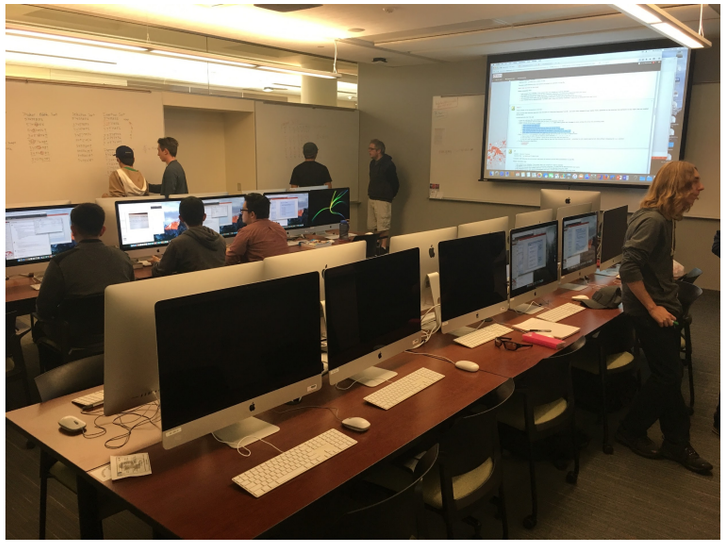
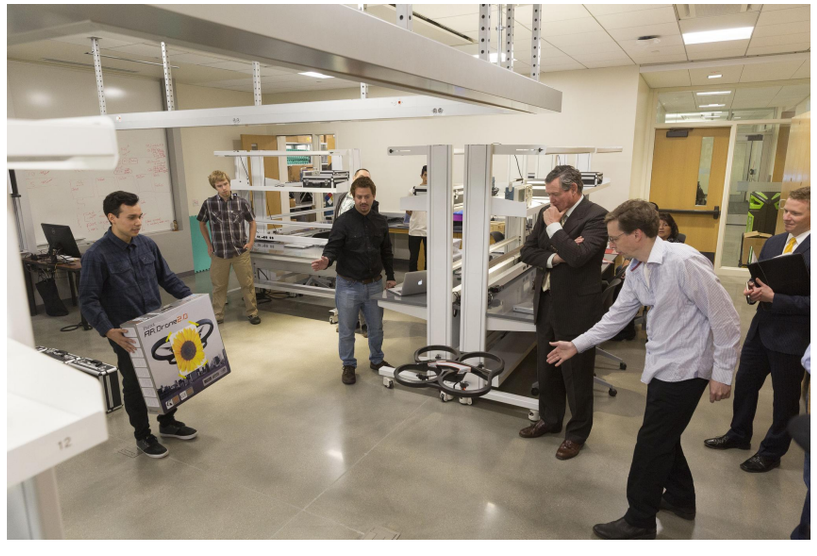
Cybersecurity Research & Education at CI

October 29, 2019
Michael Soltys

bit.ly/CyberAtCI2019

California State University at Channel Islands: Department of Computer Science





Cybersecurity

- GCTF: 40K **unfilled** jobs in California, 300K+ nation wide (https://www.cyberseek.org/heatmap.html)
- IP stolen: F-35 now the J-31
- Ransomware damages in 2018 to exceed $8B
- Baltimore City hit, $18M loss, crippled for a month (https://www.comparitech.com/antivirus/ransomware-statistics/)

Secretary Betsy DeVos
@BetsyDeVosED

We all have a role in keeping America's vital information systems & our nation safe. That's why we've partnered with @WHNSC @NSF to honor educators who are preparing the next generation of cybersecurity professionals! blog.ed.gov/2019/10/nomina...

Cybersecurity

- GCTF: 40K **unfilled** jobs in California, 300K+ nation wide (https://www.cyberseek.org/heatmap.html)
- IP stolen: F-35 now the J-31
- Ransomware damages in 2018 to exceed $8B
- Baltimore City hit, $18M loss, crippled for a month (https://www.comparitech.com/antivirus/ransomware-statistics/)

Secretary Betsy DeVos
@BetsyDeVosED

We all have a role in keeping America's vital information systems & our nation safe. That's why we've partnered with @WHNSC @NSF to honor educators who are preparing the next generation of cybersecurity professionals! blog.ed.gov/2019/10/nomina...

- We want to serve our region:
  - As a hub of expertise
  - Create a workforce
  - Offering training
  - Educating the public
  - Research & Development

“Security is the process of maintaining an acceptable level of perceived risk for a specified event”

– Richard Bejtlich

Our Philosophy
“Theory in practice”

- Strong theoretical foundations:
  - Mathematics
  - Algorithms and Protocols
  - Programming ⟶ Software Engineering
- Practical applications:
  - Hands on examples
  - R&D on real world problems
  - Partnerships with the industry

Why all these attacks?

- Large attack surface
- Complexity
- Attribution
- Skill vs Ability

- Small gains
- Skills gap
- Public education

What are the challenges?

(Challenges are opportunities!)

- Scientific foundations
- Software Engineering
- Business, IT & Academia

- Education:
  - Public
  - Workforce
- Compliance: standards, policies and regulations

October 11, 2019

8:00AM - 4:00PM

California State University Channel Islands

Petit Salon

Sponsored By

Haas Automation Inc.

CSU Channel Islands

Open to all businesses or individuals in Los Angeles, Santa Barbara, and Ventura counties with interest in cybersecurity and keeping business secure.

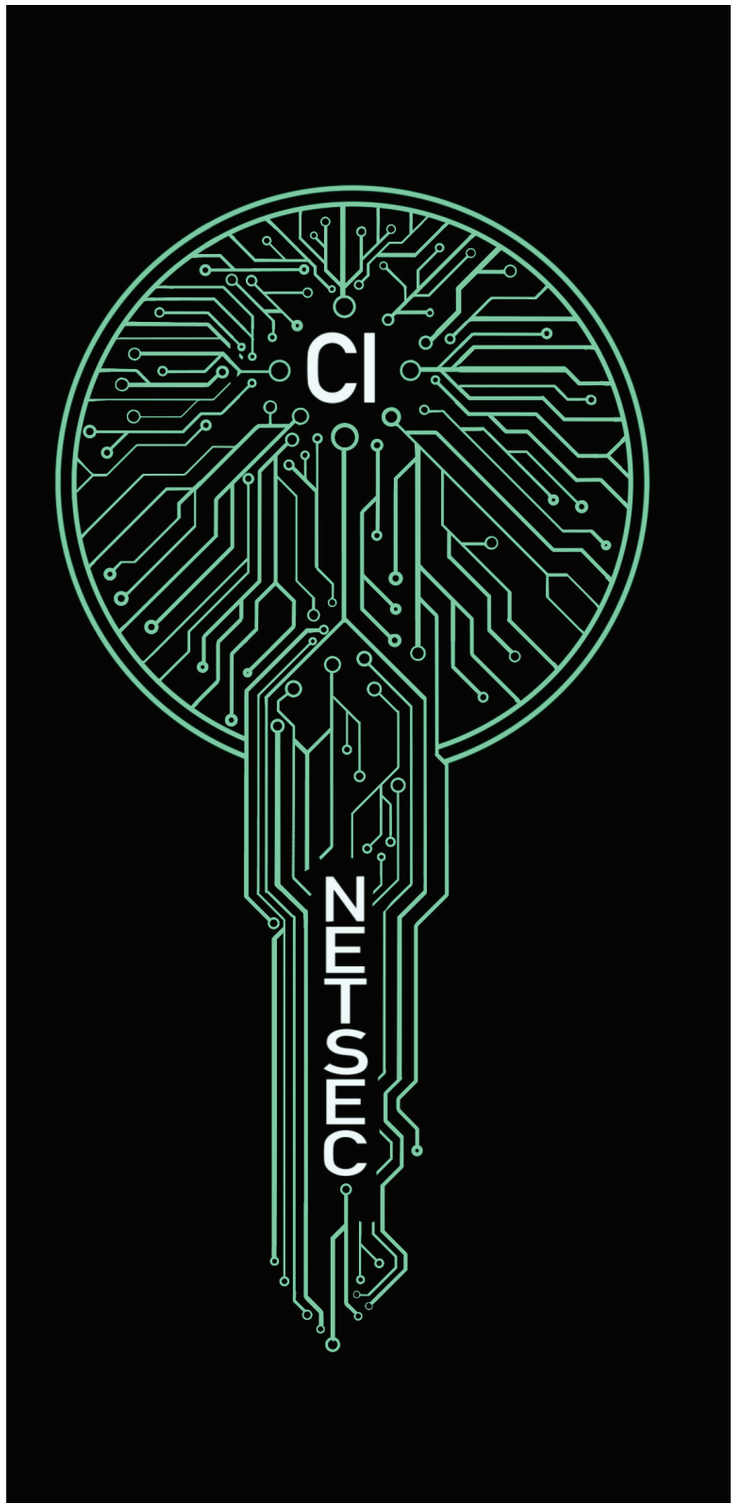
Snacks and lunch will be provided.

Please RSVP via the link below or email by Oxtober 4th:
https://bit.ly/2ZnytPH
cybersecurity-conference@haascnc.com

If you have questions please email:
cybersecurity-conference@haascnc.com

Schedule

Arrival/Registration:	8:00AM - 9:00AM
Welcome:	9:00AM - 9:30AM
Keynote:	9:30AM - 10:30AM
Presentation:	11:00AM - 12:00PM
Lunch:	12:00PM - 1:00PM
Presentation 1:	1:00PM - 1:30PM
Presentation 2:	1:30PM - 2:00PM
Presentation 3:	2:30PM - 3:00PM
Presentation 4:	3:00PM - 3:30PM
Closing:	3:30PM - 4:00PM



The NETSEC Club

The NETSEC club is a cyber security focused student organization.

What we do:
Talks from professionals in industry
Particpate in online CTFs (Capture the Flag)
Tutorials/demos of pen testing tools

GHIDRA

KALI

0x325
CI NETSEC CTF TEAM

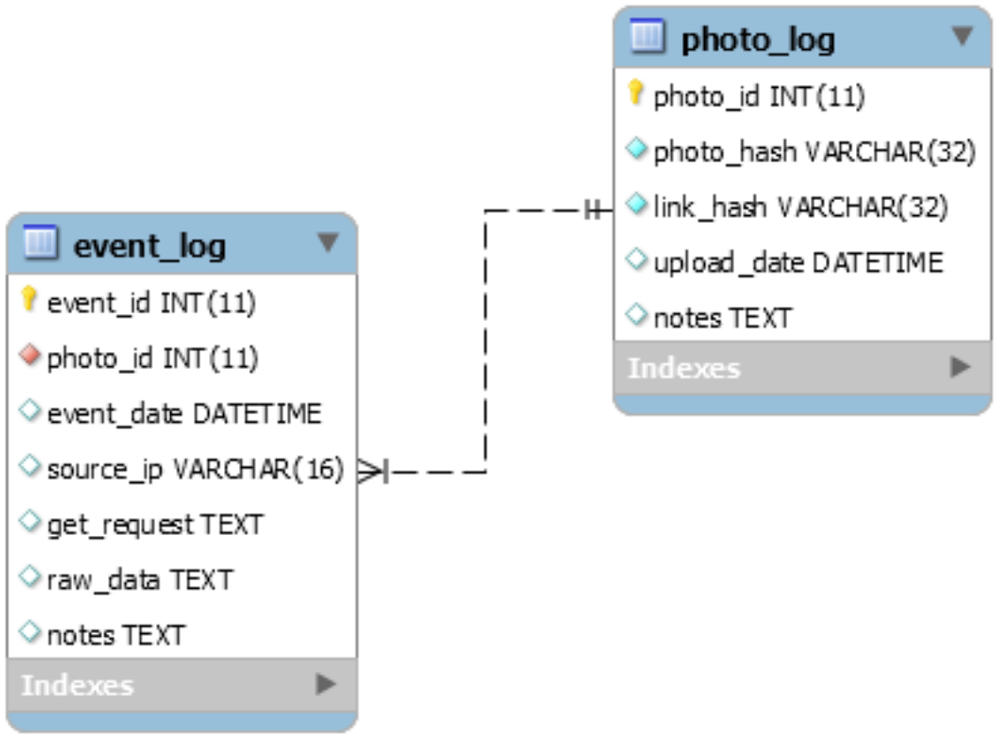
Our CTF team, 0x325, particpates in online CTF competitions during the semester.

Collaboration with SoCal HTTF

SEAKER

Password Beast

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

Virus Total

Courses

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*

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

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

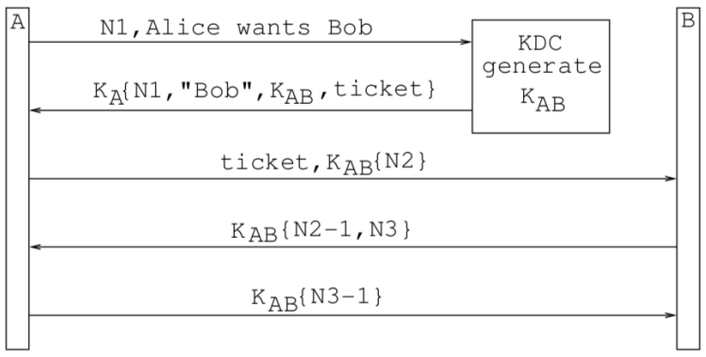
where $i, c \in \{0, \ldots, n-1\}$ *are fixed, and* $c \neq i$*.*

AWUS 036 ACH

Cryptoanalysis
How to break a code
Encoding vs Encryption

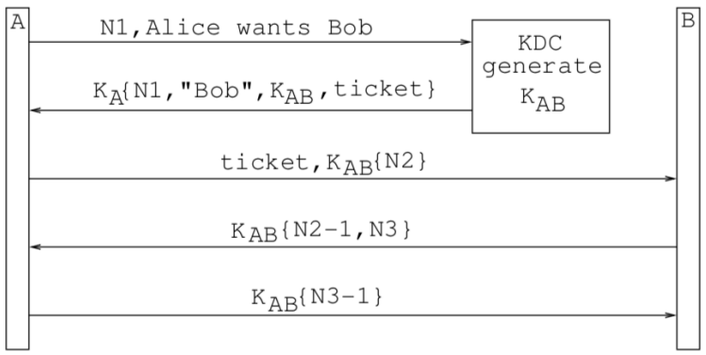
```
Base 64 Encrypted String:
oZ04bYkMsJoFV3csbYwcmXEcjnHzj3EUlHndV4kMsJoFbYkMsJ
oFeVU1wqcBtpM6bZcFtpw7wVDzV34Bbak7slU5uKc4vKkGbZQ5
bak7slUBtpw7wW/zV4w7rqjztpIAuKcHrpDztZYBsVUCv1U4xp
n/bT8WuKo/sVU5v5YAslUHta3zs5o0v5sIuVUGxpIAsqkFxmPz
Vz8cu1UKtZYHbZk8vKk0u6jzsZo4vafzuKbzvJA8sqfBbT8Vwq
cBwVUHtZnzs54FslUCs1UHtZ4BslU4xpoGiFTdmJLzwJ00wVUK
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==
```

Theory in Practice



Needham-Schroeder Protocol

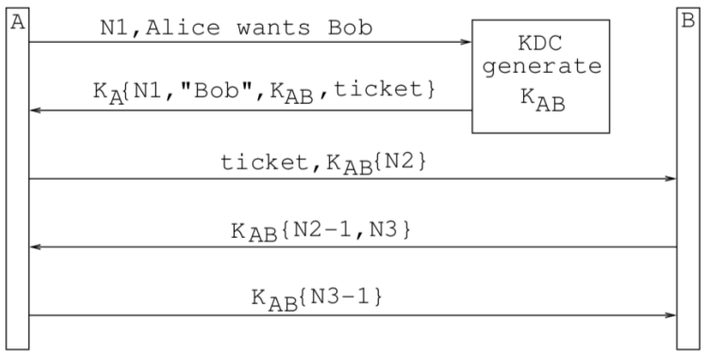
Theory in Practice



Needham-Schroeder Protocol

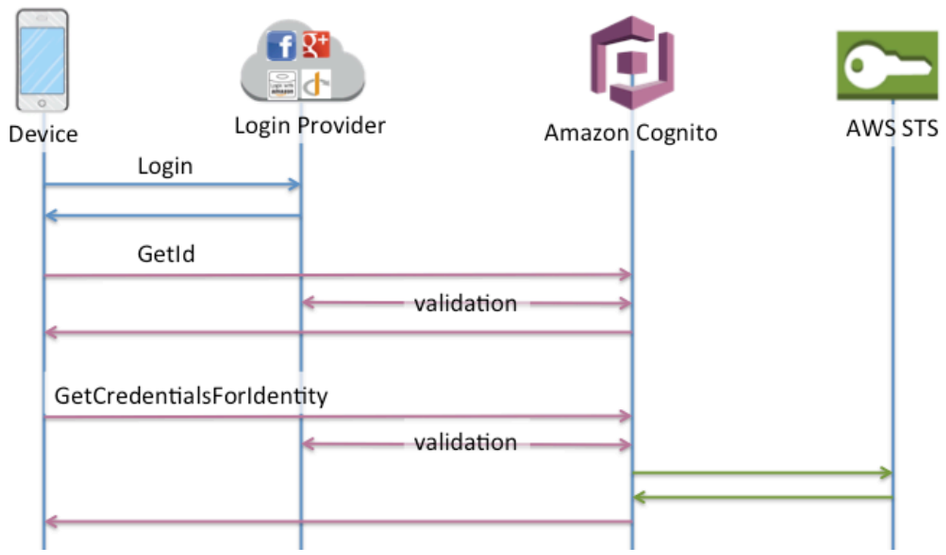
Kerberos: 3 headed hound of Hades

Theory in Practice



Needham-Schroeder Protocol

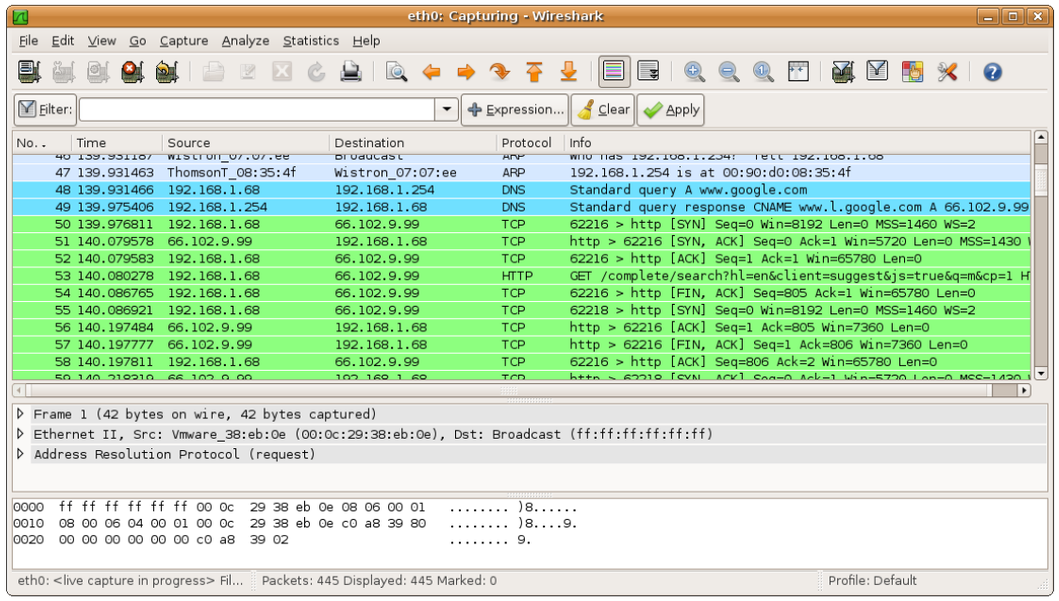
Kerberos: 3 headed hound of Hades



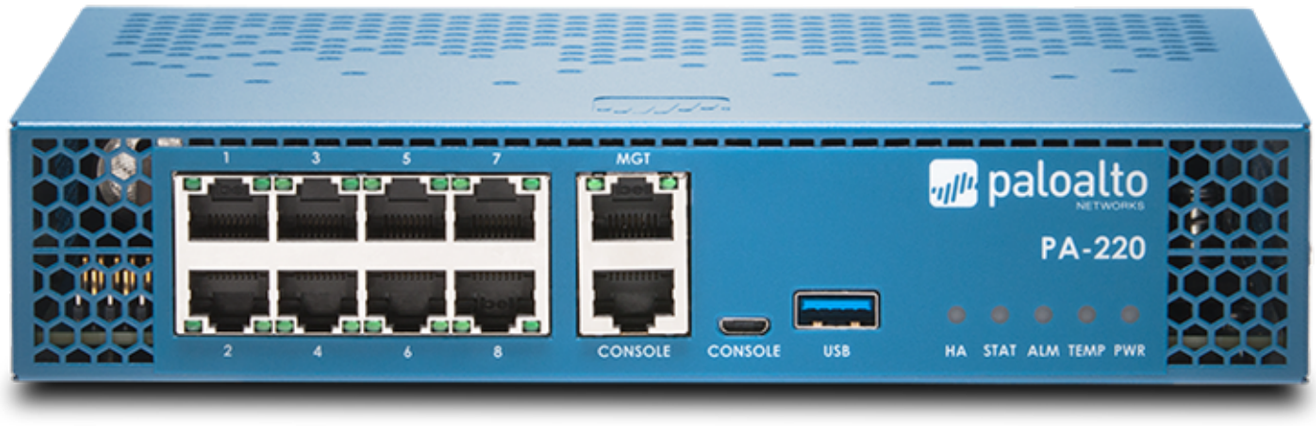
AWS Cognito: Identity Federation

Penetration Testing

Kali Linux



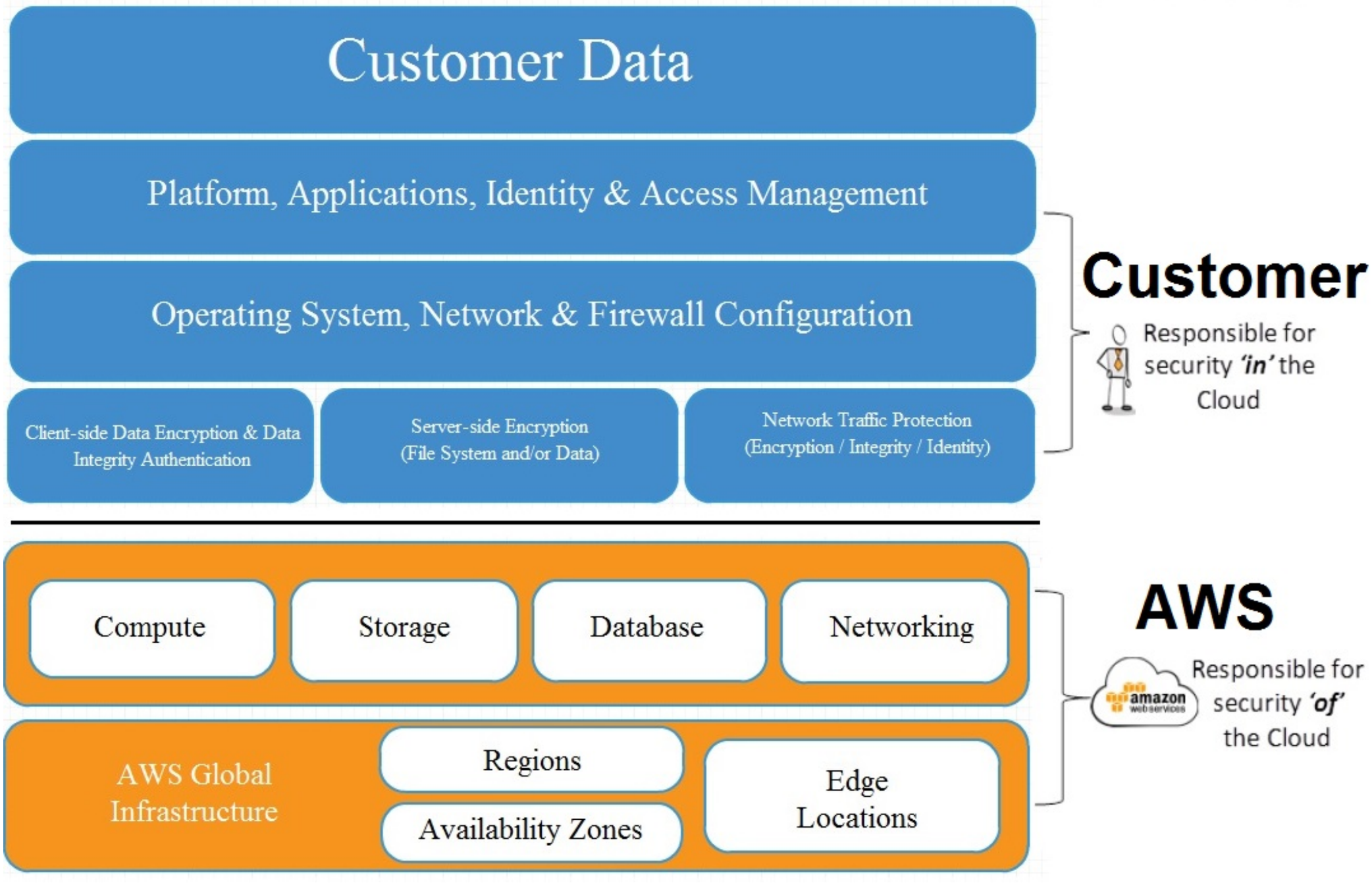
Wireshark



Palo Alto Firewall

Future: Security in the Cloud

Shared Responsibility Model

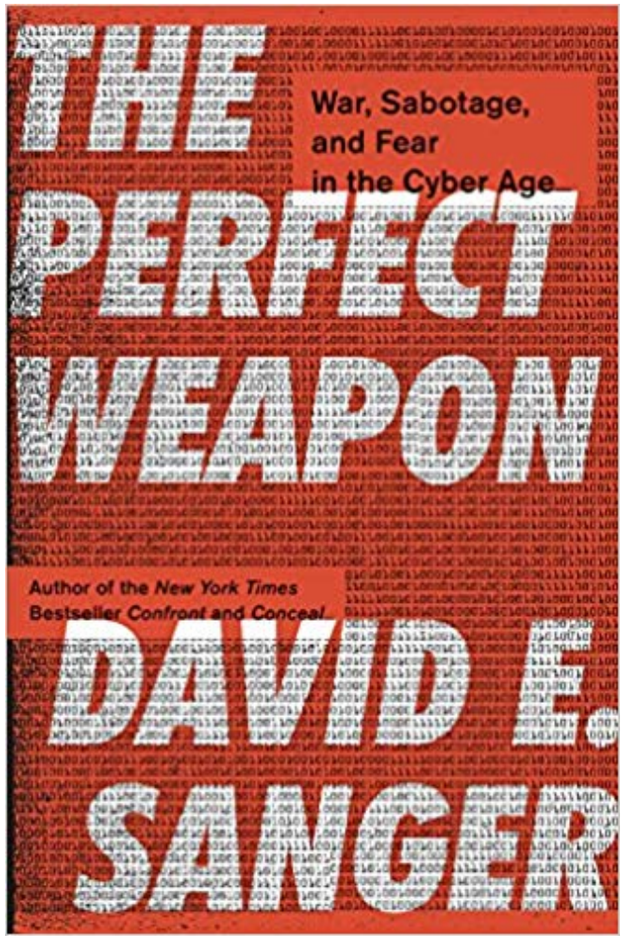


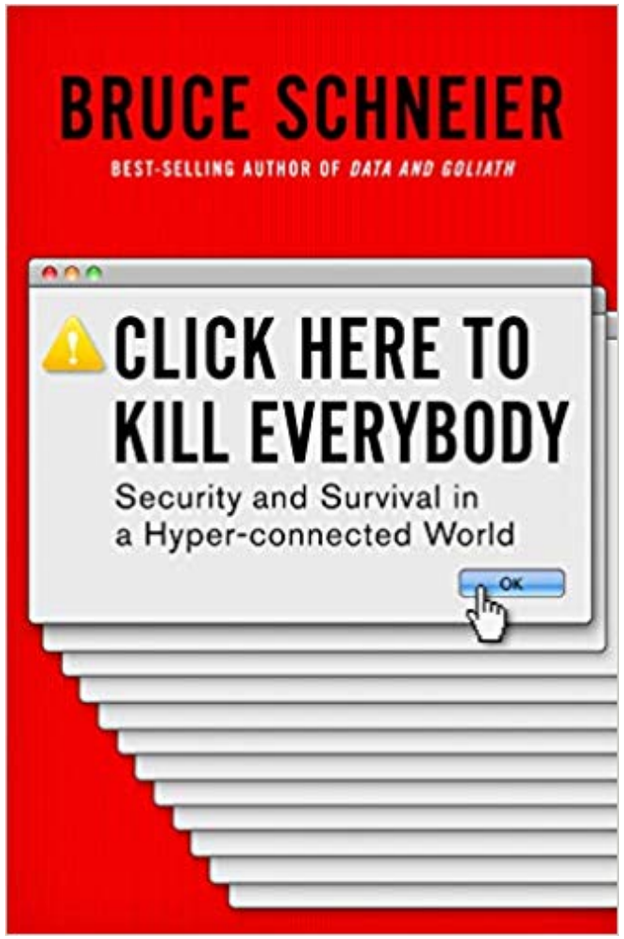
Design Principles

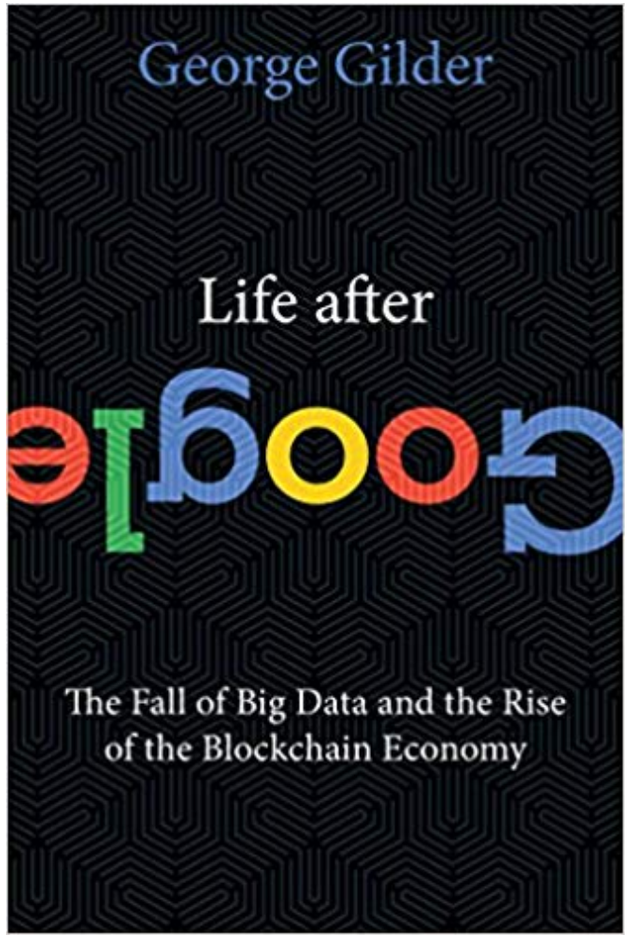
- Strong identity foundation
- Traceability
- Security at all layers
- Automate

- Protect data in transit and at rest
- Principle of least privilege
- Prepare for security events


Channel Your
POTENTIAL
with
AWS Academy
Careers in the Cloud
California State University
EXTENDED UNIVERSITY
CHANNEL ISLANDS
Contact : jeff.ziskin@csuci.edu
(805) 437-2653
COURSES
Cloud Foundations
Course Starts January 11
Cloud Architecting
Course Starts March 7


War, Sabotage,
and Fear
in the Cyber Age
THE PERFECT WEAPON
Author of the New York Times
Bestseller Confront and Conceal
DAVID E.
SANGER


BRUCE SCHNEIER
BEST-SELLING AUTHOR OF DATA AND GOLIATH
CLICK HERE TO
KILL EVERYBODY
Security and Survival in
a Hyper-connected World
OK


George Gilder
Life after
Google
The Fall of Big Data and the Rise
of the Blockchain Economy

michael.soltys@csuci.edu

@MichaelMSoltys

http://prof.msoltys.com