THE OHIO STATE UNIVERSITY

COLLEGE OF ENGINEERING

Fast Data Shields: Hardware for Security

Tawfiq Musah

Assistant Professor, The Ohio State University

About the Speaker

Tawfiq Musah
Assistant Professor, Department of Electrical and Computer Engineering, The Ohio State University

Research Area:	Integrated Circuit Design (Microelectronics)	
Current Position:	OSU Faculty	4 years
Industry Experience:	Intel Corporation	8 years
	Texas Instruments	1 semester
Teaching Experience:	Ohio State University	2018 – Present
	Oregon State University	2008
Hobbies:	Soccer, Movies	

Electrical and Computer Engineering

Electrical engineers and computer engineers work at the frontier of high technology and are involved in research, the creation of new ideas, the design and development of new products and technologies, manufacturing and marketing activities. Faculty members in ECE are active in the following areas:

Circuits

Signal Processing

Control / Robotics

Electromagnetics

Power/Energy

Networking / Communications

Solid State Devices

Computer Vision Image Processing

Computer Architecture

Electrical and Computer Engineering

Electrical engineers and computer engineers work at the frontier of high technology and are involved in research, the creation of new ideas, the design and development of new products and technologies, manufacturing and marketing activities. Faculty members in ECE are active in the following areas:

Circuits

Signal Processing

Control / Robotics

Electromagnetics

Power/Energy

Networking / Communications

Solid State Devices

Computer Vision Image Processing

Computer Architecture

Circuits @ OSU

Aim: Create and combine various devices to:

- Sense phenomena from our environment and convert to electrical signals

- Process these signals to extract useful information

- Send process signals back into the environment for control

Circuits @ OSU

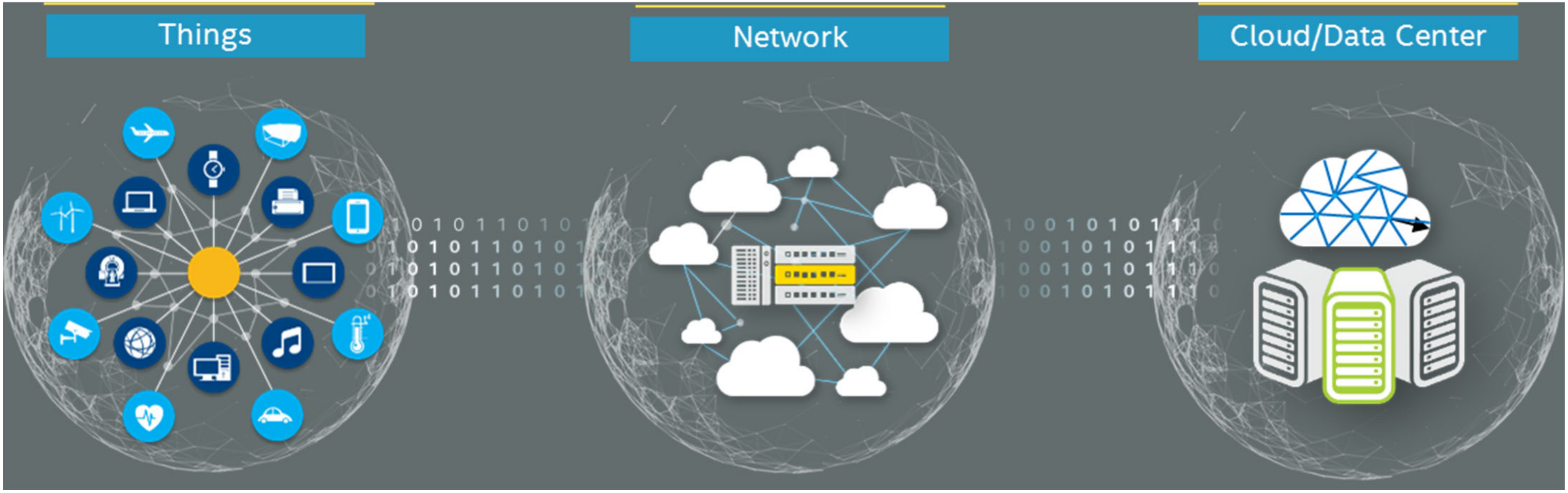
Opportunities:

- Circuit Design Engineer
  - Design at the transistor or the block level
- Product Development Engineer
  - Characterize/Debug at high volume
- Validation Engineer
  - Pre-Si/Post-Si validation: Use simulation/testing to validate chip functionality and performance and debug issues
- Hardware Design Engineer
  - PCB design and Signal Integrity
- FPGA Engineer
  - Rapid prototyping for myriad of applications

Circuits @ OSU

Employers:

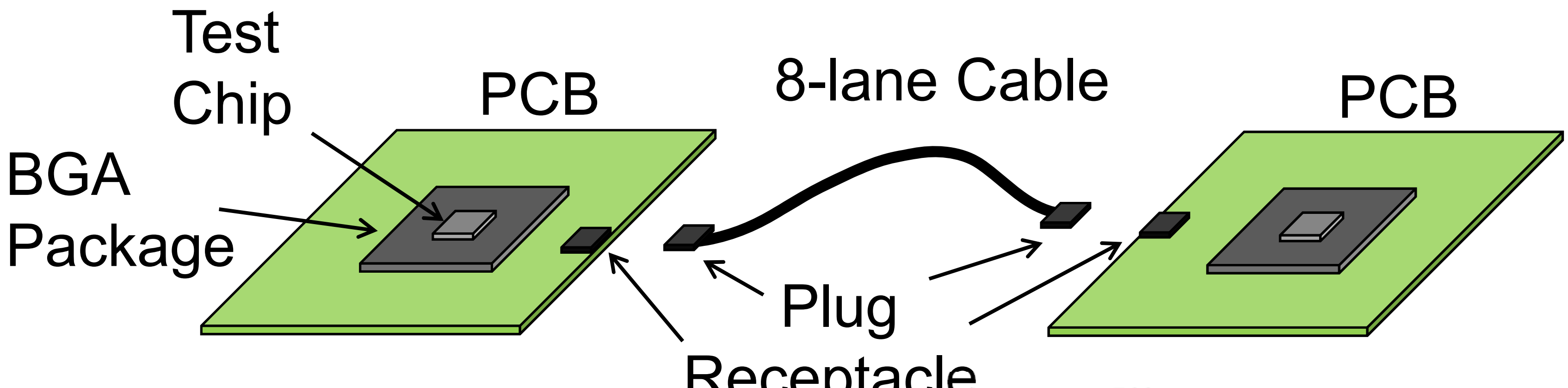
- Commercial Industries
  - Intel, Apple, TI, Qualcomm, NVIDIA, Broadcom, Silicon labs, Analog Devices, Microsoft, Amazon, Cadence, etc.
- Defense Industries
  - Raytheon, Northrop Grumman, Honeywell, Booz Allen Hamilton
- Government Labs
  - AFRL, MIT Lincoln, Brookhaven, Lawrence Livermore, Sandia
- Academia
  - Tenure track professors, research professors, lecturer, research scientist, etc
- Local: **SenseICs**

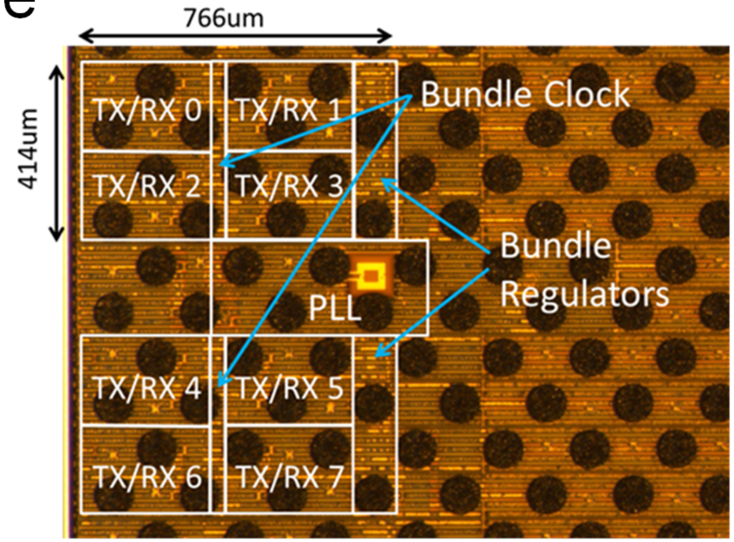


- ❖ Smart and connected devices have led to an explosion of data
- ❖ Massive data movement over conventional links have high cost
- ❖ Emerging applications call for end-to-end data security

My research focuses on hardware innovations that enable the processing and high speed transport of data in a secure and high fidelity manner.

Research Objective – High Speed Links

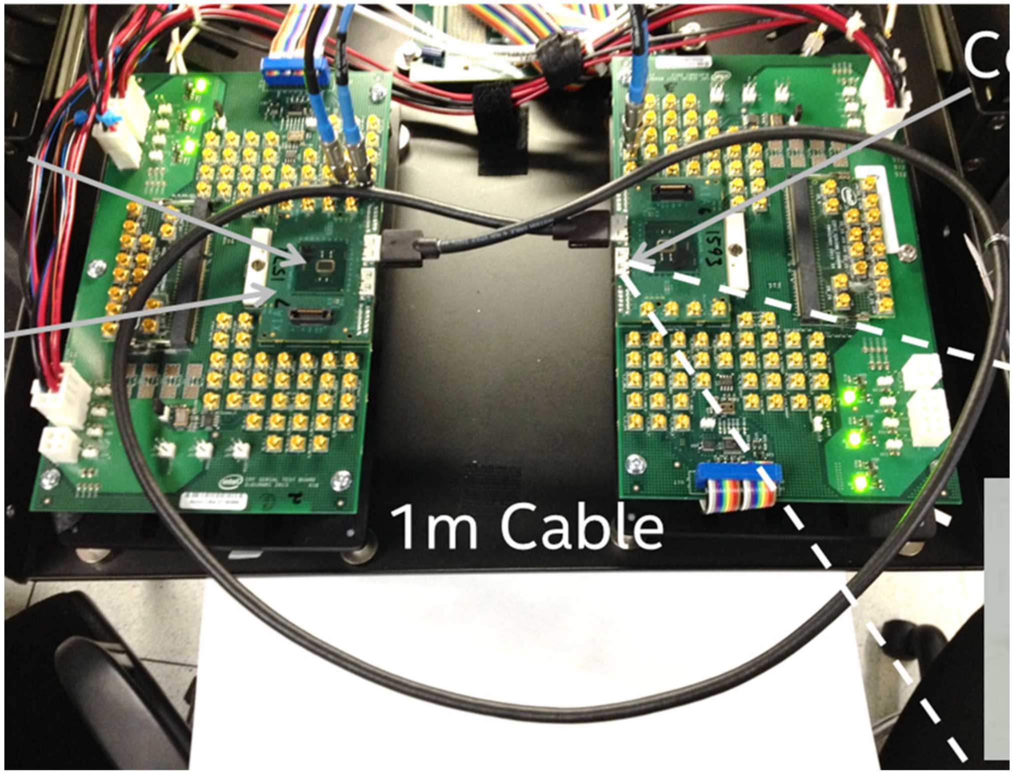




(Musah, JSSC 2014)

- Research innovative architectures to enable ultra high data rate comms.
- Use unique artefacts of the link to ensure data security
- Study new computing architectures for high efficiency signal processing

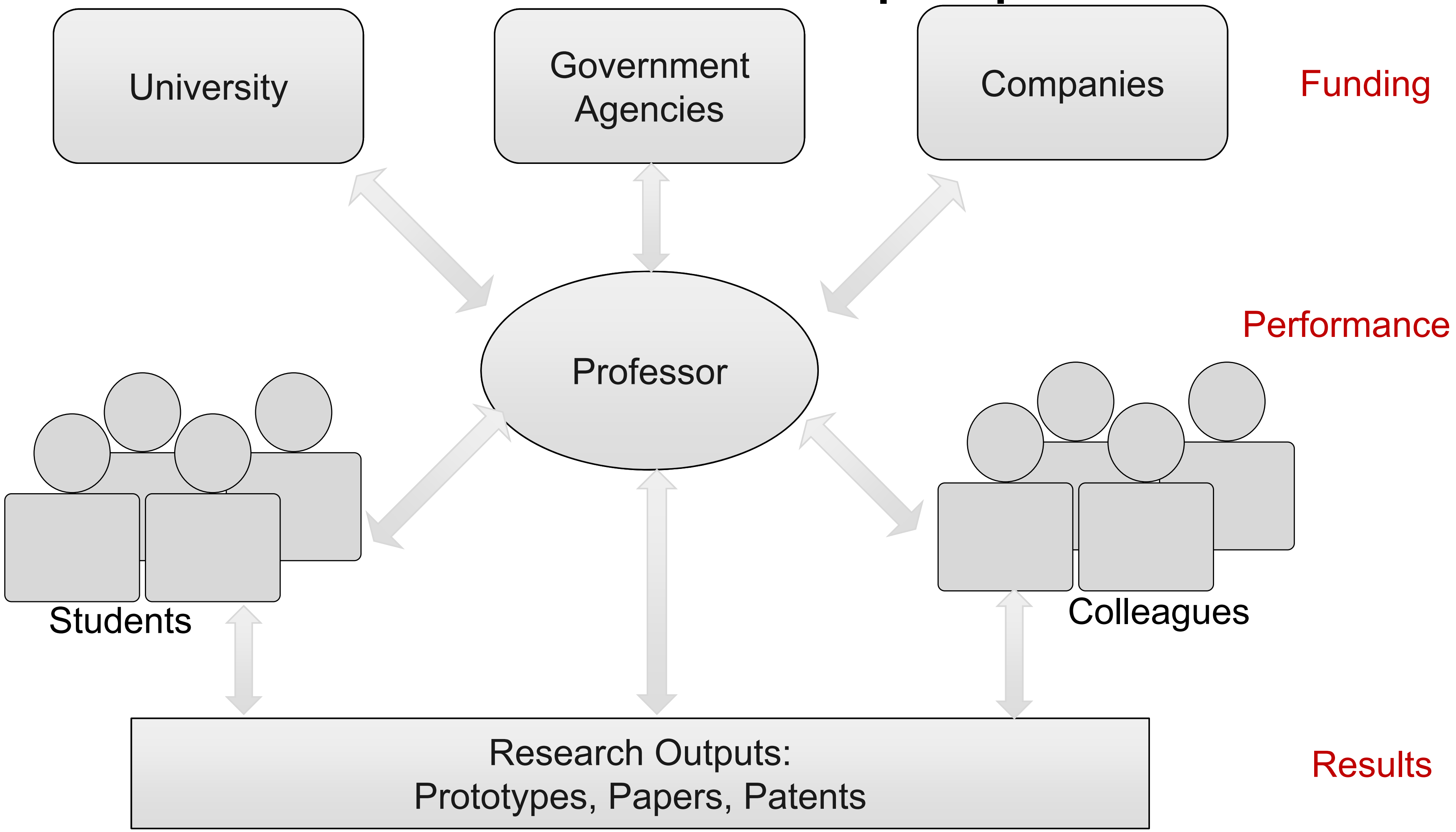
Research Objective – High Speed Links



- ❖ In 2014, demonstrated 32Gbps/lane over cable
- ❖ In comparison, USB today has 10Gbps/lane
- ❖ We are now working on 100Gbps/lane links
- ❖ Revolutionary display

- ❖ Electrical and Computer Engineering for design/test
- ❖ Mechanical Engineering for connector/thermal design
- ❖ Material Science for cable/channel/new devices design
- ❖ Computer Science for software/firmware and EDA tools

Research as a Startup Operation



Security Fundamentals

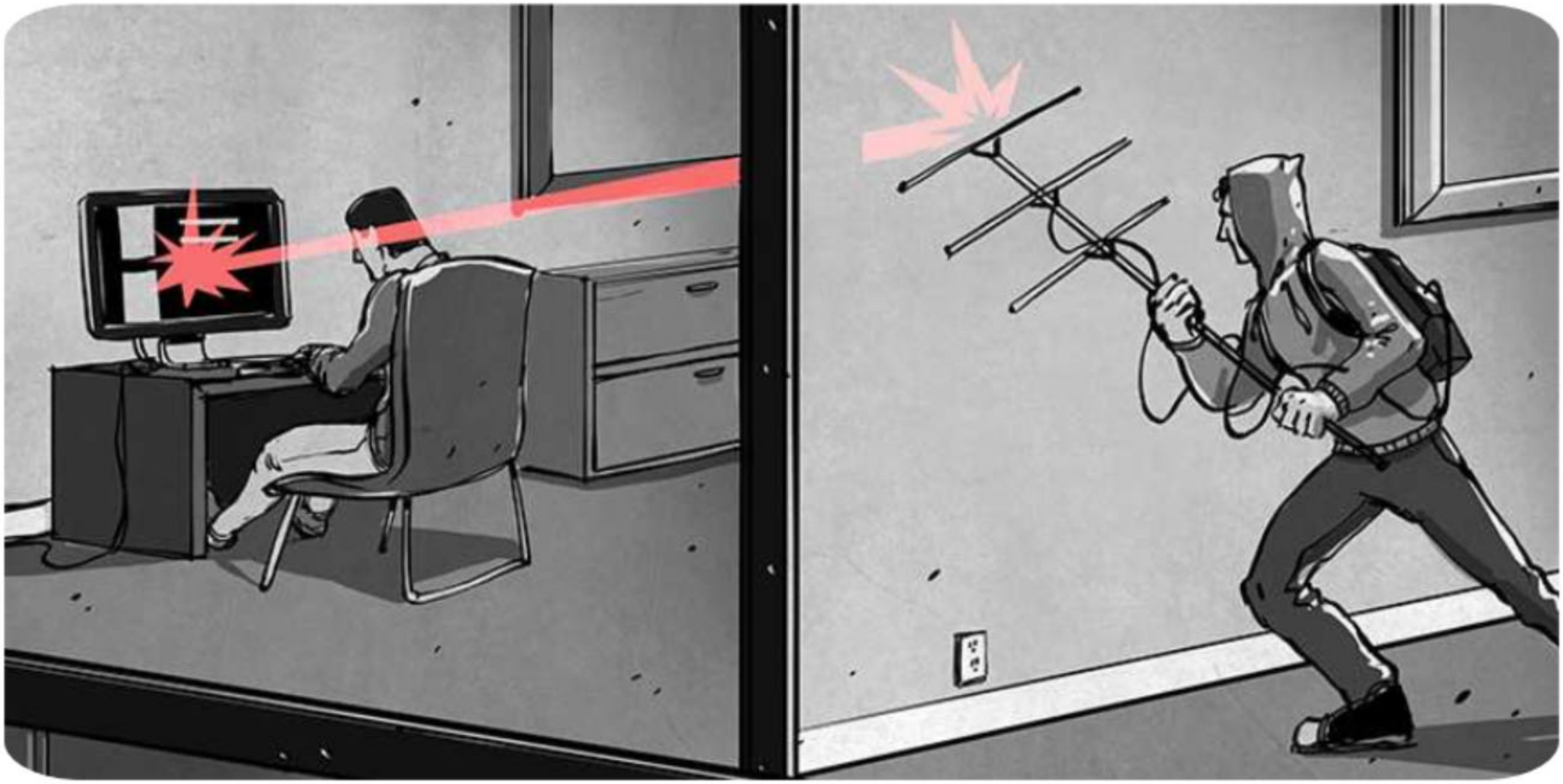


Image from [1]

❖ Information security has become one of the most important aspect of our daily lives.

Security Fundamentals

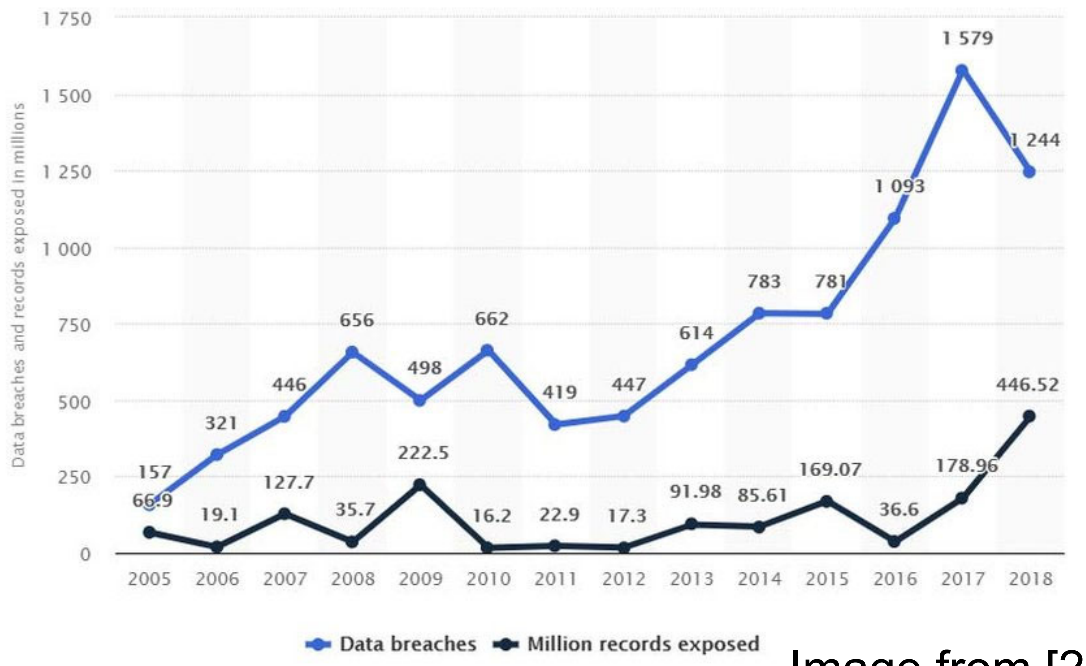
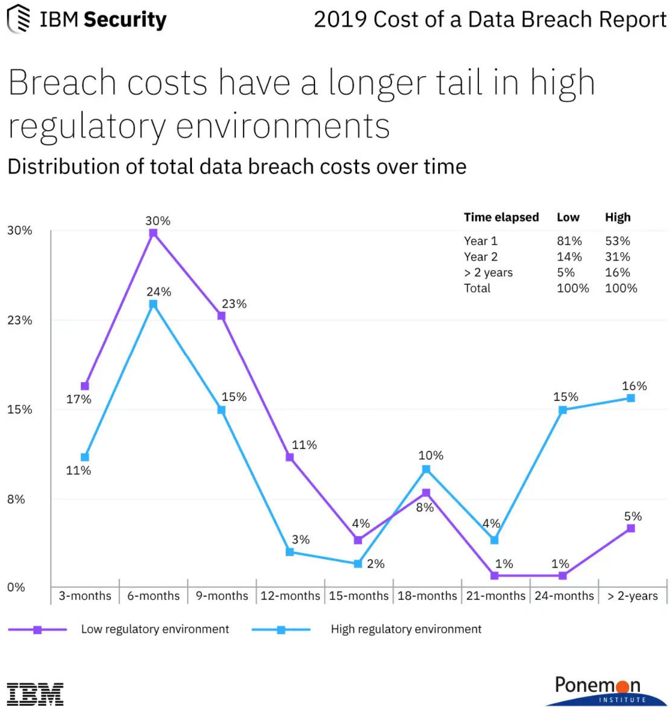


Image from [2]


IBM Security 2019 Cost of a Data Breach Report

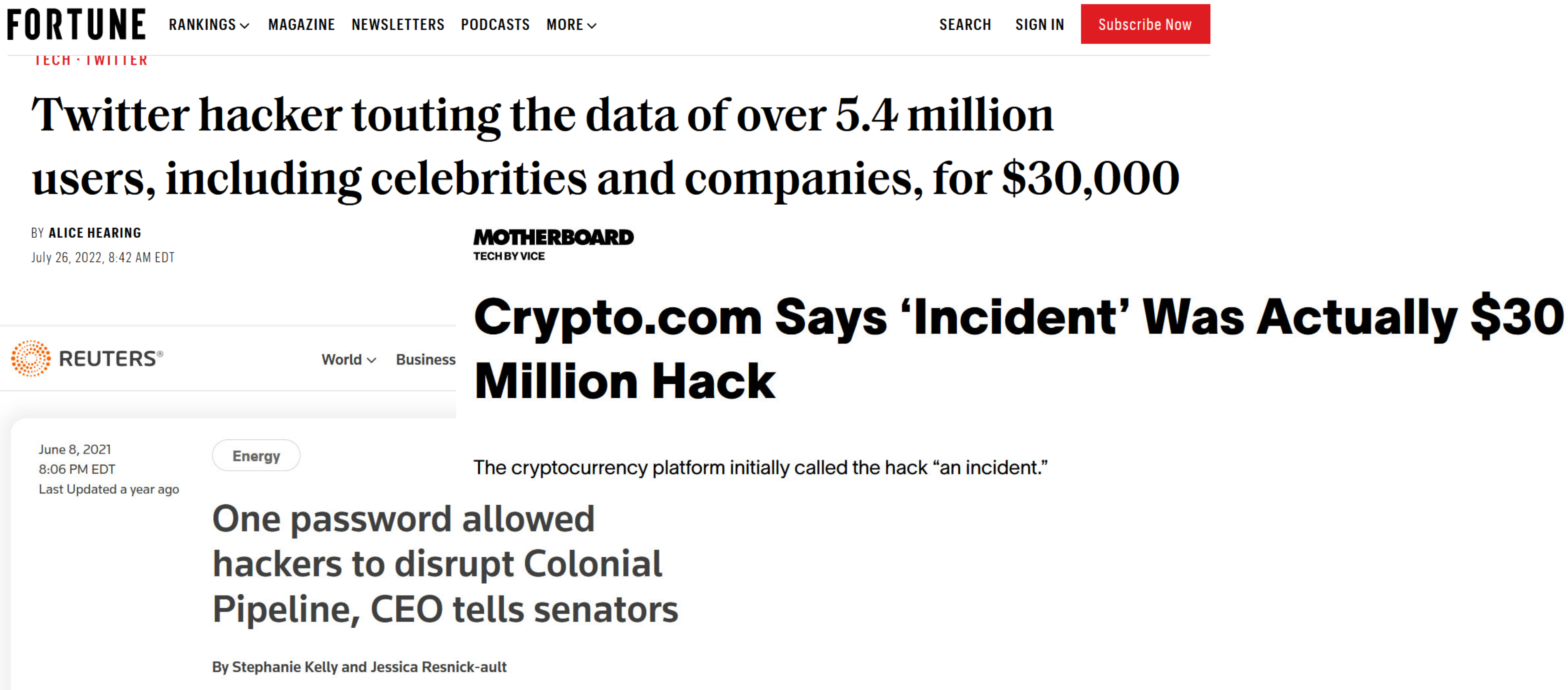
Breach costs have a longer tail in high regulatory environments

Distribution of total data breach costs over time

Time elapsed	Low	High
Year 1	81%	53%
Year 2	14%	31%
> 2 years	5%	16%
Total	100%	100%

❖ Information security has become one of the most important aspect of our daily lives.

Security Fundamentals



TECH · TWITTER

Twitter hacker touting the data of over 5.4 million users, including celebrities and companies, for $30,000

BY ALICE HEARING
July 26, 2022, 8:42 AM EDT

Crypto.com Says 'Incident' Was Actually $30 Million Hack

The cryptocurrency platform initially called the hack "an incident."

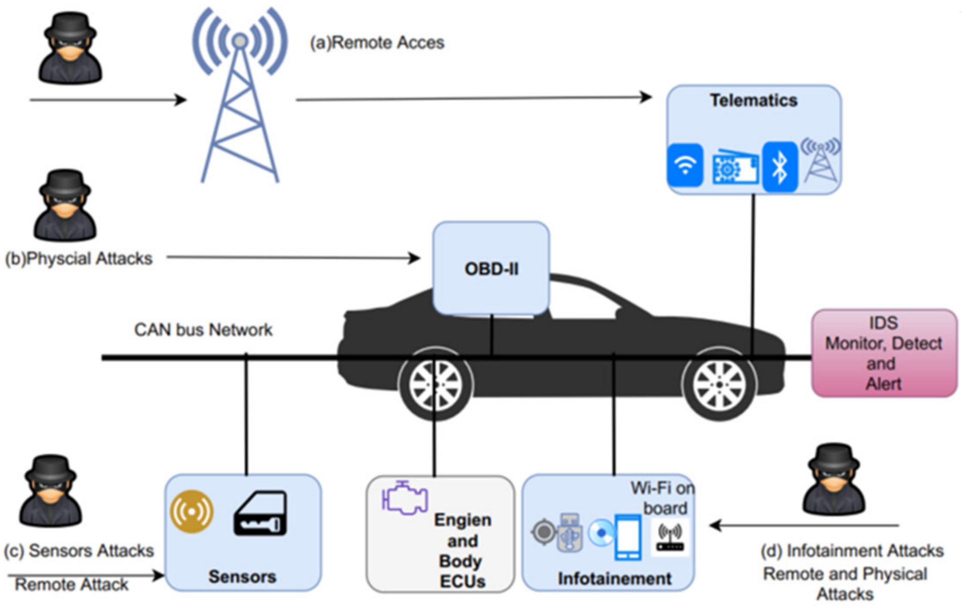
June 8, 2021
8:06 PM EDT
Last Updated a year ago

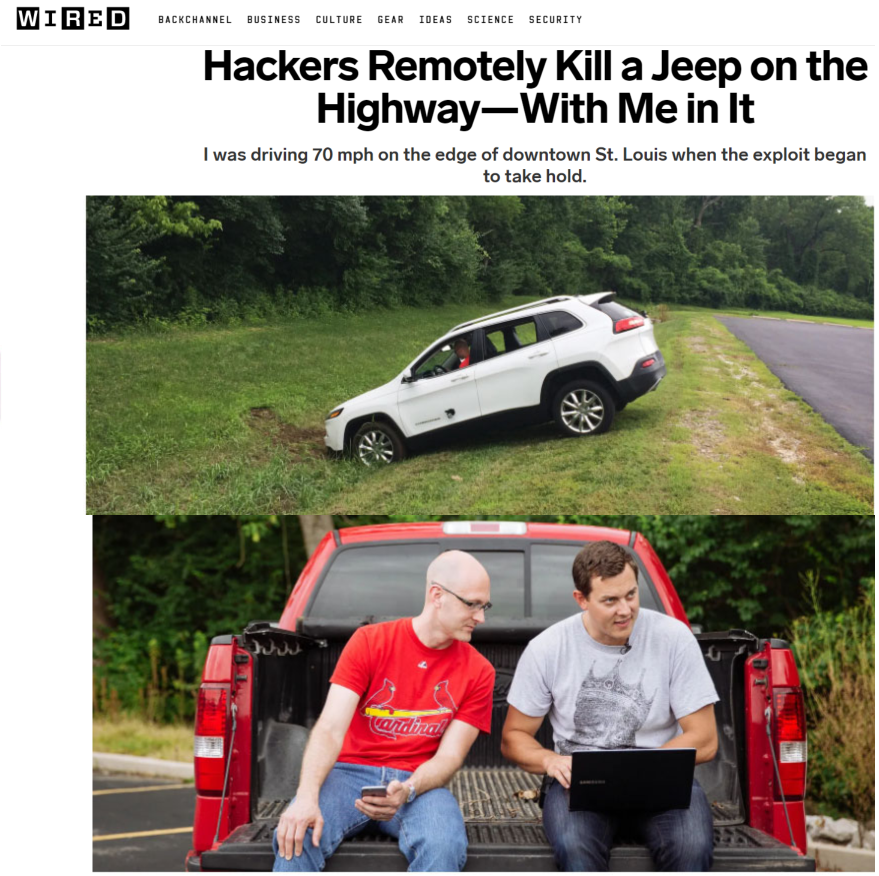
One password allowed hackers to disrupt Colonial Pipeline, CEO tells senators

By Stephanie Kelly and Jessica Resnick-ault

- ❖ Information security has become one of the most important aspect of our daily lives.
- ❖ It has impacts on both our real and digital (virtual) worlds.

Automotive Examples





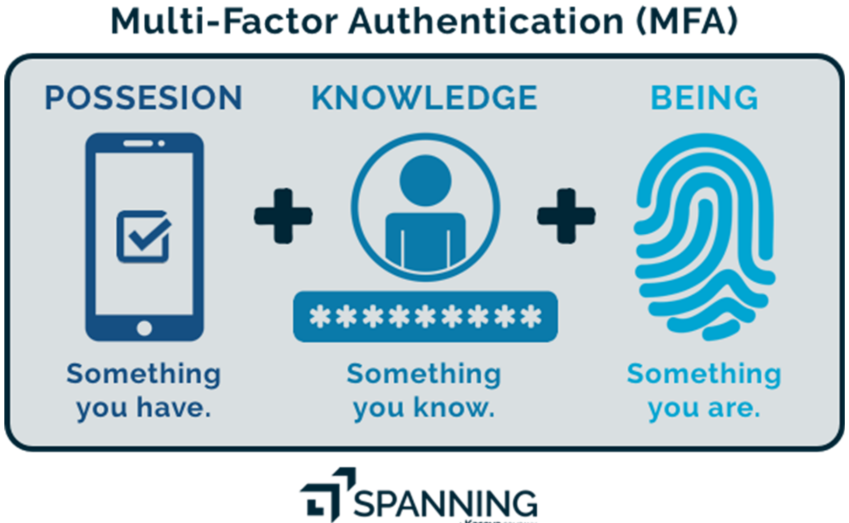
Hackers Remotely Kill a Jeep on the Highway—With Me in It

I was driving 70 mph on the edge of downtown St. Louis when the exploit began to take hold.

- ❖ Automotive networks, with the numerous ECUs needed for ADAS and autonomous driving provide a wide attack surface
- ❖ The health/safety implications of breaches can't be overstated

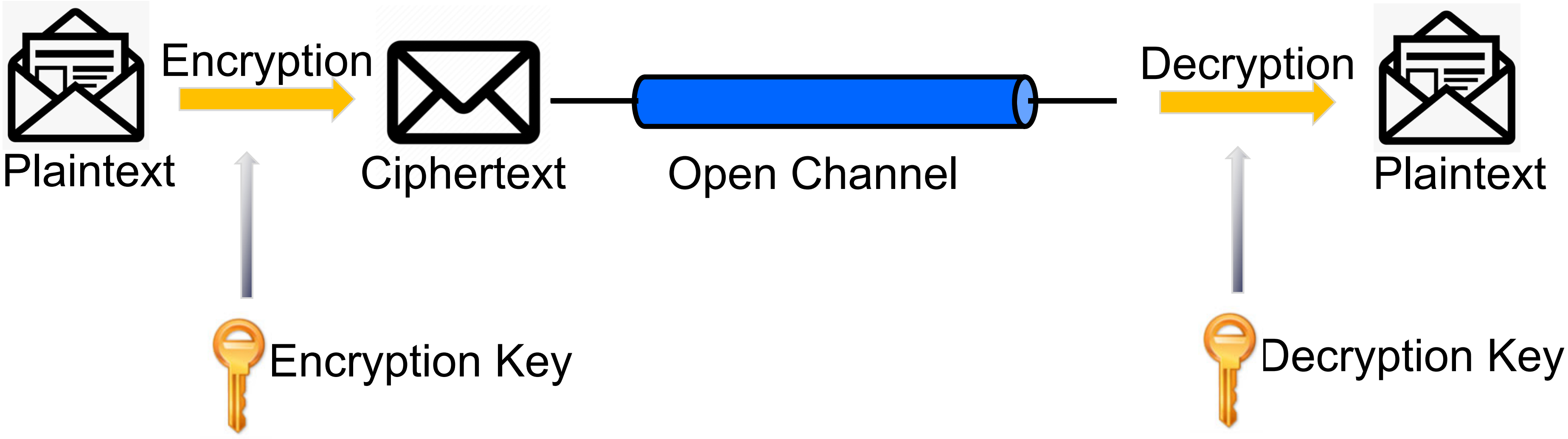
Security Fundamentals

iproov
What Is the Best Authentication Method? 5 Types of Authentication
SMS
SMS/Email codes
Voice
Passwords
Fingerprint
Face Verification



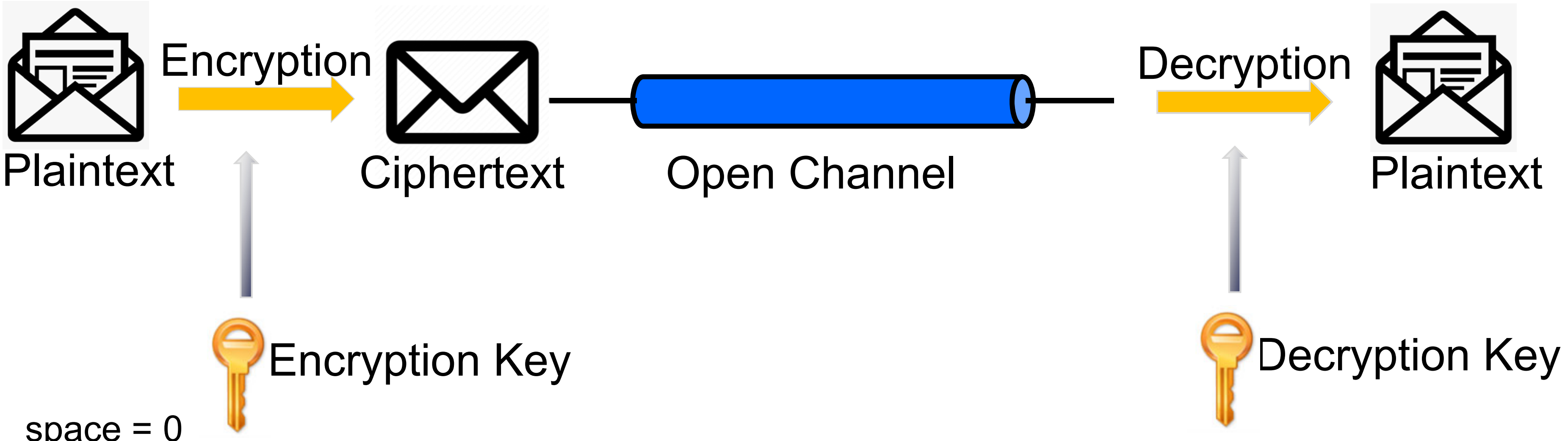
- ❖ Authentication can be used to restrict access to legitimate users
  - ❖ Type of authentication approaches include:
  - ❖ Personal Identification Number (PIN)
  - ❖ Passwords
  - ❖ Smartcards
  - ❖ Biometrics (fingerprint, face, iris, etc)
- ❖ Ultimately, encryption is required to ensure the data is only accessible to only legitimate receivers

Cryptography



- ❖ Cryptography ensures information secrecy by encrypting message before transmission on public channels
- ❖ The legitimate target receiver needs information about the key used for encryption to decrypt the message
- ❖ Various encryption/decryption mechanisms exist with varying degrees of secrecy and complexity

Cryptography - Examples



Encryption

Plaintext

Ciphertext

Open Channel

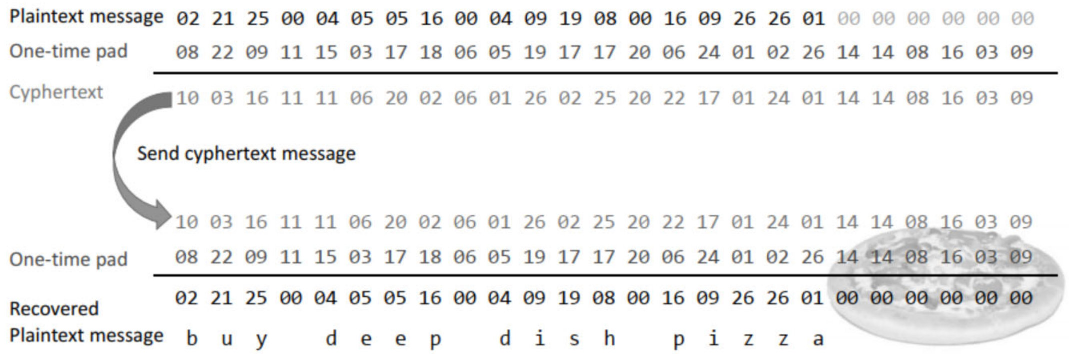
Decryption

Plaintext

Encryption Key

Decryption Key

space = 0
a = 1
b = 2
c = 3
.
.
z = 26

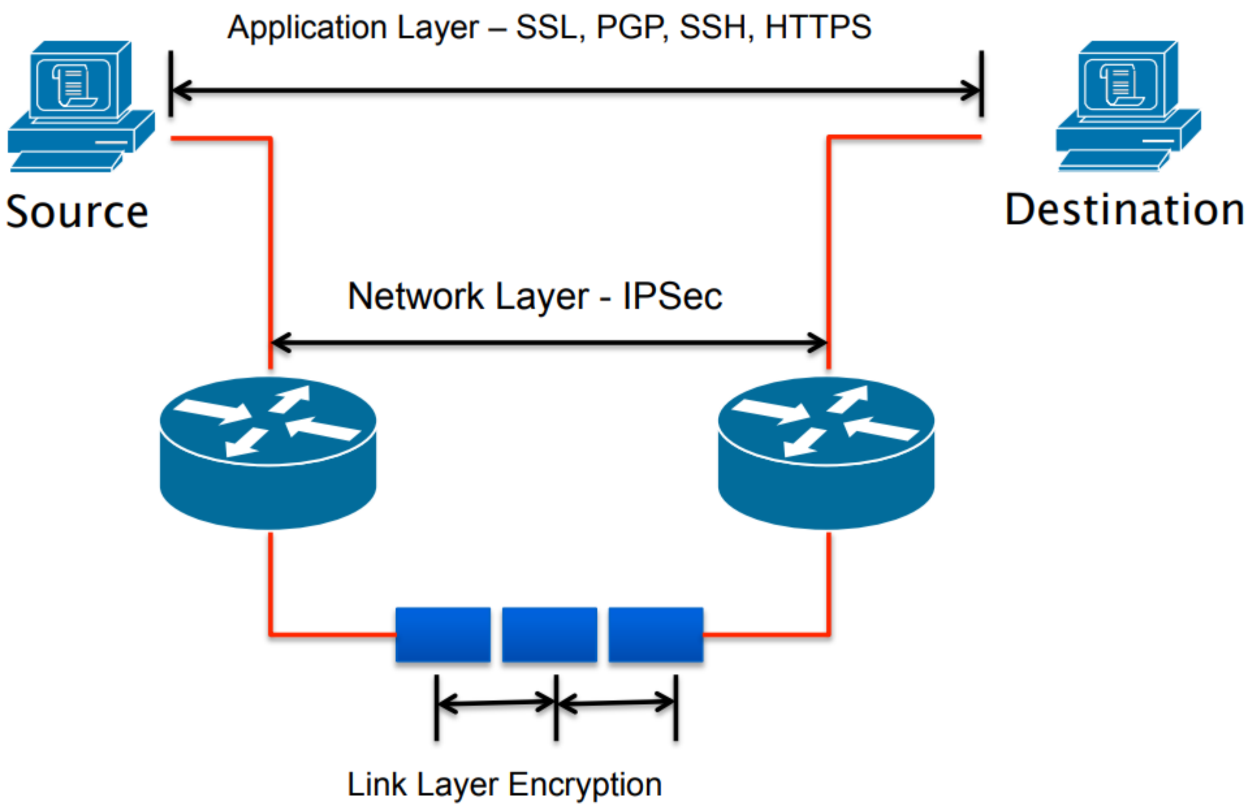


Plaintext message	02	21	25	00	04	05	05	16	00	04	09	19	08	00	16	09	26	26	01	00	00	00	00	00	00
One-time pad	08	22	09	11	15	03	17	18	06	05	19	17	17	20	06	24	01	02	26	14	14	08	16	03	09
Cyphertext	10	03	16	11	11	06	20	02	06	01	26	02	25	20	22	17	01	24	01	14	14	08	16	03	09
Send cyphertext message																									
	10	03	16	11	11	06	20	02	06	01	26	02	25	20	22	17	01	24	01	14	14	08	16	03	09
One-time pad	08	22	09	11	15	03	17	18	06	05	19	17	17	20	06	24	01	02	26	14	14	08	16	03	09
Recovered	02	21	25	00	04	05	05	16	00	04	09	19	08	00	16	09	26	26	01	00	00	00	00	00	00
Plaintext message	b	u	y		d	e	e	p		d	i	s	h		p	i	z	z	a						

- ❖ Cryptography approaches include the use of Vernam cipher, data encryption standard (DES), advanced encryption standard (AES), RSA (Rivest-Shamir-Adleman)

Security Fundamentals

- Application
- Presentation
- Session
- Transport
- Network
- Data Link
- Physical (PHY)



Application Layer – SSL, PGP, SSH, HTTPS

Source

Destination

Network Layer - IPSec

Link Layer Encryption

❖ Security is implemented at different layers of the software stack

❖ Key distribution and encryption/decryption computation are major design and implementation concerns

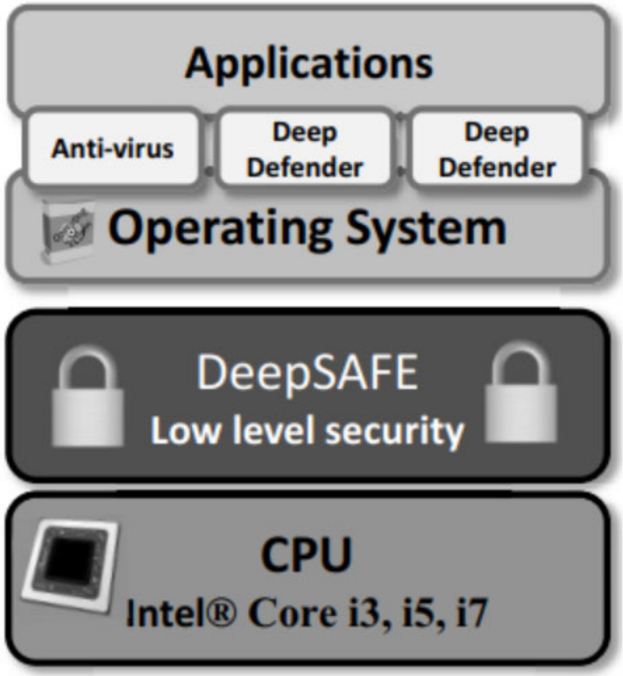
Activity – Cipher

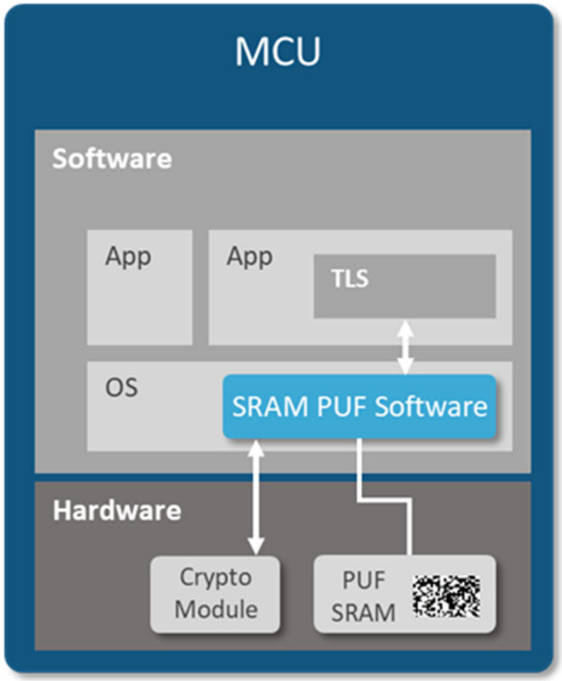
- Can you decode the following text?

FOHJOFFST IBWF UIF NPTU GVO

The Role of Hardware

Image from [3]





- ❖ Hardware resources can be used to aid security in two main ways
    - ❖ Cryptographic algorithm acceleration
    - ❖ PHY layer noise and signatures for authentication and secrecy

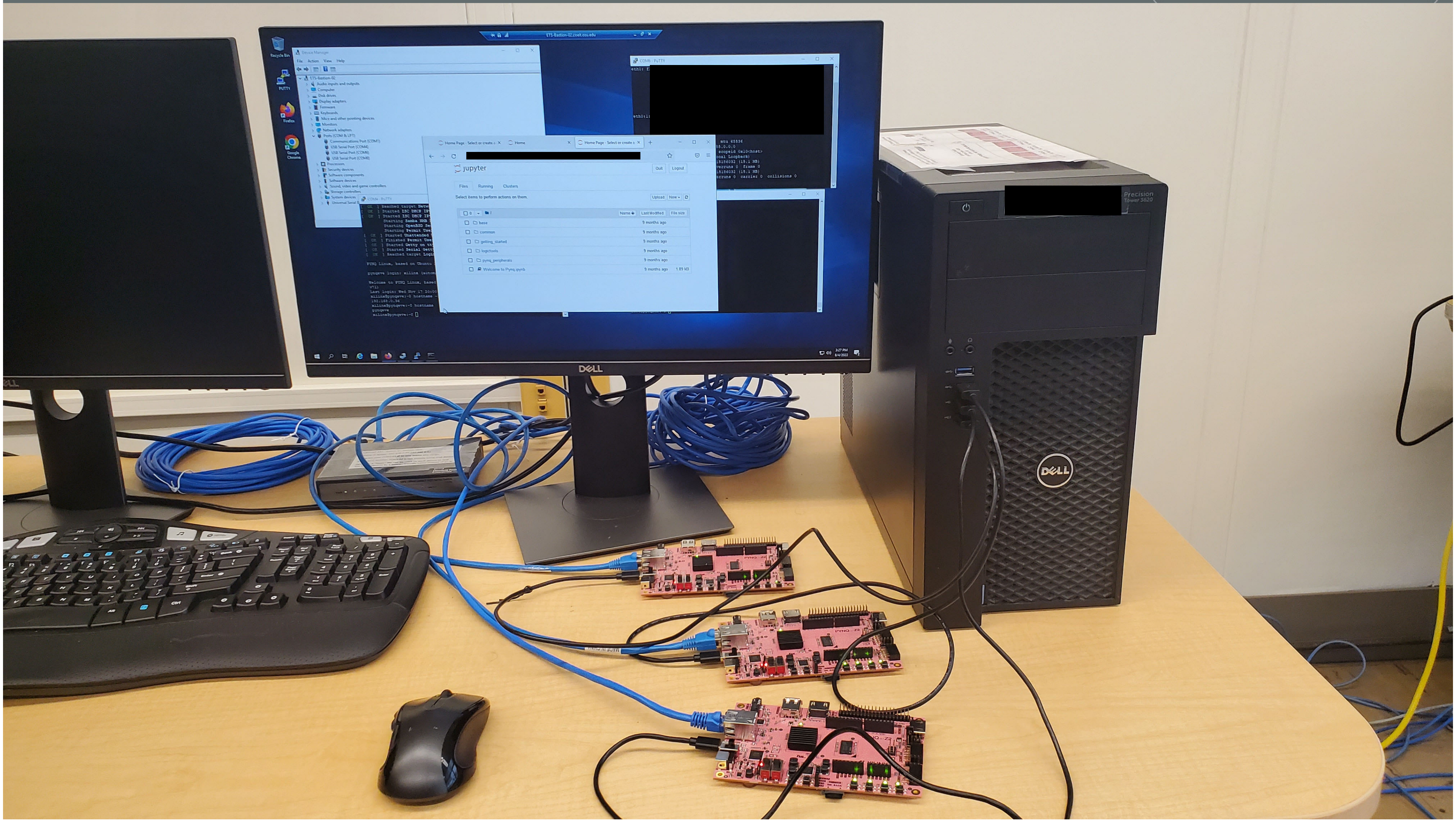
Class Agenda

Week 1

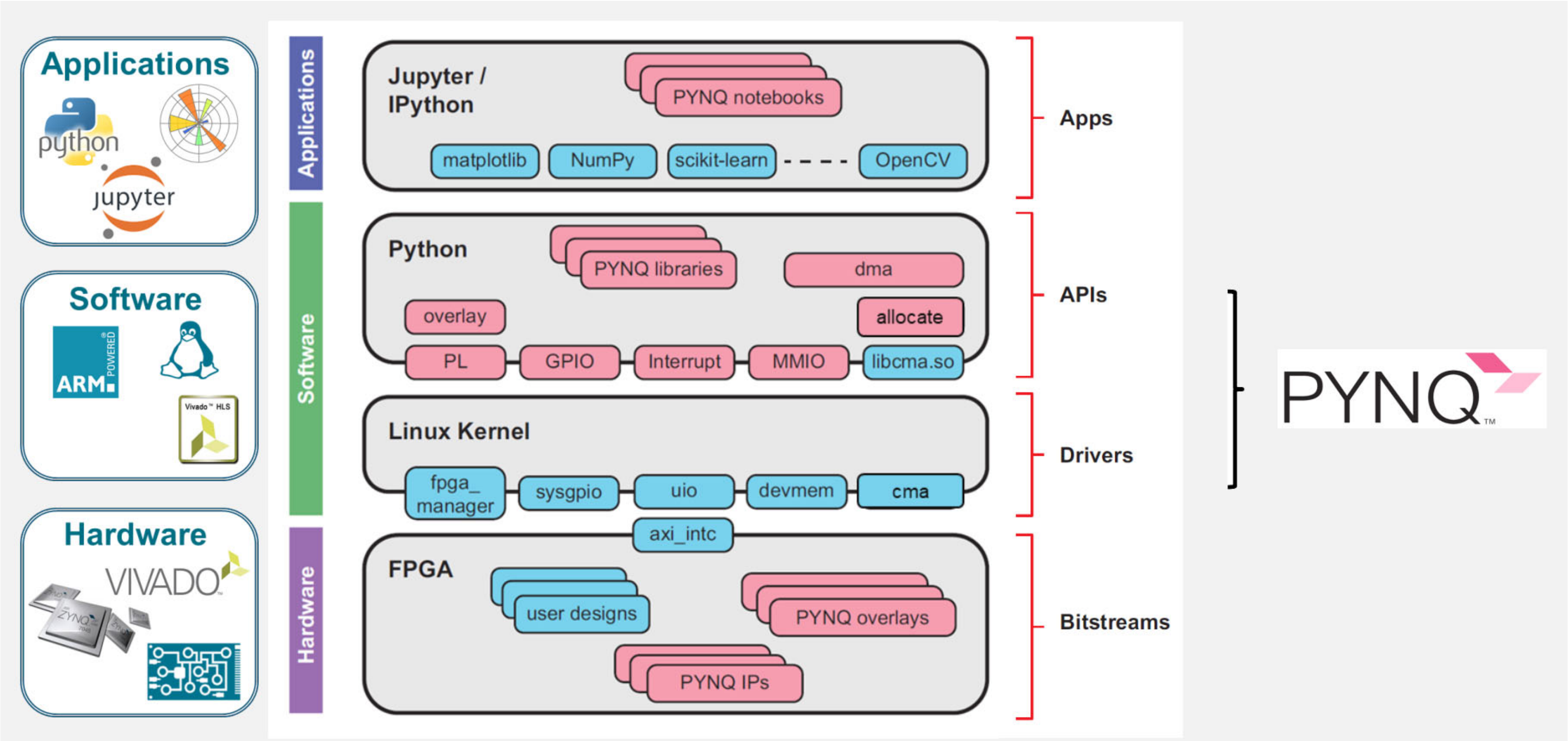
- Day 1: Introduction to hardware security
- Day 2: The PYNQ-Z2 board and Jupyter design environment
- Day 3: Getting started with Notebooks
- Day 4: Design examples software/hardware
- Day 5: Design examples software/hardware

Week 2

- Day 1: Group project work
- Day 2: Group project work
- Day 3: Group project work
- Day 4: Presentation prep work
- Day 5: Presentation

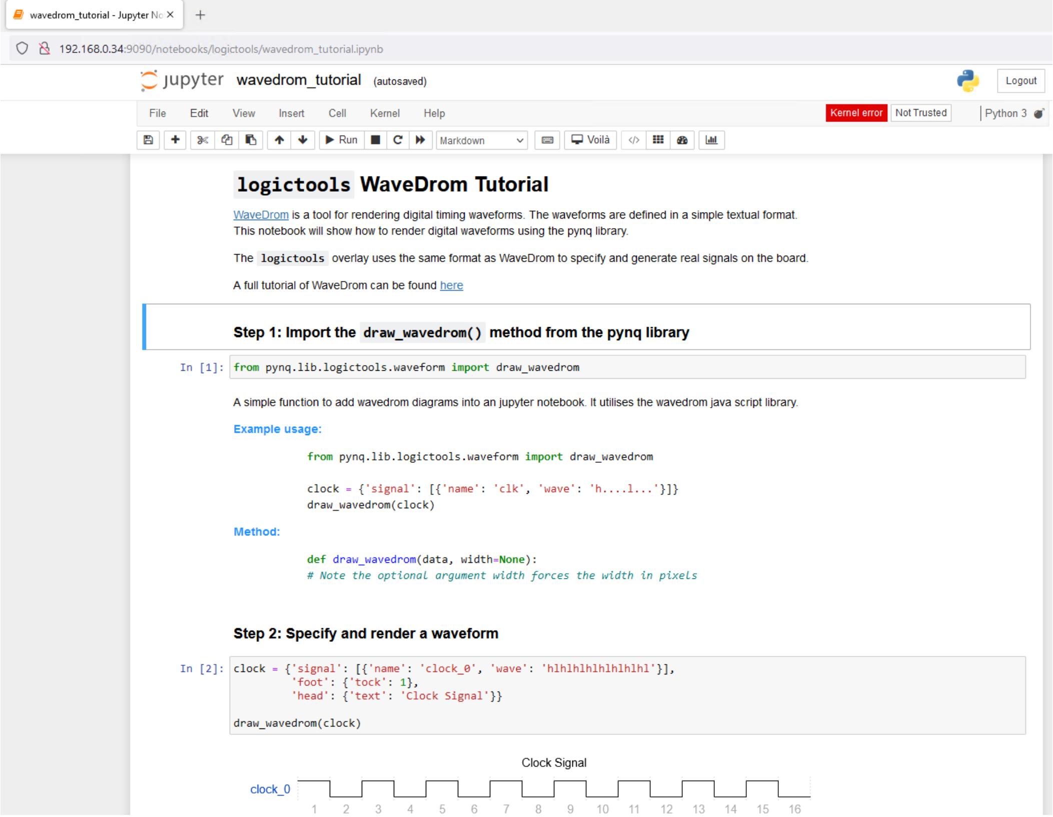


❖ Our hardware devices (PYNQ-Z2 boards) are isolated from the public network.



Learn more at the PYNQ Tutorial.

Jupyter Notebooks


wavedrom_tutorial - Jupyter No
192.168.0.34:9090/notebooks/logictools/wavedrom_tutorial.ipynb
jupyter
wavedrom_tutorial (autosaved)
Logout
File
Edit
View
Insert
Cell
Kernel
Help
Kernel error
Not Trusted
Python 3
Run
Markdown
Voilà

logictools WaveDrom Tutorial

WaveDrom is a tool for rendering digital timing waveforms. The waveforms are defined in a simple textual format.
This notebook will show how to render digital waveforms using the pynq library.

The `logictools` overlay uses the same format as WaveDrom to specify and generate real signals on the board.

A full tutorial of WaveDrom can be found here

Step 1: Import the `draw_wavedrom()` method from the pynq library

```
In [1]: from pynq.lib.logictools.waveform import draw_wavedrom
```

A simple function to add wavedrom diagrams into an jupyter notebook. It utilises the wavedrom java script library.

Example usage:

```
        from pynq.lib.logictools.waveform import draw_wavedrom

        clock = {'signal': [{'name': 'clk', 'wave': 'h....l...'}]}
        draw_wavedrom(clock)
```

Method:

```
        def draw_wavedrom(data, width=None):
        # Note the optional argument width forces the width in pixels
```

Step 2: Specify and render a waveform

```
In [2]: clock = {'signal': [{'name': 'clock_0', 'wave': 'hlhlhlhlhlhlhlhl'}],
                 'foot': {'tock': 1},
                 'head': {'text': 'Clock Signal'}}

        draw_wavedrom(clock)
```

Learn more at the Jupyter Notebooks.

- ❖ This shows and example of redering digital timing waveforms using Jupyter

Group Project

- I am grouping you into three teams
- Each team should develop 3 notebooks
  - Image Transmitter with encryption
  - Image Receiver with decryption information
  - Eavesdropper notebook that tries to guess encryption key
- We will work on your notebooks Monday, Tuesday, some of Wednesday
- On Wednesday, we will test the performance of each notebook by groups playing one of the three roles with members of the other groups

Q & A

References

[1] (Image Source) E. Williams, "TEMPEST: a Tin Foil Hat for Your Electronics and Their Secrets", October 2015
[2] Trabelsi, Slim. (2019). Monitoring Leaked Confidential Data. 1-5. 10.1109/NTMS.2019.8763811.
[3] Chan, Philip & Barnett, Thomas & Badawy, Abdel-Hameed & Patrick, Jungwirth. (2018). Cyber defense through hardware security. 22. 10.1117/12.2302805.