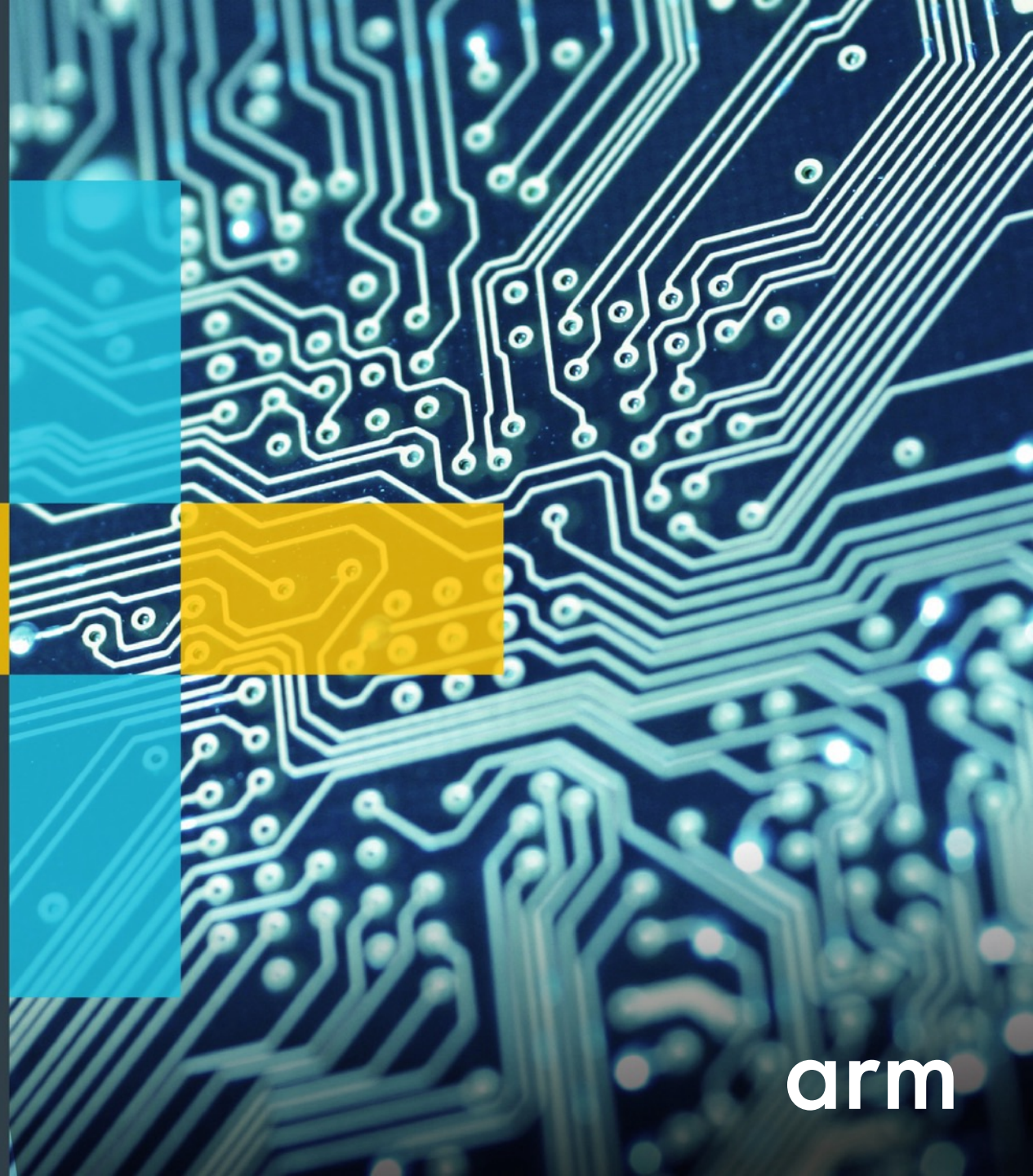
IoT and Silicon Security

Dissecting a Real-Life IoT Attack



Chowdary Yanamadala

Technology Strategy

Arm

arm

Agenda

- An overview of silicon security
- Side Channel Attacks explained
- Dissecting a real life IOT attack
- Emerging threats
- Defending against silicon threats

arm

Silicon Security Overview

Large Attack Surface – Recent Exploits

Google Security Blog

The latest news and insights from Google on security and safety on the Internet

Advisory: Security Issue with Bluetooth Low Energy (BLE) Titan Security Keys

May 15, 2019

Peekaboo vulnerability exposes hundreds of thousands of security cameras to hacking

BY DUNCAN RILEY

A new vulnerability discovered in firmware from NUUO Inc. allows malicious actors to view and tamper with video surveillance recordings, according to researchers from security firm Tenable Inc.

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE

RELOADED —

New variants of Mirai botnet detected, targeting more IoT devices

Palo Alto Networks researchers spot versions for 5 more processors in the wild.

SEAN GALLAGHER - 4/9/2019, 12:49 PM

Enterprise Security: Major Flaws Found in Bluetooth Chips

Security firm Armis has discovered two vulnerabilities in Bluetooth Chips from several networking industry leaders.

By Sydny Shepard | Nov 05, 2018

Two serious chip-level vulnerabilities that could potentially put "millions" of enterprise access points at risk was discovered last week by researchers at security firm Armis.

Security flaw can leak ME encryption keys

Intel has released updates for Intel ME, SPS, and TXE firmware to address encryption key-spilling flaw.

By Catalin Cimpanu for Zero Day | September 13, 2018 -- 19:26 GMT (12:26 PDT) | Topic: Security

13,513 views | Jul 27, 2017, 05:00pm

Criminals Hacked A Fish Tank To Steal Data From A Casino

New Chip Bug Can Expose All Data on a Computer to Hackers

By: Wayne Rash | March 30, 2019

NEWS ANALYSIS: Security researchers report that the Intel VISA chips can be exploited to expose information from signals that pass through the system boards of some computers.

c|net BEST PRODUCTS REVIEWS NEWS VIDEO HOW TO SMART HOME CARS DEALS

SMART HOME

Hackers can peek through surveillance cameras, report says

A researcher in Argentina showed he could log into tens of thousands of DVR cameras and view the video stream live, according to Bleeping Computer.

CPUs impacted by new Zombieload side-channel attack

researchers, academics detail new Microarchitectural Data Sampling (MDS) attacks.

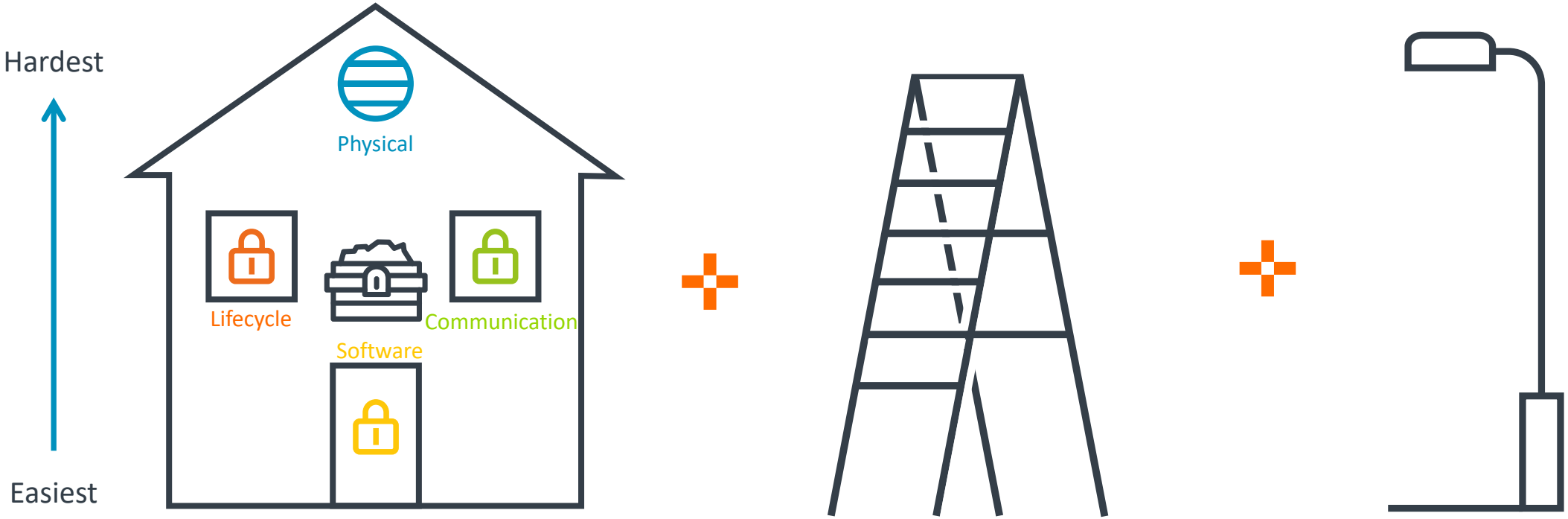
By Catalin Cimpanu for Zero Day | May 14, 2019 -- 17:00 GMT (10:00 PDT) | Topic: Security

System Security: You're Only As Strong As Your Weakest Link

The attack surface is growing

Attacks are becoming easier

The risk is only increasing



Matching Vulnerability, Mitigation

Platform Security Architecture

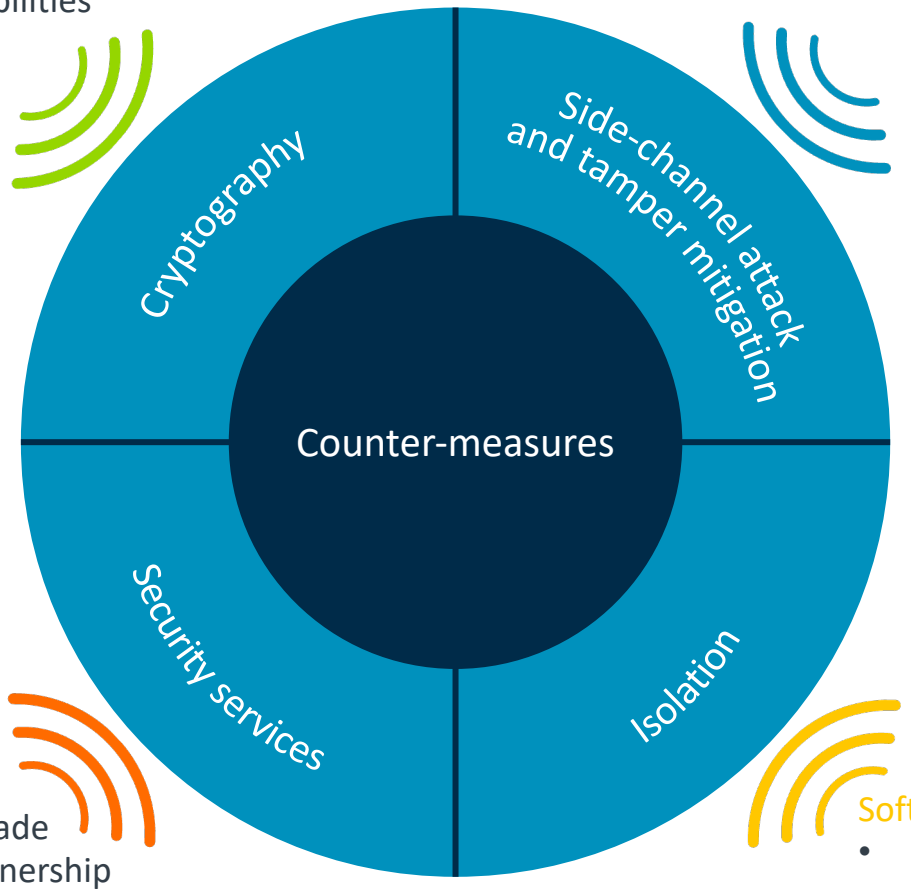
Analyze
Threat modelling

Architect
Hardware & firmware architect specs

Implement
Firmware source code

Certify
Independently tested

Communication
- Man-in-the-middle
- Weak RNG
- Code vulnerabilities



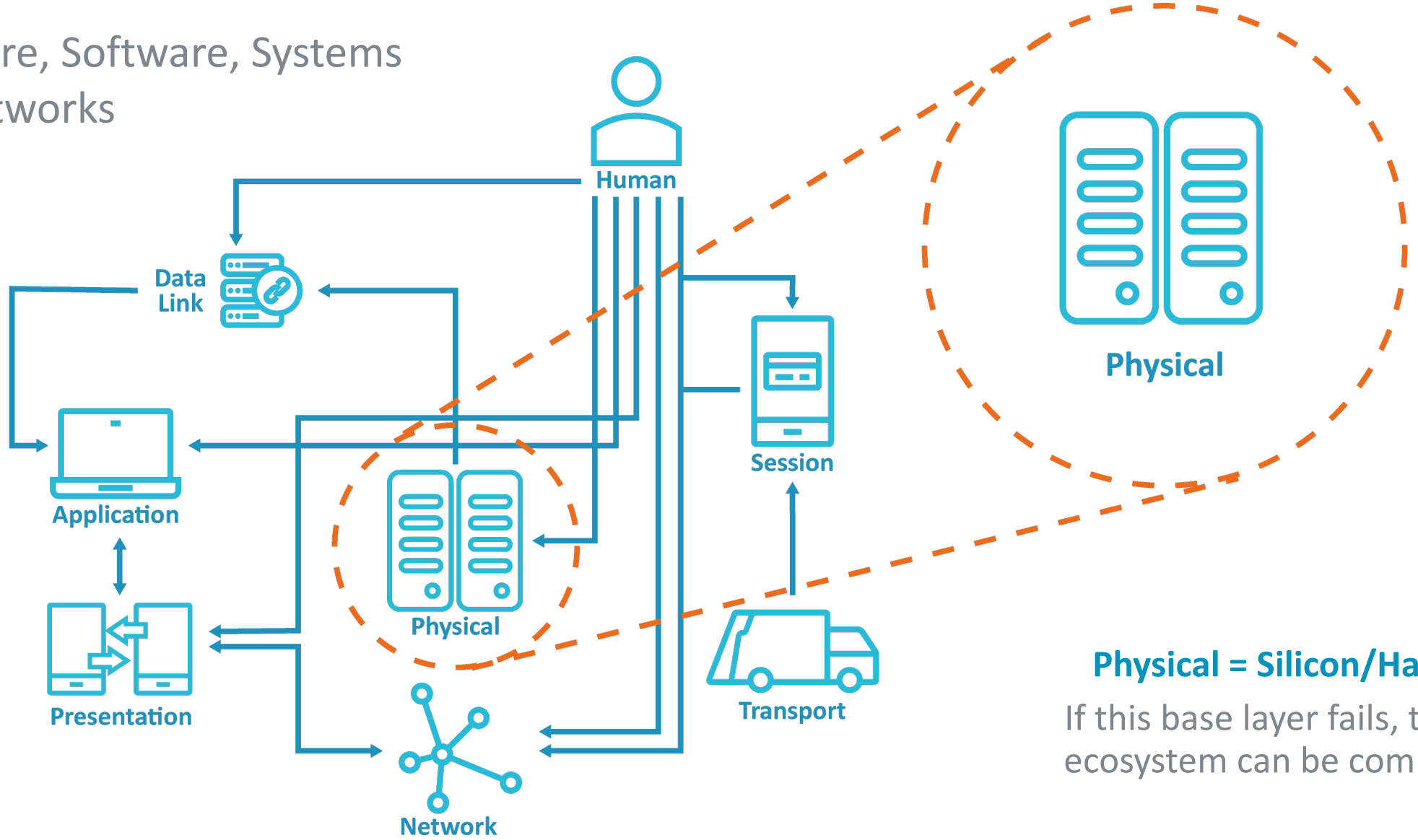
Physical
- Non-invasive: e.g. clock or power glitch or SCA
- Invasive: package removal, e.g. microprobe station FIB

Lifecycle
- Code downgrade
- Change of ownership or environment
- Factory oversupply

Software
- ROP, e.g. buffer overflows
- Interrupts
- Malware

Attack Surface

Hardware, Software, Systems and Networks



Physical = Silicon/Hardware

If this base layer fails, the entire ecosystem can be compromised

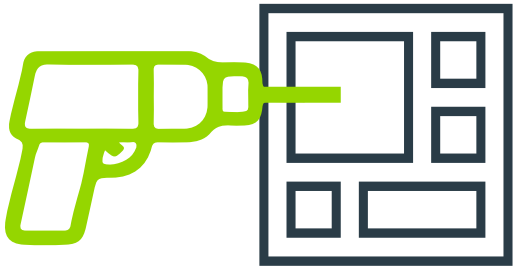
Defining Physical Attacks

Non-invasive attacks

- Observation methods
- Attacks leave no trace

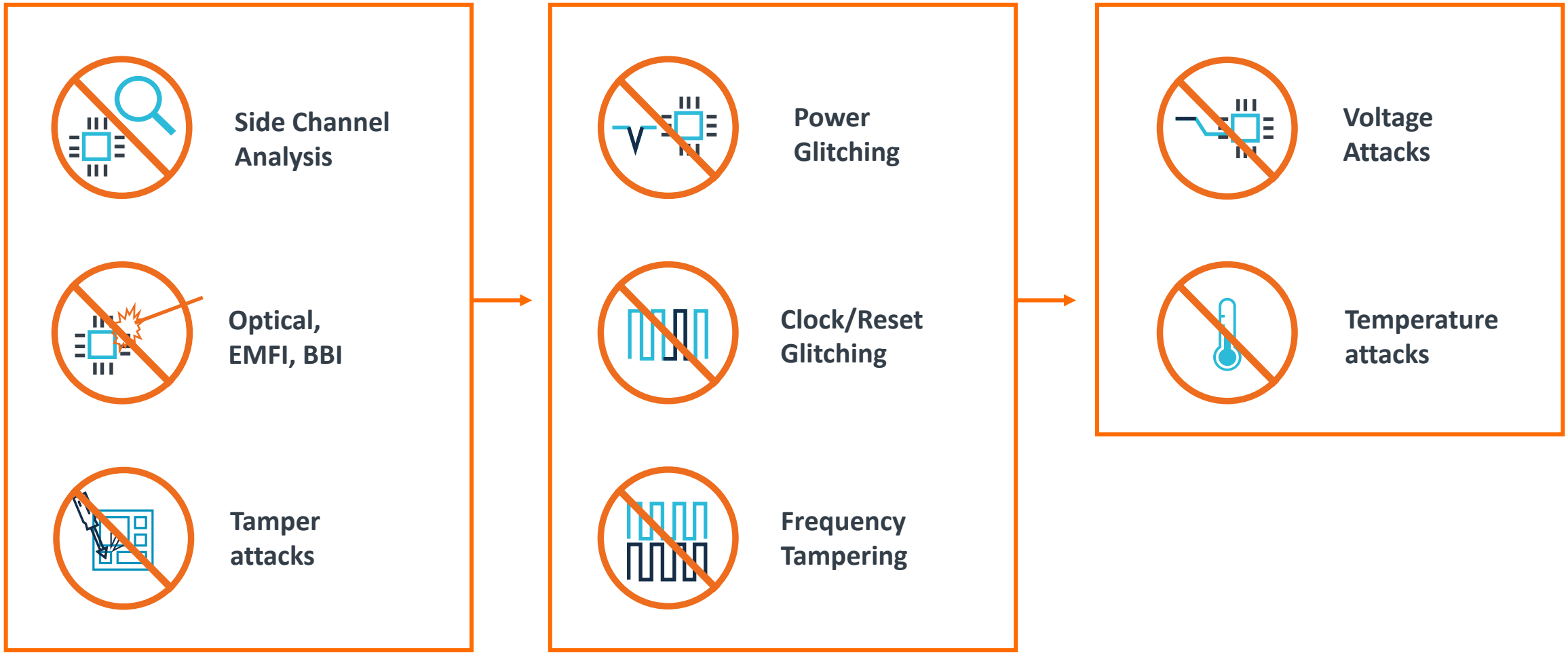
Invasive attacks

- Manipulation of chip
- Requires chip surface to be exposed



Unlike Spectre and Meltdown, physical attacks are close-proximity attacks, not remote-style attacks that require installation of malware

Defending Against Physical Vulnerabilities



What is Side Channel Analysis (SCA) attack

SCA attack explained with AES encryption example

AES encryption Scheme

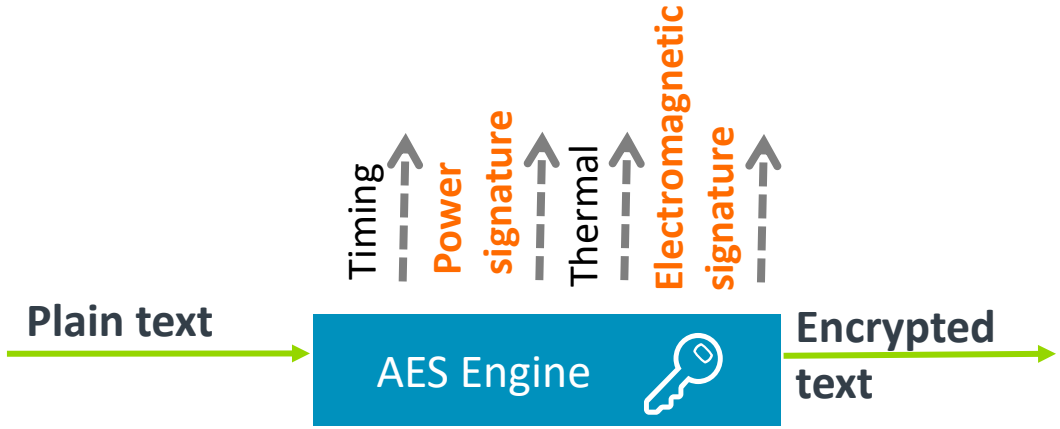
AES decryption Scheme

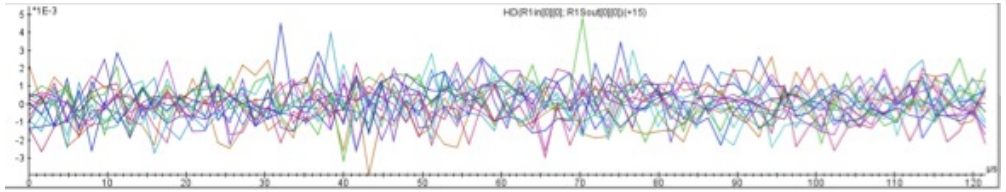
- AES is a symmetric key encryption algorithm. AES scheme consists of three components-
  - Plain text
  - Encrypted text
  - Secret key

- AES algorithm is mathematically strong. Impractical to decrypt using mathematical attack (computational brute force).

arm

Principle of SCA attack





The primary goal of an SCA attacker is to gain knowledge of the key

Semiconductor devices consume current during switching.

Power signature varies when switching from 1 -> 0 or 0 -> 1.

Shape of power consumption reveals secret keys of crypto engine.

Analysis of power profiles can reveal sensitive data (secrets)

arm

History of SCA attack

1995 Timing Analysis Attack is the first SCA attack introduced by Paul.K

2000 EM Analysis Attack demonstrated. Can be applied from distance

1998 Power Analysis Attack is introduced. Much more efficient technique

201X DL/ML enabled SCA attacks on the rise..

arm

arm

Dissecting a real life attack

“IoT Goes Nuclear: Creating a ZigBee Chain Reaction” (1)

https://eprint.iacr.org/2016/1047.pdf

Scenario

IoT devices infect each other with a worm that rapidly spreads over large areas (Depending on critical mass).

“IoT Goes Nuclear: Creating a ZigBee Chain Reaction” (1)

Impact

Starts with infecting a single street lamp with a worm.

The worm spreads to wider network of street lamps

Enables an attacker to control and abuse city lights & Massive DDOS attack

Interesting note: In Paris (~105 Sq.KM), critical mass is fewer than 15K randomly selected smart street lamps.

“IoT Goes Nuclear: Creating a ZigBee Chain Reaction” (2)

How did attackers

- ***gain control of an already installed lamp ?***
- ***perform an un-authorized over-the-air firmware update ?***

“IoT Goes Nuclear: Creating a ZigBee Chain Reaction” (3)

How did they gain control of an already installed lamp ?

“We overcame the first **problem by discovering and exploiting a major bug in the implementation of the Touchlink part of the ZigBee Light Link protocol…**

How to *perform an un-authorized over-the-air firmware update ?*

“ a side channel attack to extract the global AES-CCM key (for each device type) that manufacturer uses to encrypt and authenticate new firmware.”

“IoT Goes Nuclear: Creating a ZigBee Chain Reaction” (4)

How was the Side Channel Attack performed?

“all the lamps (at least from the same product type) use the same global key. ….**deduce all the secret cryptographic elements** ….., using novel **side channel attacks** …“.

“…Once we obtained these secret values, we could create any new firmware and upload it into any …. lamp.”

Interesting note The equipment used in the SCA attacks costs just a few $100.

Security Issues Demonstrated In This Attack …

Protocol implementation bug in the ZLL (Zigbee light link) was not revealed in protocol validation…

Usage of symmetric keys shared within a large class of devices

- A ZLL symmetric master key (for initial delivery of a network encryption key) is used by all ZLL certified products
- A symmetric key for firmware update is shared across all devices of a certain type

Not protecting these keys very well…

- ZLL master key leaked long ago…
- The firmware update key was extracted through a side channel attack

arm

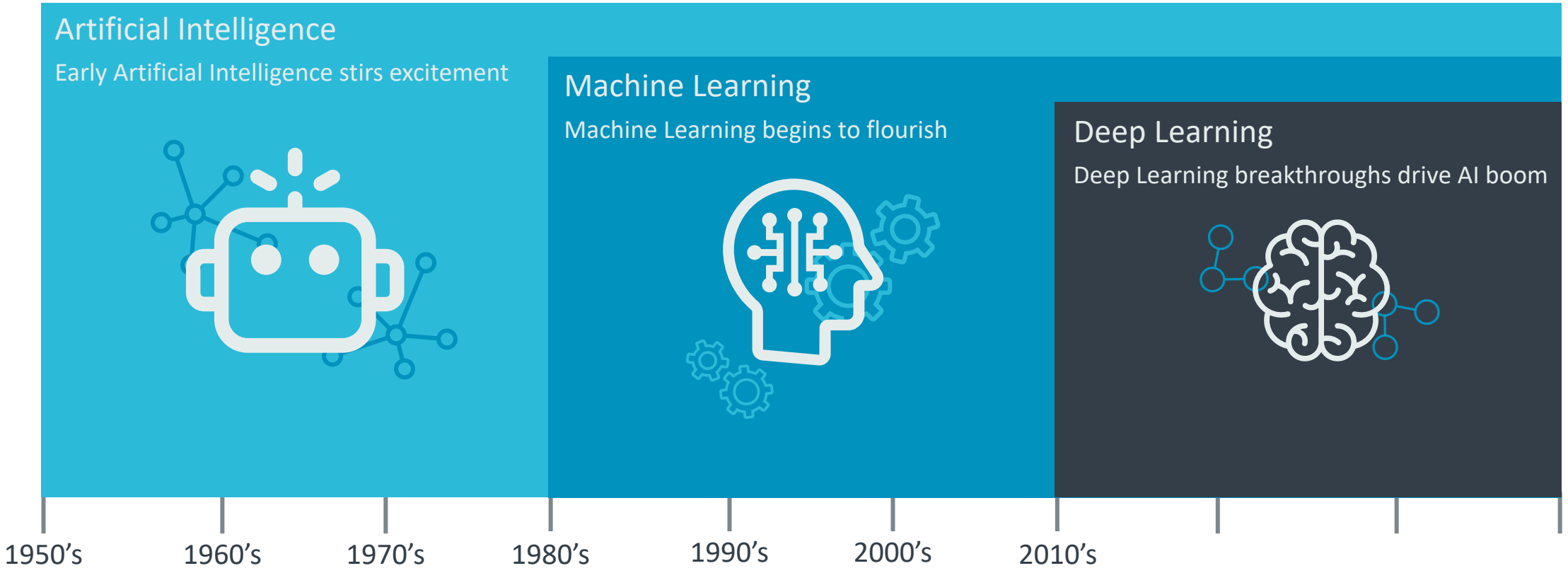
Silicon Security : Advanced Threats

Enabled by Artificial Intelligence , Machine Learning & Deep Learning

Silicon Security : Advanced Threats

Enabled by Artificial Intelligence , Machine Learning & Deep Learning

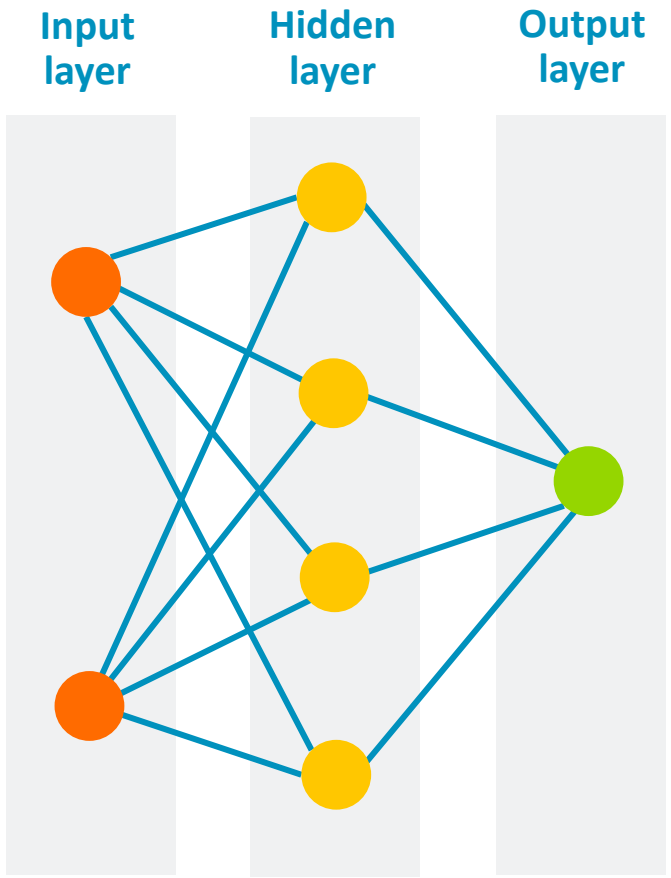
AI, ML and DL Overview



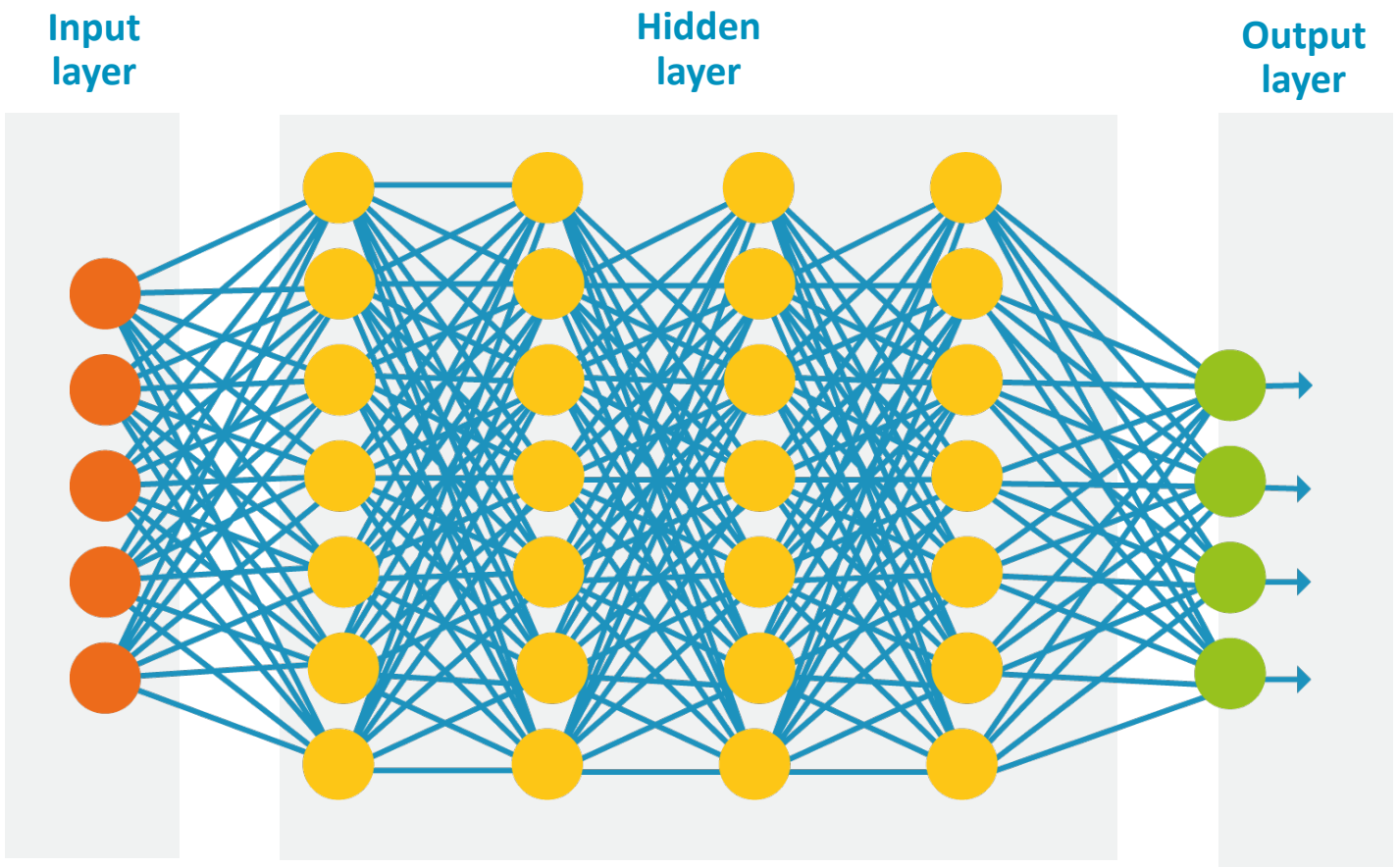
Since an early flush of optimism in the 1950's, smaller subsets of artificial intelligence – first machine learning, then deep learning, a subset of machine learning – have created ever larger disruptions

Deep Learning Explained

What is a Deep Learning network?



A Simple Neural Network

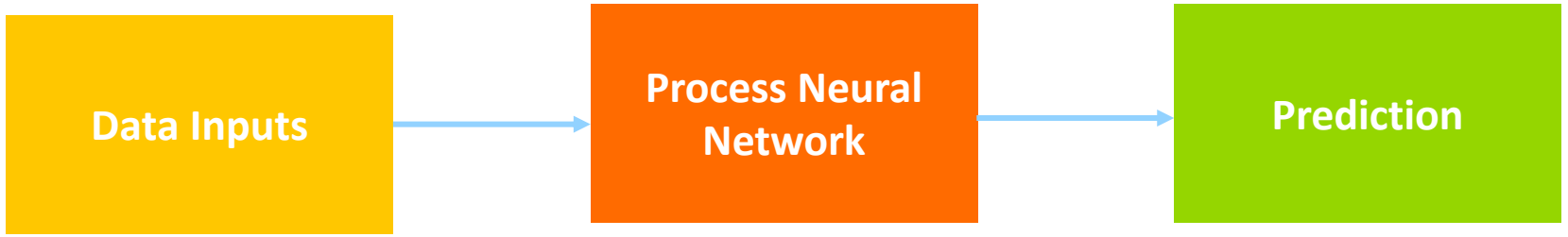


Deep Learning network

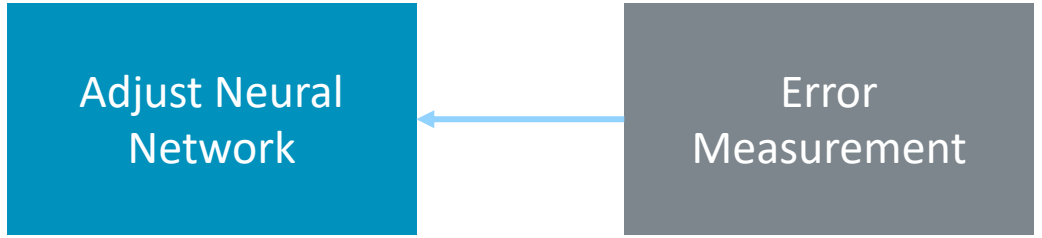
Deep Learning Explained

How does Deep Learning learn?

Forward Pass

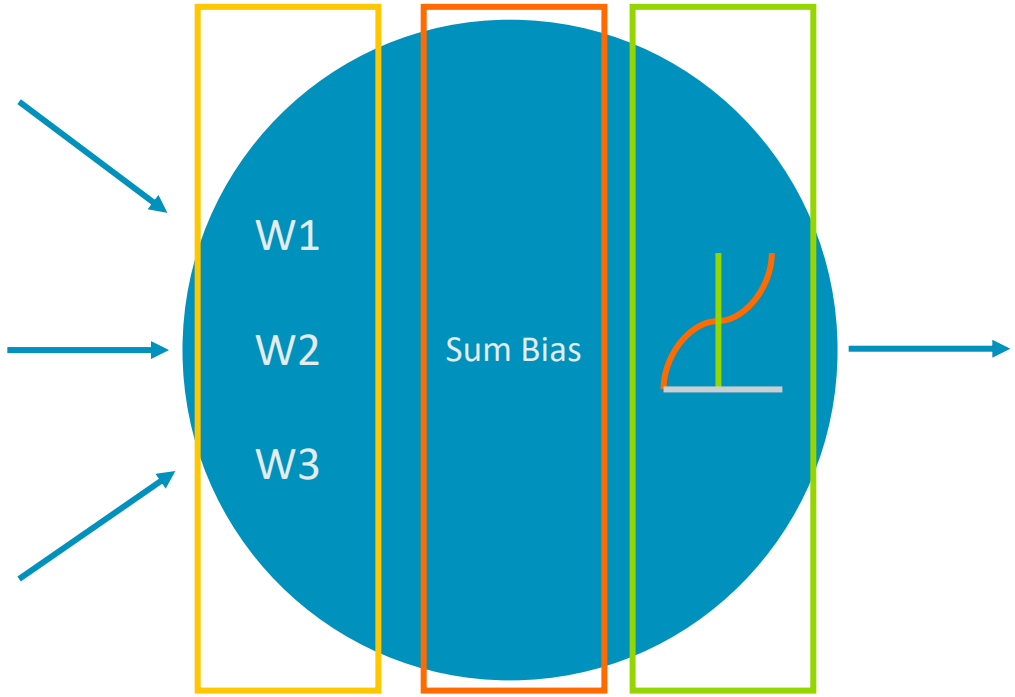


Backward Pass
(aka Backpropagation)



Deep Learning Explained

Forward Pass at a Node level

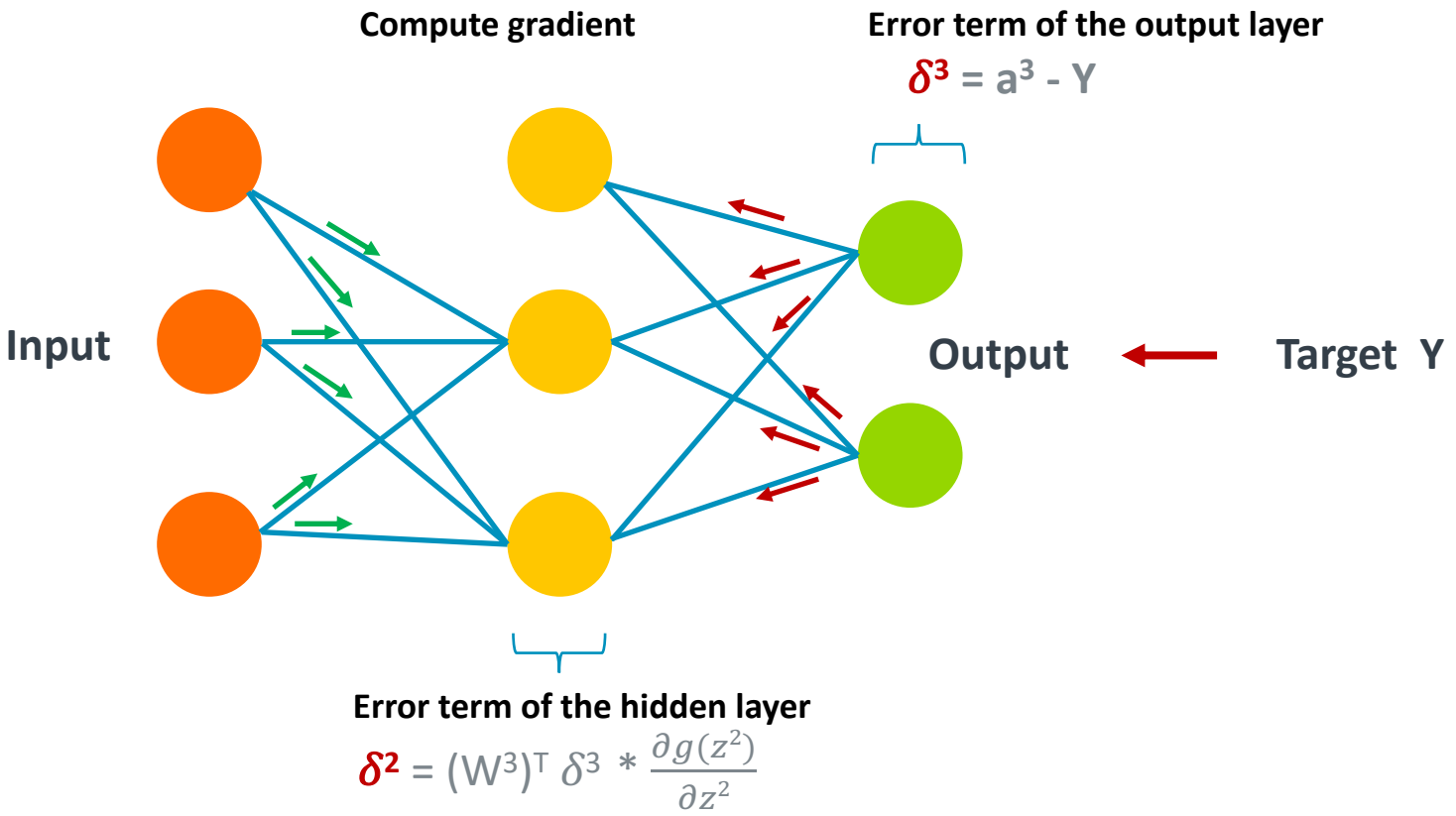


1. Apply the weights
2. Add weights and apply bias
3. Apply activation function

arm

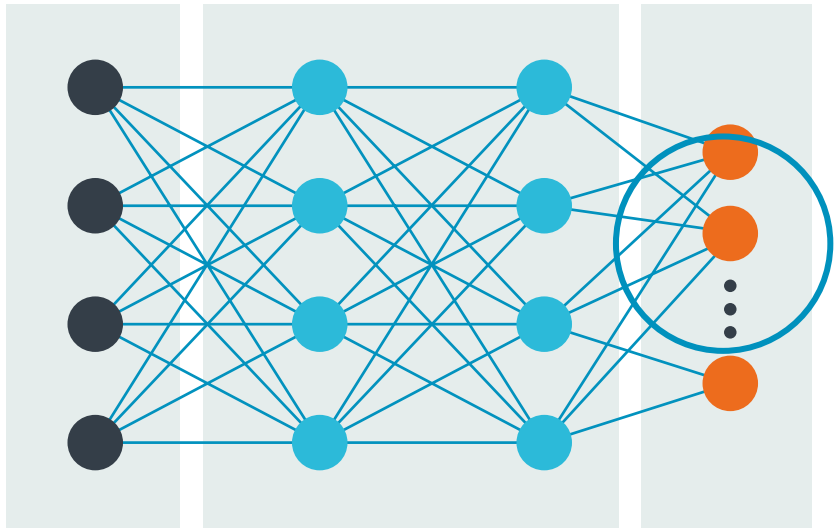
Deep Learning Explained

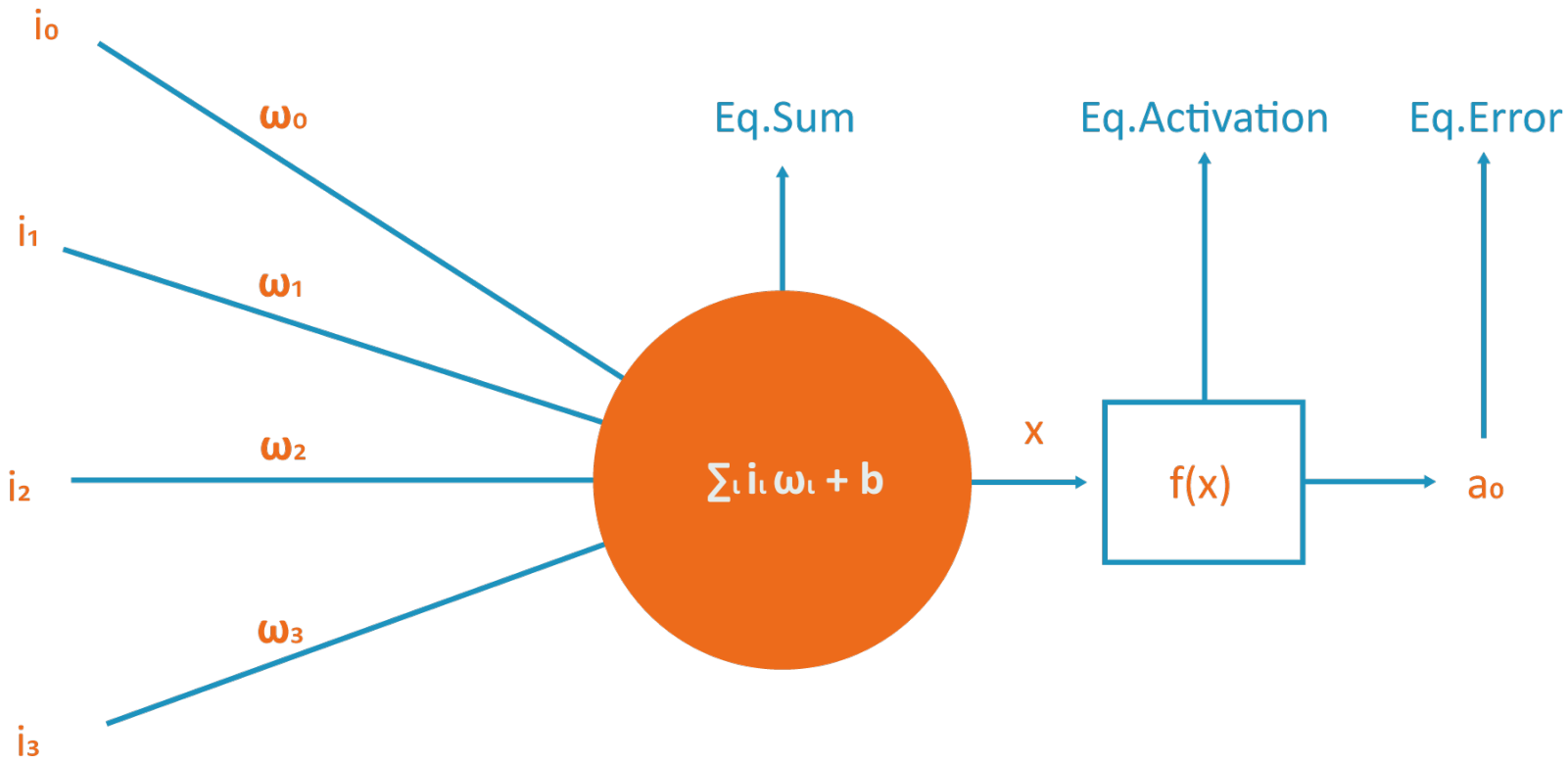
Back propagation



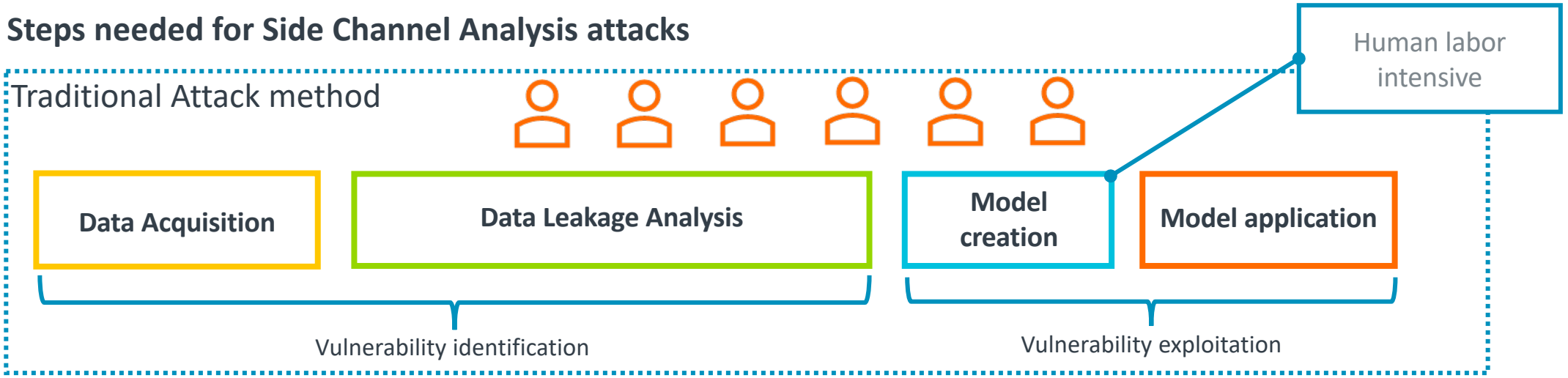
Update weights and gradients to decrease Loss function

Deep Learning – Back Propagation

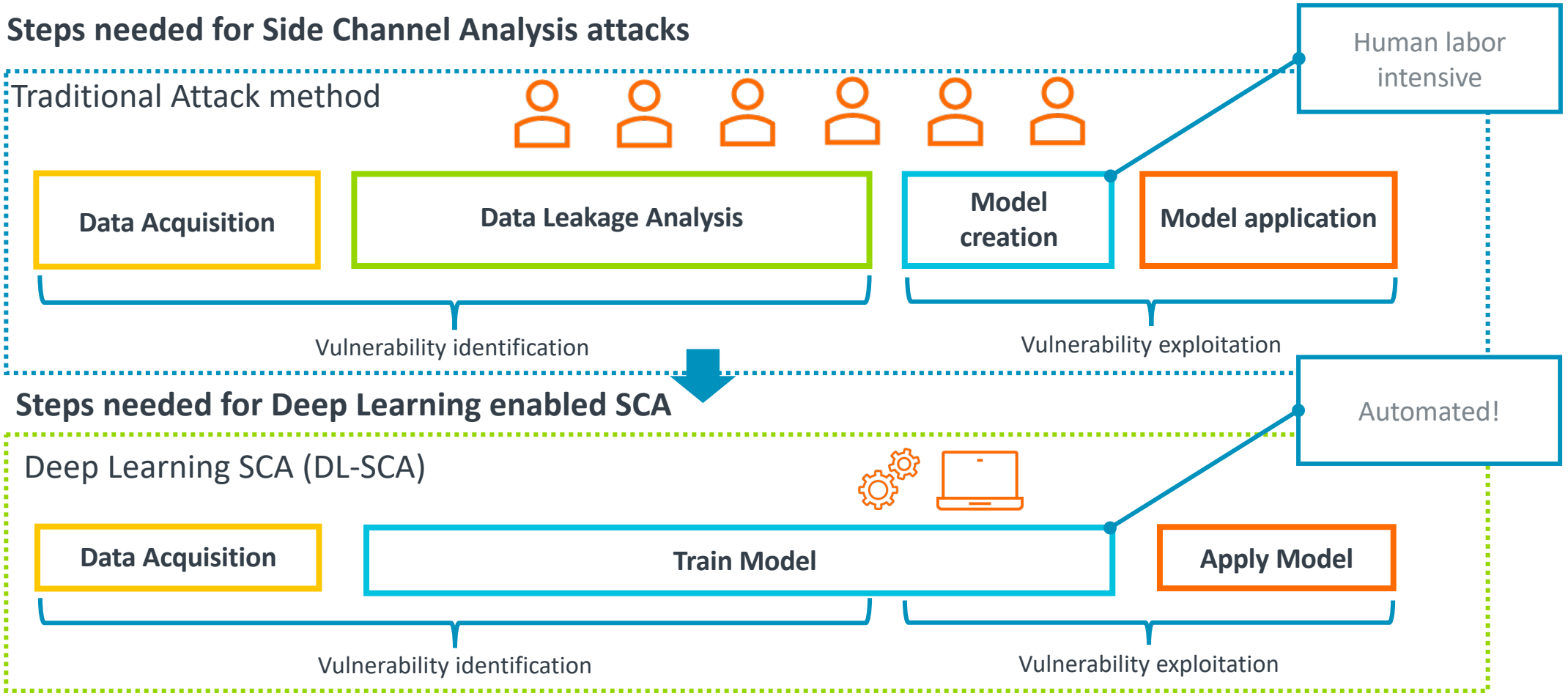




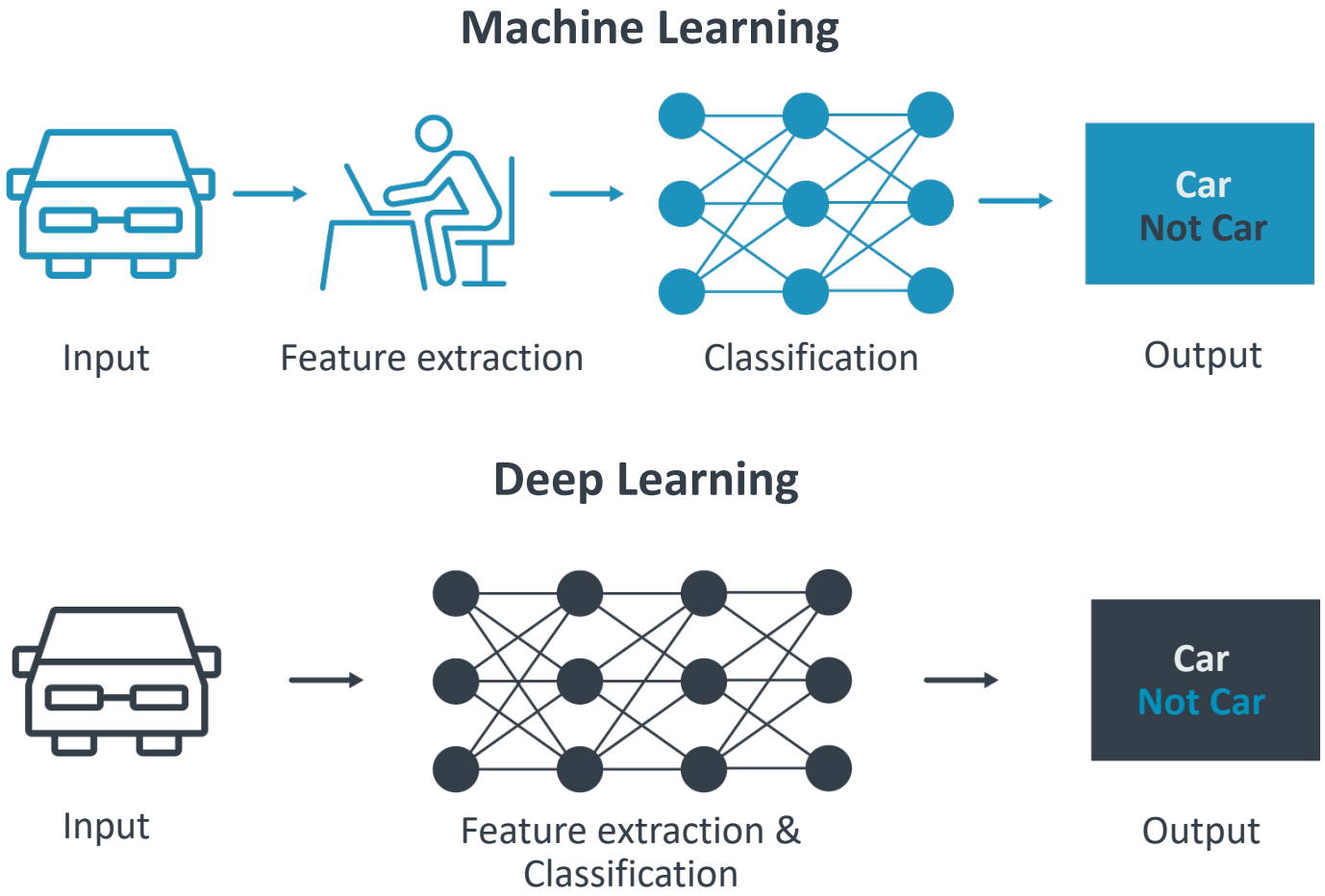
Emerging Threats: Deep Learning Based Side Channel Attacks

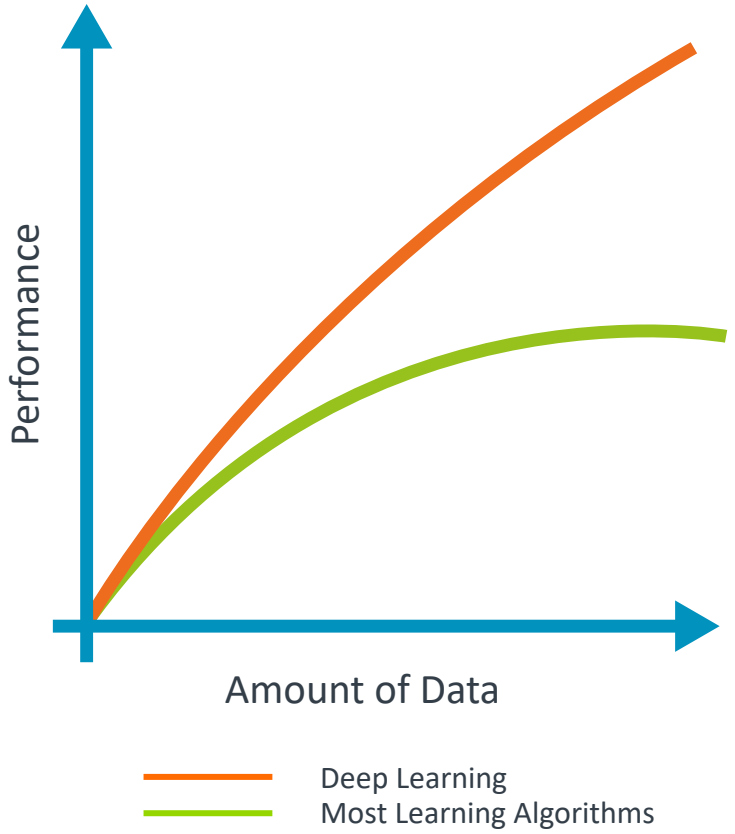


Emerging Threats: Deep Learning Based Side Channel Attacks

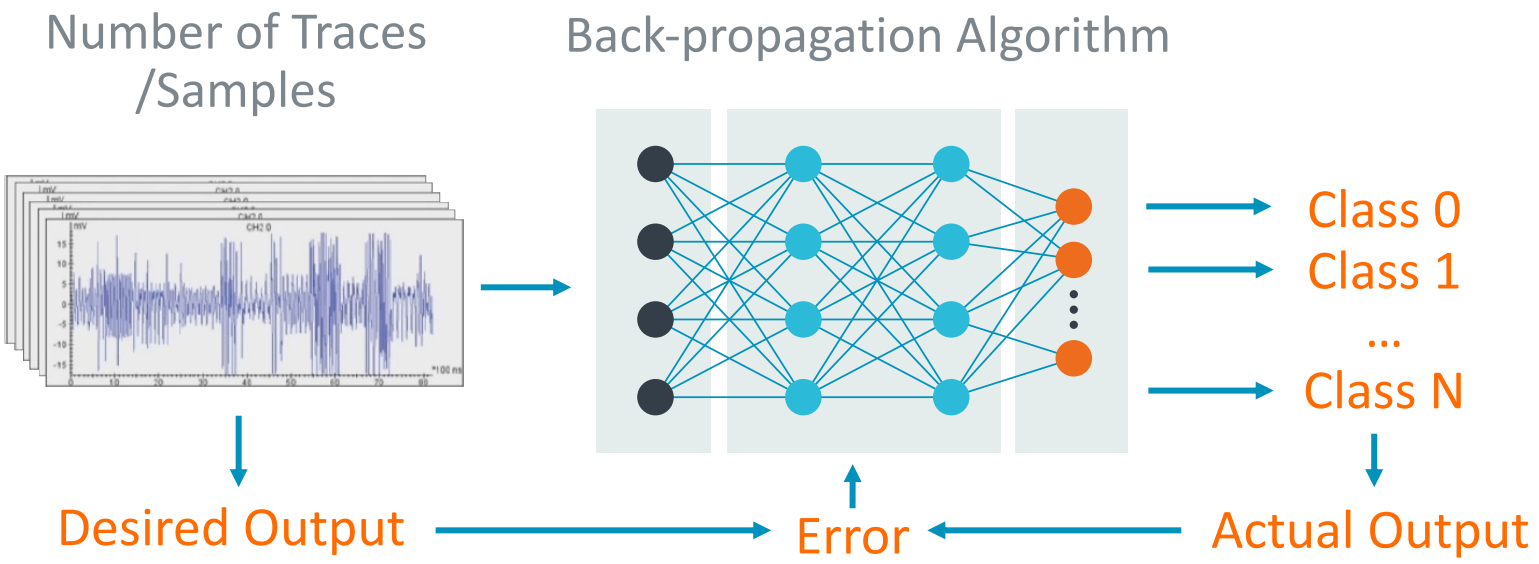


Deep Learning + SCA – Basic Facts





Deep Learning + SCA – Basic Facts

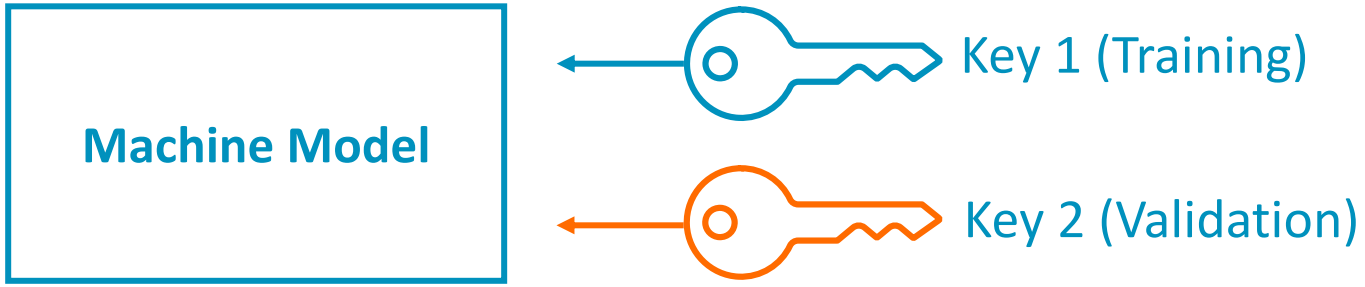


AES
S-Box Out
Hamming Weight
9 possible classes

DES
S-Box Out
Hamming Weight
5 possible classes

Two objectives for DL-SCA

- **Extract the secret keys**
- **Efficient Neural network**



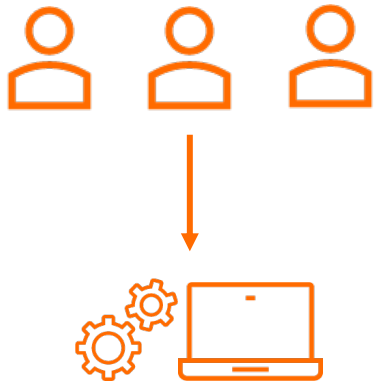
Model is generalizing if it can break different keys

Deep Learning + SCA – Summary of the Threat

Deep learning is a computationally intense technique which requires more time and memory resources than traditional SCA. However, it has clear benefits to an attacker.

Trades human effort with machine effort.

Automatic feature extraction enabled by CNN – points of interest selection is no longer necessary.



DL-SCA can pose serious threat to traditional counter-measures

CNNs can extract features independently of their position in the data.

DL-SCA can bypass jitter-based effects from unstable clock domains or even random delays counter-measures.

Deep learning might be able to break widely adopted counter-measures like masking or shuffling.

arm

Silicon Security: Defending Against Threats

Vision For Security

Key security considerations

1 Security needs to be built-in from the ground up

2 A collective industry responsibility

3 Security needs to be simple, with seamless integration

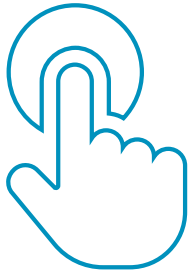
Platform Security Architecture (PSA) is the perfect starting point

Providing a framework to ensure consistent security

In summary...

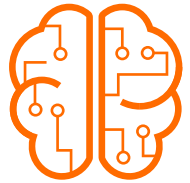
SCA "Push-button Attack" is optimistic at this point for protected implementations

SCA attacks requires some level of expertise. However, unprotected implementations are easy to break.



SCA is rapidly evolving to become a practical attack

SCA will become a dominant tool for silicon attackers. Mitigating against SCA and other physical attacks is essential.

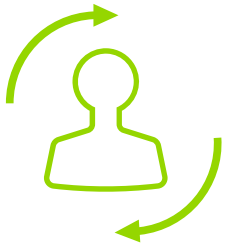


Today, Traditional mitigations are generally holding up against Physical attacks

DL-SCA may force us to move away from some mitigations (time based). And strengthen existing countermeasures

Security is not binary. Awareness and Adaptability is the key

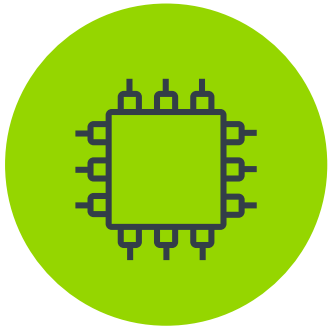
Best way to build defense is to be aware of the offensive tactics.
Adapt and enhance our defensive IP continuously against emerging threats



IoT is Quicker, Easier, More Flexible and Secure with Arm

Low power,
scalable compute

Security, Identity
& Platform Security
Architecture



Configurable SoC
Frameworks

OS & Tools

System-level solutions to simplify IoT development and deployment:

Secure | Scalable | Configurable | Power efficient | Consistent

arm

arm

Thank You
Danke
Gracias
Grazie
谢谢
ありがとう
Asante
Merci
감사합니다
धन्यवाद
Kiitos
شكرًا
ধন্যবাদ
תודה
ధన్యవాదములు