EE 1322 Module 7 (Guest Lecture)
Introduction to Cyber-Security:
Cyber Security: Basic concepts, Research and Workforce Opportunities

UTSA®
The University of Texas at San Antonio™
The Cyber Center For Security and Analytics

Elias Bou-Harb, Ph.D., CISSP
elias.bouharb@utsa.edu

Elias Bou-Harb

Associate Director
Associate Professor

Expertise

Operational Cyber Security
Cyber Forensics
Critical Infrastructure Security
Data Science
Digital Investigation
Internet Measurements

Research Grants

NSF OAC Core: Small: Devising Data-driven Methodologies by Employing Large-scale Empirical Data to Fingerprint, Attribute, Remediate and Analyze Internet-scale IoT Maliciousness

NSF CyberTraining CIP: Cyberinfrastructure Expertise on High-throughput Networks for Big Science Data Transfers

Recent Publications

Miranda, C., Kaddoum, G., **Bou-Harb, E.**, Garg, S. and Kaur, K., 2020. A Collaborative Security Framework for Software-Defined Wireless Sensor Networks. IEEE Transactions on Information Forensics and Security.

Torabi, S., **Bou-Harb, E.,** Assi, C. and Debbabi, M., 2020. A Scalable Platform for Enabling the Forensic Investigation of Exploited IoT Devices and Their Generated Unsolicited Activities. Forensic Science International: Digital Investigation.

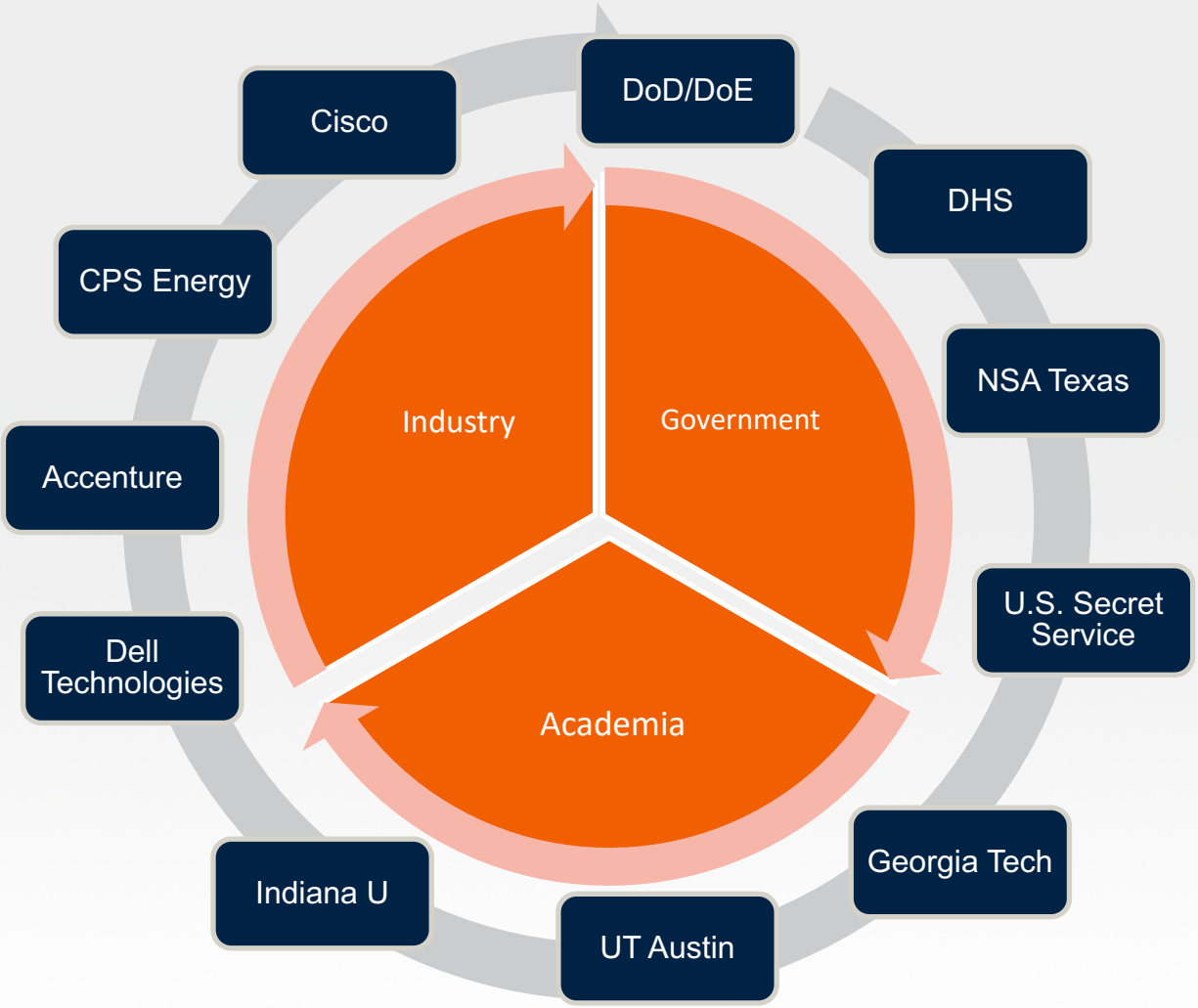
Torabi, S., **Bou-Harb, E.,** Assi, C., Karbab, E.B., Boukhtouta, A. and Debbabi, M., 2020. Inferring and Investigating IoT-Generated Scanning Campaigns Targeting A Large Network Telescope. IEEE Transactions on Dependable and Secure Computing.

Pour, M.S., Mangino, A., Friday, K., Rathbun, M., **Bou-Harb, E.**, Iqbal, F., Samtani, S., Crichigno, J. and Ghani, N., 2019. On Data-driven Curation, Learning, and Analysis for Inferring Evolving Internet-of-Things (IoT) Botnets in the Wild. Computers & Security, p.101707.

Neshenko, N., **Bou-Harb, E.,** Crichigno, J., Kaddoum, G. and Ghani, N., 2019. Demystifying IoT security: an exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations. IEEE Communications Surveys & Tutorials, 21(3), pp.2702-2733.

Cyber Threat Intelligence
Digital Forensics
Infrastructure Security
Cross-disciplinary R&D Themes
Data Science
Software/ICT Security

Industry-Public Sector-Academia



Vision

R&D Projects

- Blockchain-Based Cyber Security
- Early Detection of Stealthy User Behavior
- Analytics-Driven Profiling of Grid Security
- IoT Threat Analytics

Studies

- IoT Malware
- Cyberterrorism Communities
- Offensive Language Classifiers
- Modeling public response to data breaches

Training

- NSF/DoD Cybertraining
- NSA/CAE Training
- U.S. Army Reserve
- CTF/Hackathons

Impact

- R, D & T For K12/Minorities
- IoT Exploitations' Database
- Ransomware Prevention
- TTP/Patents

Basic concepts

- Blockchain-Based Cyber Security
- Early Detection of Stealthy User Behavior
- Analytics-Driven Profiling of Grid Security
- IoT Threat Analytics

Cyber attacks have hit 36 per cent of Canadian businesses

Google Warns Thousands Of Users About Potential State-Sponsored Cyber Attacks

ISIL aims to launch cyberattacks on U.S.

Chinese cyberattack hits Canada's National Research Council

Alert (ICS-ALERT-14-281-01E)
Ongoing Sophisticated Malware Campaign Compromising ICS

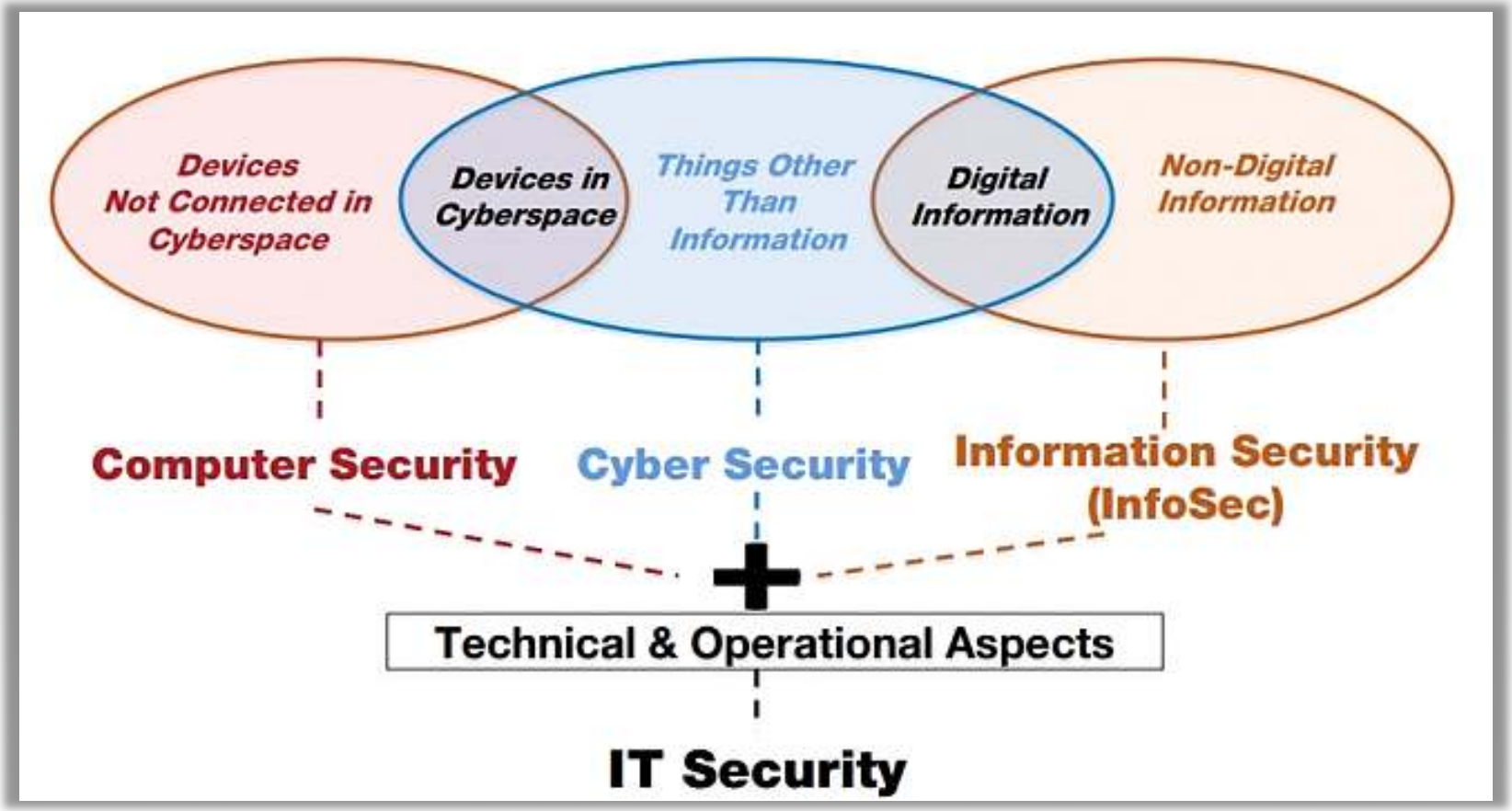
- Blockchain-Based Cyber Security
- Early Detection of [illegible] User Behavior
- [illegible] Profiling of Grid Security
- IoT Threat Analytics

Deep cyberattacks cost U.S. banks millions

MIRAI AND HAJIME LOCKED INTO IOT BOTNET BATTLE

Facebook computers compromised by zero-day Java exploit

"WannaCry" ransomware attack losses could reach $4 billion


Devices Not Connected in Cyberspace
Devices in Cyberspace
Things Other Than Information
Digital Information
Non-Digital Information
Computer Security
Cyber Security
Information Security (InfoSec)
Technical & Operational Aspects
IT Security

Computer Security:

- Protection of hosts' hardware and software against malevolent activities
- Aims to preserve various **security properties** (i.e., secrecy, availability, integrity, etc.)

Cyber Security:

- Protection of interconnected hosts on local and Internet networks against knowns and zero-day threats
- Aims at securing the **OSI layers** in a communication network

Security Properties

- Confidentiality/Secrecy
- Integrity
- Availability
- Auditability
- Non-repudiation

Confidentiality/Secrecy

- Protects against unauthorized disclosure of information.
- The trait to keep some information confidential.
- Allows the intended receiver in a communication session to know what was sent, but unintended parties cannot determine what was sent.

Integrity

- Ensuring that information will not be accidentally or maliciously altered or destroyed.
- The data is transmitted from source to destination without alteration.
- The message data can only be altered by the sender without detection.
- Integrity protects against unauthorized creation, alteration or destruction of data.

Availability

- Guarantees that the service being requested is available for legitimate users.
- Techniques and protocols to prevent illegitimate misuse of a service.

Auditability

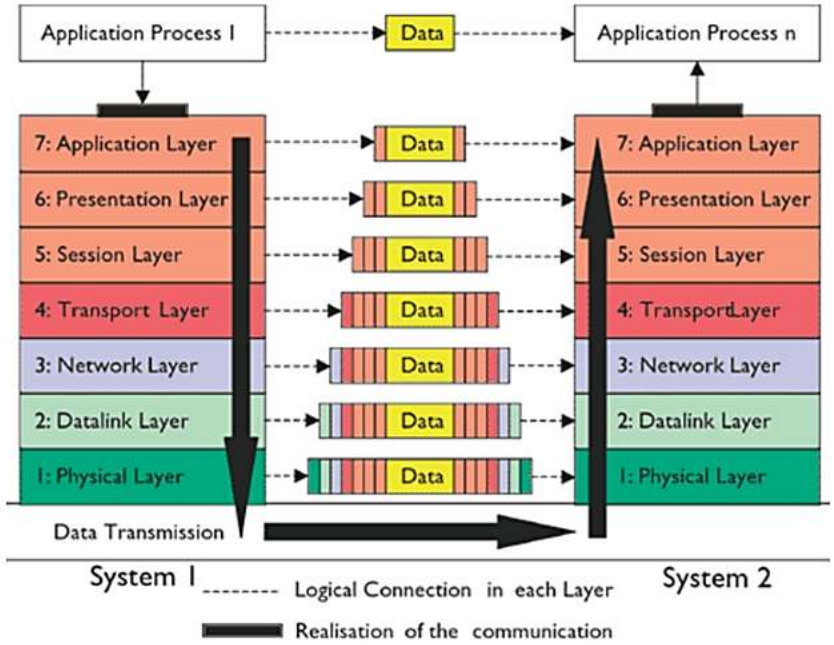
- Allows the track-back of OS, network and application activities.
- Provides methods to alert, in real-time, of any anomalous behavior.

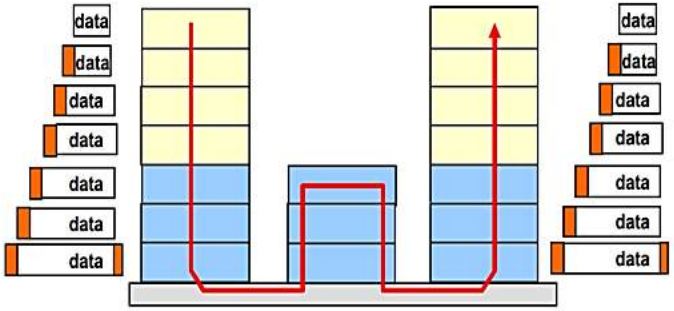
Non-repudiation

- Defined as the impossibility for one of the entities involved in a communication denying having participated in all or part of the communication.
- Provides a protection against false denial of having been involved in the communication.
- Aims to collect, maintain, make available, and validate irrefutable evidence in order to resolve disputes about the occurrence or non-occurrence of that event or action.

Open System Interconnection (ISO/OSI reference model)

All
People
Seem
To
Need
Data
Processing





ISO/OSI reference model

Application layer
- End-User Interaction
- Application layer protocols
- Name a few?

Presentation layer
- Helps map application layer protocols to lower level layers
- Provides common formats that the lower levels can understand
- Compression/Encryption of application information is accomplished

Session layer
- Establishes the concept of a session between two communicating hosts
  - Crucial for network investigation
    - Mapping of sessions
    - Measuring traffic/protocols/anomalies
- Could be considered as virtual connections between applications

ISO/OSI reference model

Transport layer

- Decision between connection-oriented and connectionless
- Various functionalities
  - Segmentation
  - Error control
  - Multiple session handling

Network layer

- Provides logical addressing to route packets
- Routing algorithms
- Buffering and queuing theories
- Encapsulated data into the notion of packets

ISO/OSI reference model

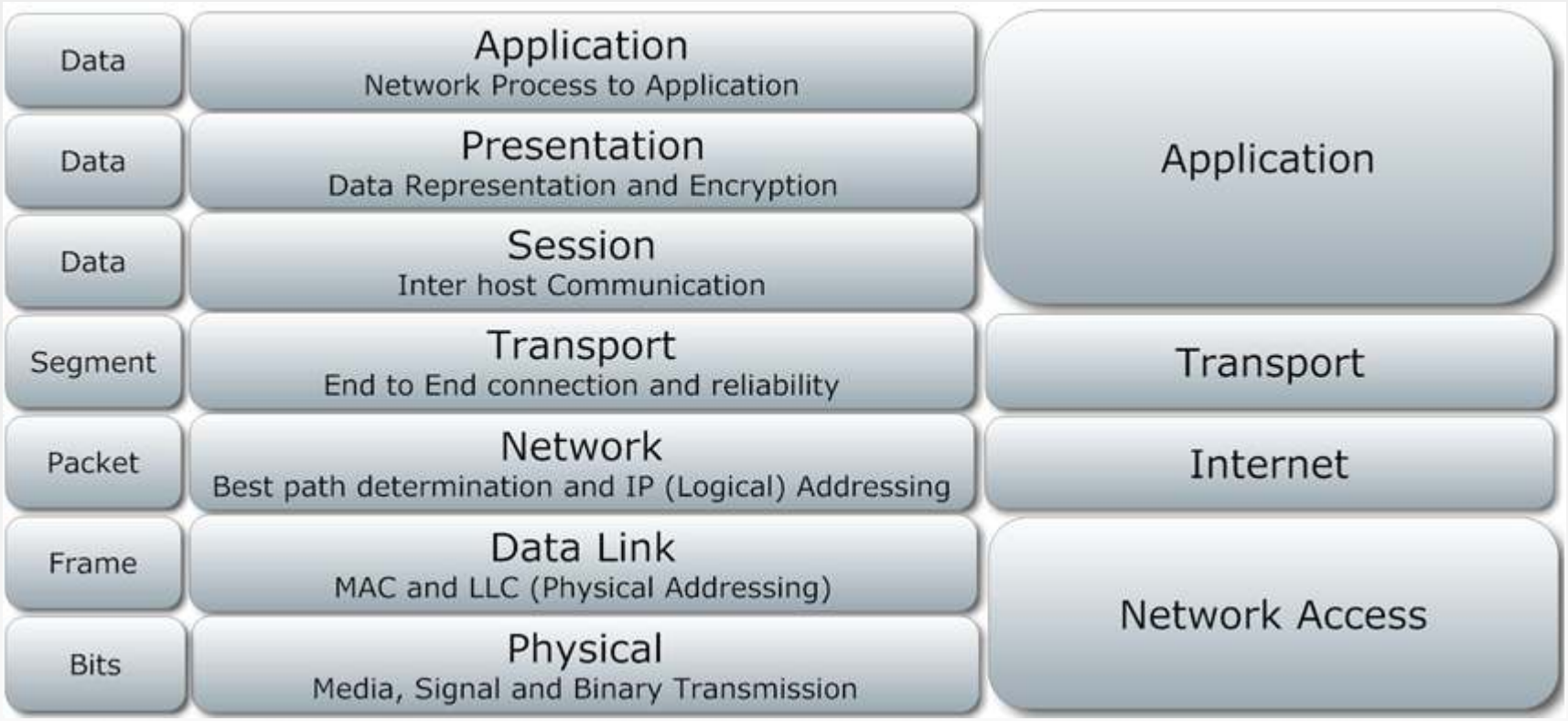
Data-link layer

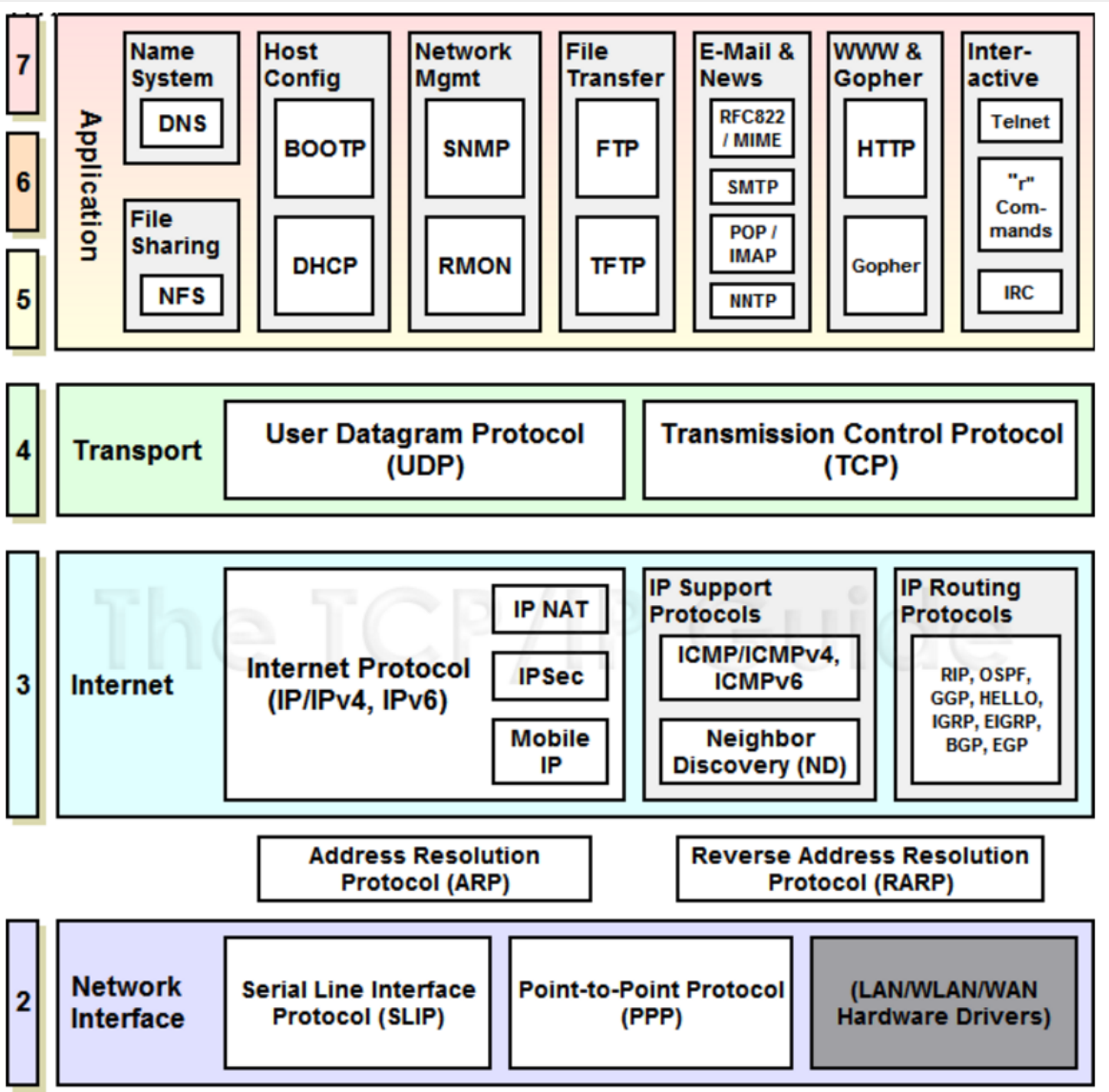
- Allows devices to access the network
- Introduces the concept of physical addresses
- Prepares data to be sent over network media
- Adapts to the physical medium

Physical layer

- Deals with putting the frame on the wire
- Establishes hardware requirements

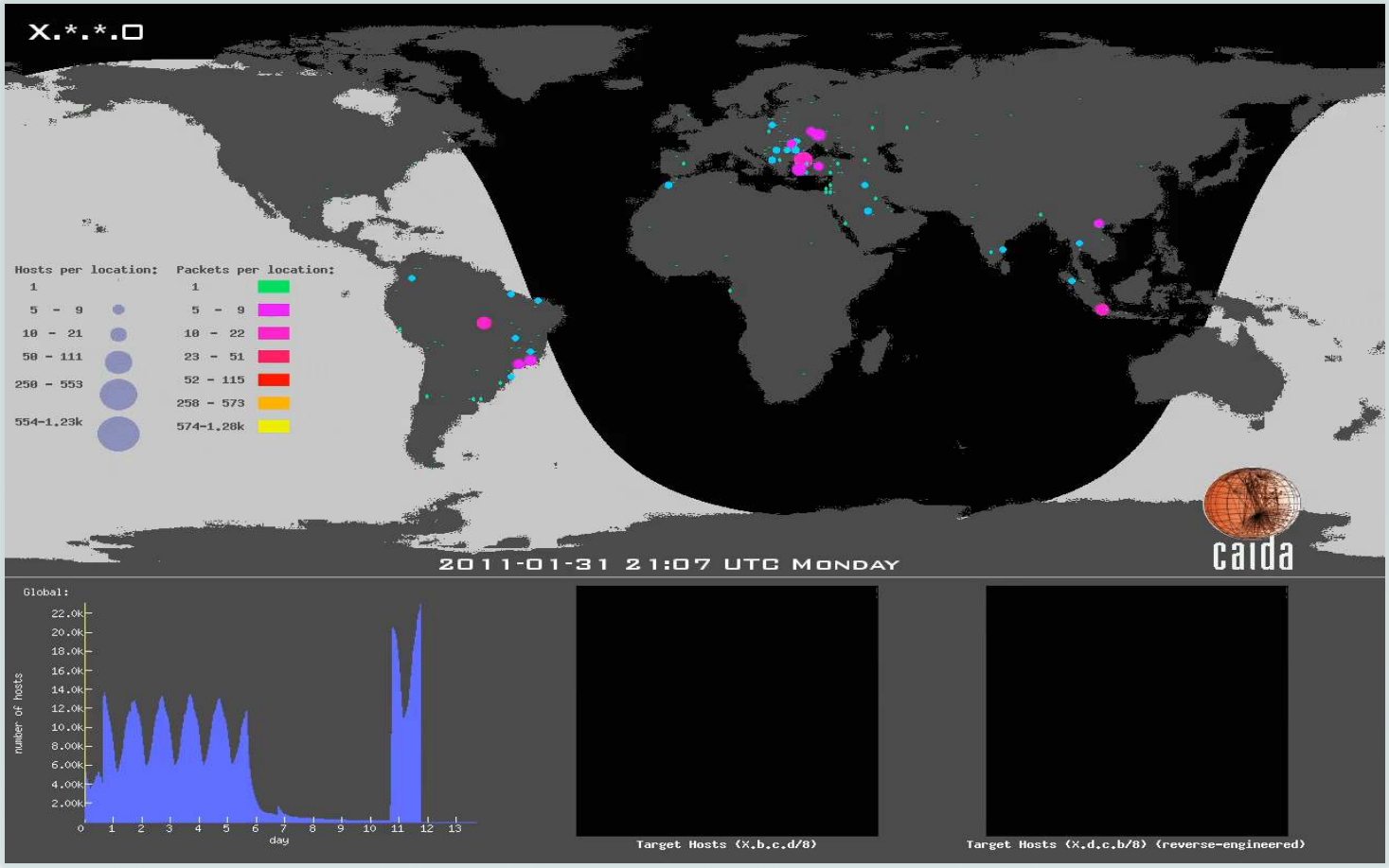
ISO/OSI reference model-Relation to TCP/IP




7
6
5
Application
Name System
DNS
File Sharing
NFS
Host Config
BOOTP
DHCP
Network Mgmt
SNMP
RMON
File Transfer
FTP
TFTP
E-Mail & News
RFC822 / MIME
SMTP
POP / IMAP
NNTP
WWW & Gopher
HTTP
Gopher
Inter-active
Telnet
"r" Com-mands
IRC
4
Transport
User Datagram Protocol (UDP)
Transmission Control Protocol (TCP)
3
Internet
Internet Protocol (IP/IPv4, IPv6)
IP NAT
IPSec
Mobile IP
IP Support Protocols
ICMP/ICMPv4, ICMPv6
Neighbor Discovery (ND)
IP Routing Protocols
RIP, OSPF, GGP, HELLO, IGRP, EIGRP, BGP, EGP
Address Resolution Protocol (ARP)
Reverse Address Resolution Protocol (RARP)
2
Network Interface
Serial Line Interface Protocol (SLIP)
Point-to-Point Protocol (PPP)
(LAN/WLAN/WAN Hardware Drivers)

Research

- Blockchain-Based Cyber Security
- Early Detection of Stealthy User Behavior
- Analytics-Driven Profiling of Grid Security
- IoT Threat Analytics



Bou-Harb, E., Assi, C. and Debbabi, M., 2016. Csc-detector: A system to infer large-scale probing campaigns. *IEEE Transactions on Dependable and Secure Computing*, *15*(3), pp.364-377.

https://tinyurl.com/yyleclnc

Fachkha, C., **Bou-Harb, E.**, Keliris, A., Memon, N.D. and Ahamad, M., 2017, February. Internet-scale Probing of CPS: Inference, Characterization and Orchestration Analysis. In *NDSS*.

https://tinyurl.com/yyslzhe5

The Insecurity of the IoT Paradigm

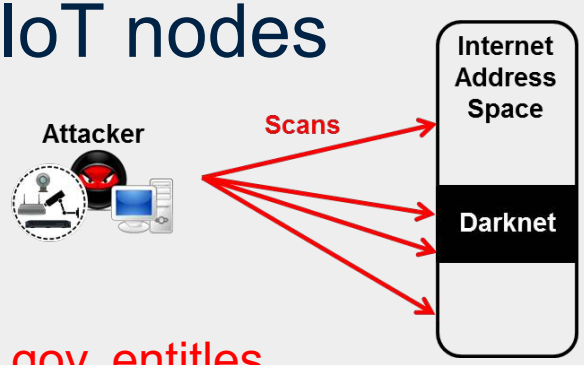
Neshenko, N., **Bou-Harb, E**., Crichigno, J., Kaddoum, G. and Ghani, N., 2019. Demystifying IoT security: an exhaustive survey on IoT vulnerabilities and a first empirical look on internet-scale IoT exploitations. *IEEE Communications Surveys & Tutorials*, *21*(3), pp.2702-2733.

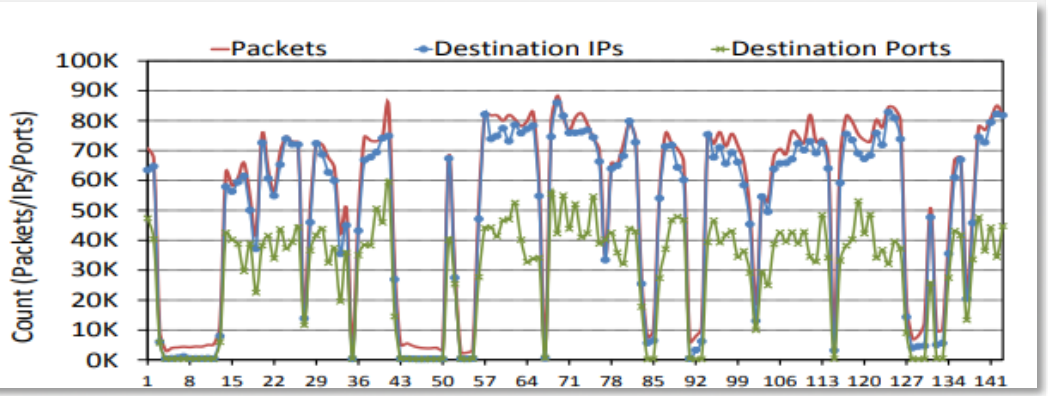
https://tinyurl.com/y2ynz8pr

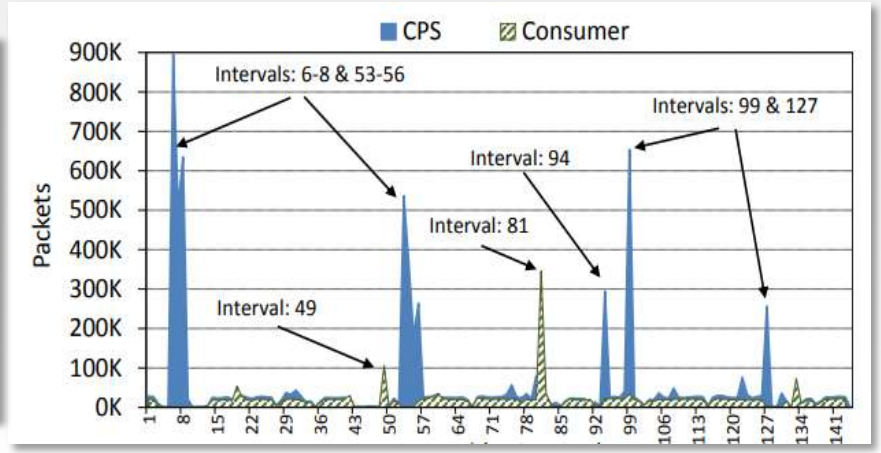
Detecting scanning from Infected IoT nodes

Malicious scans from compromised IoT devices

- 2 TB of Darknet Data (Daily)
- 840K global IoT exploitations (25K in the US)
- Exploitations in health services, manufacturing plants, gov. entitles







Cyber Security Workforce

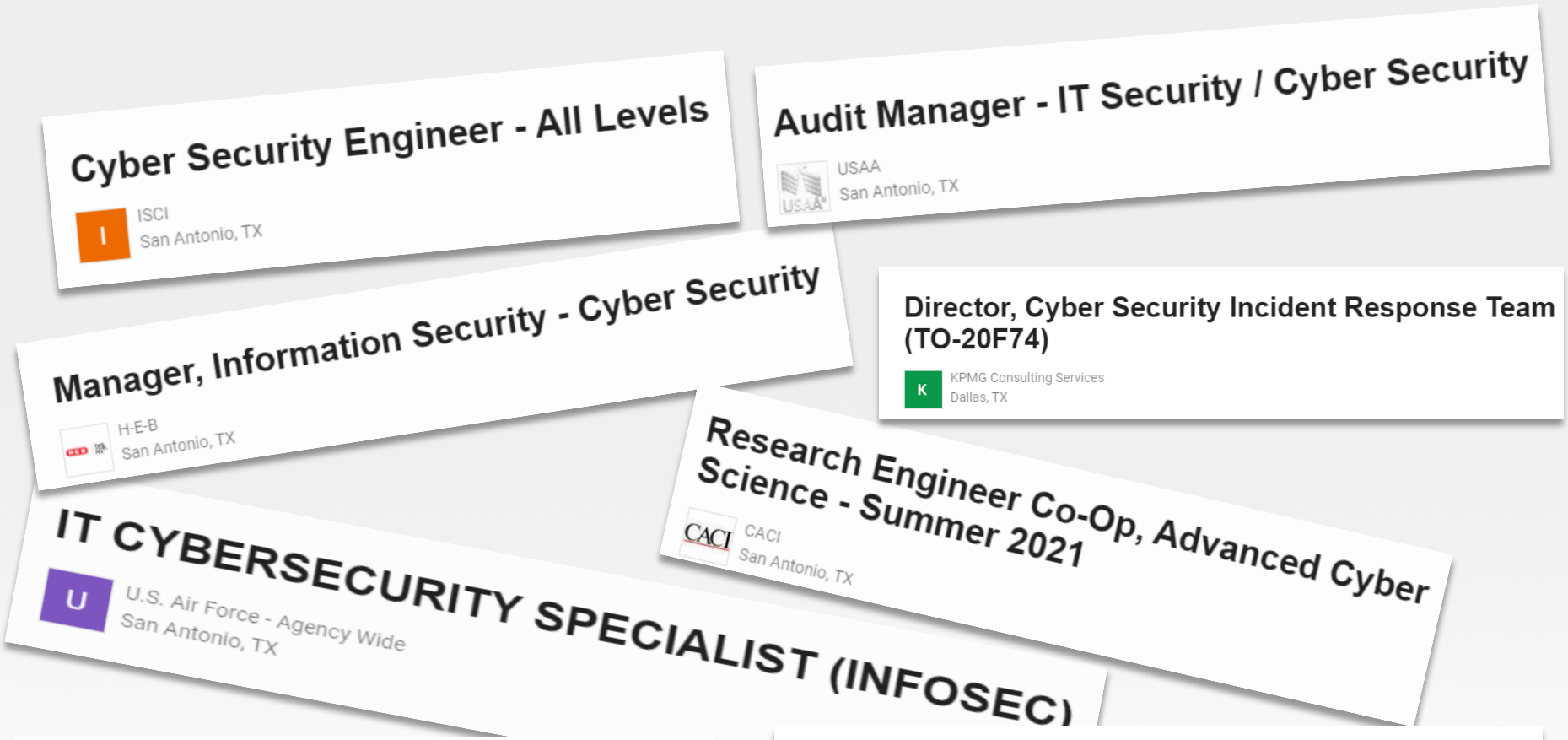
Cyber Security Workforce

- Huge skills gap; more than 75% of organizations report that they are facing a severe *crisis* when it comes to acquiring talents related *to data science*, *cyberinfrastructure*, and *cyber security*.

- In need by industry, academia and the public sector (DHS, DoD, Airforce, USSS, NSA, etc.)

- More than 300 jobs (as of Oct 5th, 2020) in San Antonio listed on google job's site
  Dell, IBM, Deloitte, USAA, EY, Siemens, USAA, Booz Allen, etc.

Cyber Security Workforce



Guest Lecture

Cyber Security: Basic concepts, Research and Workforce opportunities

Elias Bou-Harb, Ph.D., CISSP
elias.bouharb@utsa.edu