Future of IoT with Embedded A.I. and its New Security Implications

Prof Yu Chien Siang
Chief Innovation Officer
Certis Group

Agenda

- Introduction
  - A.I. First and Cyber Security
  - Embedded A.I. Changes IoT
  - Era of Distributed Intelligence at the Edge
- A.I. Errors
- Conclusion

Latest - Mobile Phones support A.I.

Introduction

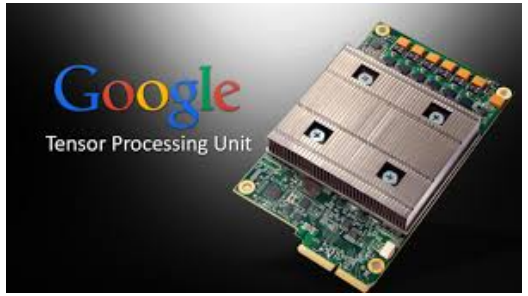
A.I. First

- Baidu's CEO Robin Li, “Gone is the era of PC, and soon we will say goodbye to the era of mobile internet…
  We believe that coming is the **era of artificial intelligence**.”

  Baidu has made A.I. its main focus for future growth and will be applying this technology in its financial services business.

- **AlphaGo Zero** is a software version created without using data from human games, and by playing games against itself.
  It is interestingly, stronger than any previous version.

- More and more global and MNC efforts are directed at Self Driving/Connected Cars and autonomous robots/drones
  (to arrive by 2020).



How A.I. and Machine Learning could Defend our Enterprises

A.I. cyber security at the Edge to manage IoT Security

A.I. Anomaly Detection for Event Monitoring

A.I. to speed up Incident Response & remediation

A.I. to analyse incoming files for malware and to discover software / system vulnerabilities

AI core that continuously learns to create a Neural Databank for cognitive enterprise

Machine Learning to spot insider attacks & fraud

Crown Jewel

certis

Rapid Developments of New Low Power, Cognitive Chips

- **Embedded A.I. for Deep Learning**
  - *A11 bionic neural engine (A.I. chip in iPhone X)*
  - *Neural Processing Unit (NPU) in Huawei Kirin 970*
  - *Neural Processing in Qualcomm Snapdragon 835*
    - *Snapdragon Neural Processing (SNPE) software development kit (SNPE-SDK) offers any combination of the mobile's CPU, GPU and DSP processors to handle deep learning.*
  - *Intel Movidius*

Movidius

- A.I. algorithms redesigned for mobile phones
  - MobileNet (Google)
  - Use Quantisation (TensorRT) to speed up

certis

Embedded A.I. Hardware

Xiaomi Mi 6

- Chipset: Qualcomm MSM8998 Snapdragon 835
- CPU: Octa-core (4x2.45 GHz Kryo & 4x1.9 GHz Kryo)
- GPU: Adreno 540
- Primary Camera: Dual 12 MP
- Secondary Camera: 8 MP
- WLAN: Wi-Fi 802.11 a/b/g/n/ac, dual-band, Wi-Fi Direct, DLNA, hotspot
- Bluetooth: 5.0, A2DP, LE
- GPS: Yes, with A-GPS, GLONASS, BDS
- Approx Price: $S 599

HUARAY | alhua TECHNOLOGY + Movidius bringing mobile to life

Movidius Neural Compute Stick

- USB stick containing a Movidius Myriad 2 processor
- Approx Price: US $79

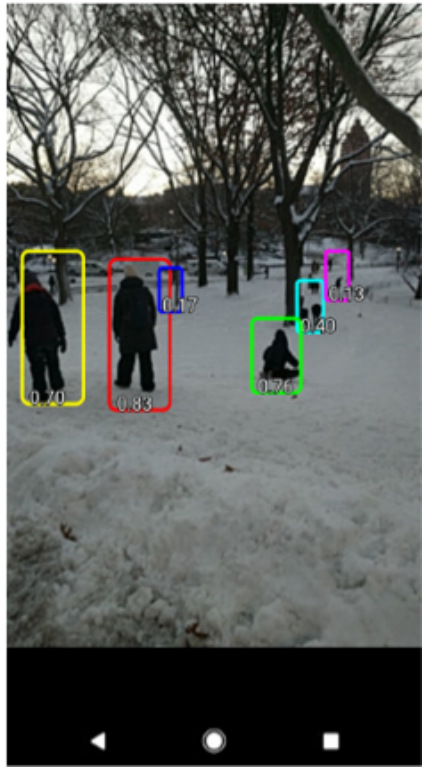
Movidius has provided visual intelligence solution for a number of products such as DJI drones, Hikvision/Dahua cameras.

certis

Embedded A.I. Applications

Video – Object Detection On Embedded AI Chips

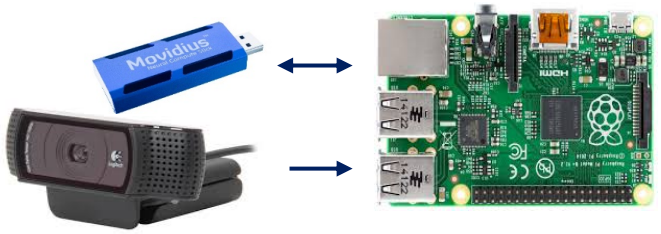
1. Object Detection running on Mi 6

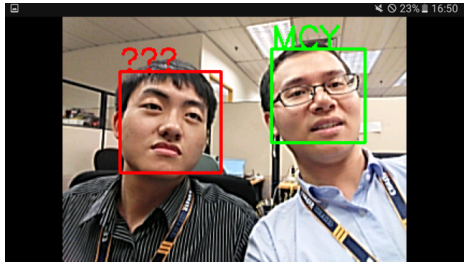


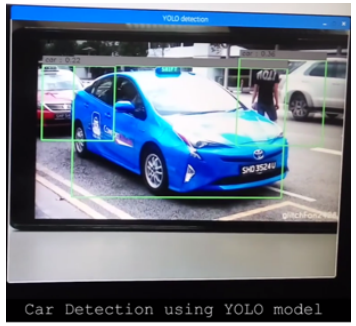
We tested image classification model and facial recognition model which can fit in latest SNPE runtime.

CPU: 0.55 seconds per image
GPU: 0.45 seconds per image

2. Object Detection running on Movidius







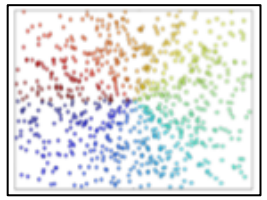
Facial Recognition via Mobile

certis

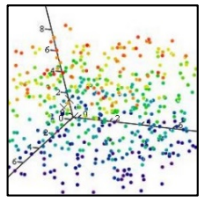
Sound Recognition

Model Training

Training Dataset
(*urban sound 8k*)



Feature Extraction



Classification

Model file for deployment

Model Deployment

Sound Detector

Sound Recording

Preprocessing
(e.g. Noise Reduction)

Detection

Detected Sound

Sound Recognition
(webservice in Docker)

Model inference
for classification

Send results to AI-integrated system

certis

These Self-learning, Adaptive Low Power Embedded Systems will Revolutionise IoT Systems

- Much improved price performance.
- **Low cost intelligence** at the edge and can collaborate well with each other by exploiting smart agents and cloud A.I. backend.
- Heralds new mainstream capabilities for IoT, via the emergence of A.I. powered smart cameras, robotic and drone autonomous controls and next generation devices for smart building maintenance and facility management.
- We successfully tested a few deep learning models (e.g. image classification, object detection and facial recognition). We used the latest SDK (SNPE SDK v1.2.2 and Movidius NC SDK v1.09) for a number of common neural network layers and operations.

A.I. Deep Learning will Empower Attackers as well

- Deep Learning (DL) is an advanced brand of Artificial Intelligence (A.I.), empowering users with capabilities beyond what Machine Learning (ML) was able to offer in the past, in terms of statistical outlier analysis.
- Hacking DL will enable hackers to sift through complex network data sets, discover vulnerabilities and how best to attack in a fully automated fashion. **Will learn and essentially "teaches" itself to recognise the world, people, objects, words or sentences as part of a hacker's processing stream.**
- Improves the hacker's arsenal and problem solving capabilities **without external intervention (operates inside an air gap)**
- Can speak like a human and emulate the voice of anyone if it can get training data. Done by WaveNet from DeepMind, Google. Improved on by Baidu.
- Mobile phones can run A.I. for insider hack, attacking the enterprise from within. Can navigate within a **complex networks, possibly better than a human.**

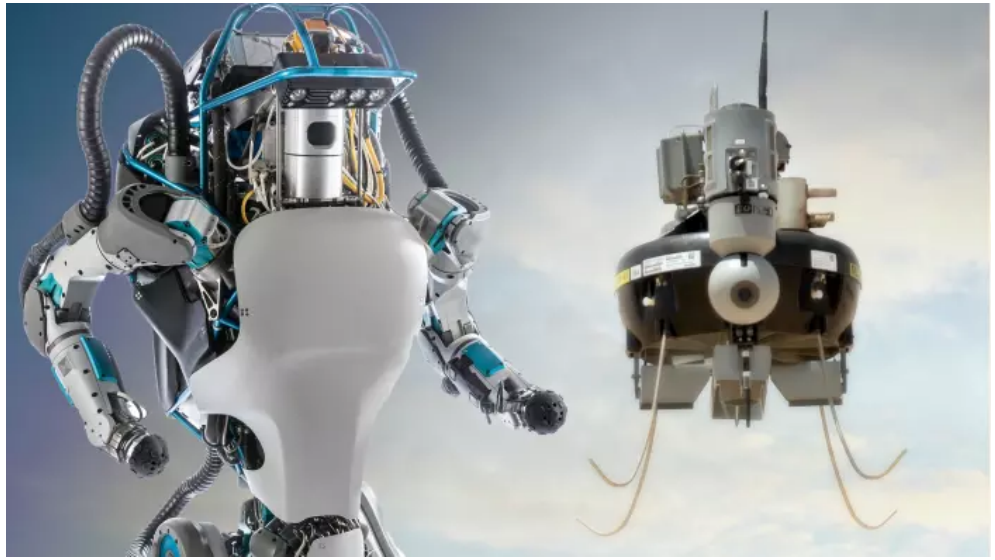
When people start telling you that you're crazy, you just might be on to the most important innovation in your life

– Larry Ellison

Is this Not a New Arms Race Using A.I.?

https://www.ft.com/content/b56d57e8-d822-11e6-944b-e7eb37a6aa8e

- We fear this to be the **Next Gen Cyber War**
- FT, 12/1/17 – A.I. arms race risks spiralling out of control, report warns



Despite the Buzz, A.I. is Not the Panacea for All Things that Cannot be Done Previously

- Since cyber criminals have also stepped up their attempts to deploy A.I. for offensive operations, **cyber defenders are hurrying to arm themselves with A.I. tools** to do the following:
  - automate the detection of malware and network cyber attacks,
  - remediate and investigate using A.I. and
  - seamlessly sort, manage, collate and handle the vast amount of cyber security intelligence that is coming in on a daily basis

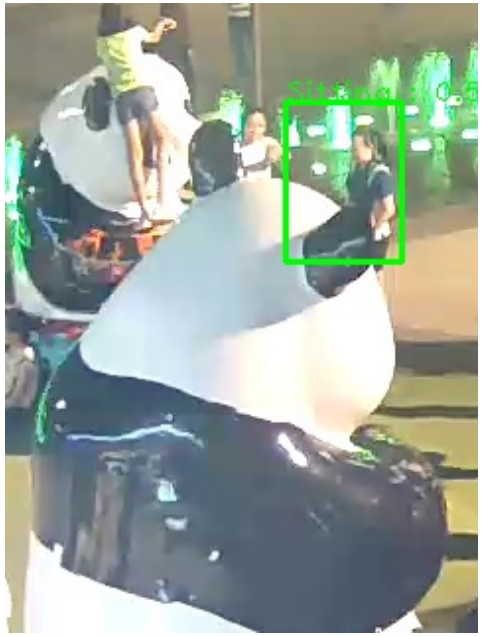
A.I. & Cyber Security will eventually converge!

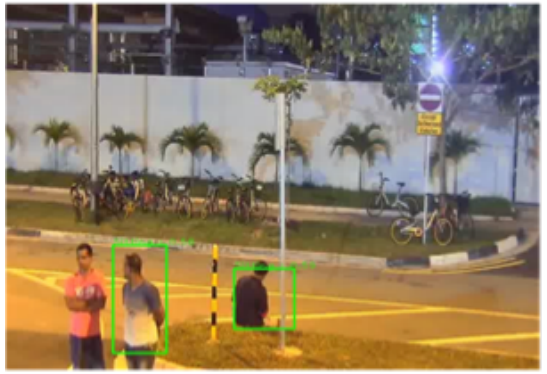
The Limitations of A.I.

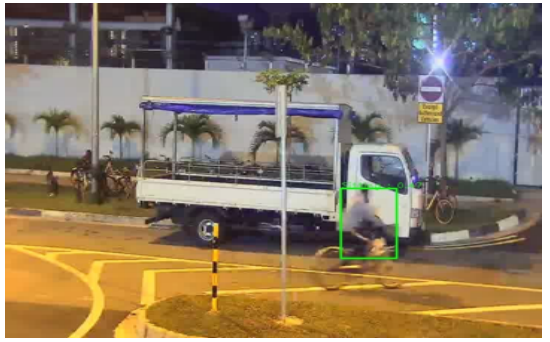
Why should we not overrate A.I. for Cyber Security?

- Machine learning will offer very good classifiers that can look at data and classify it into buckets that have been previously defined. They work very well if the attacks or behaviours are similar to the classification pattern that they were trained on.
- If there were a state-sponsored attack, like an election attack, that has similar characteristics to things that have been seen before, these would be well-served by machine learning and can be detected.
- But if a sophisticated state actor executes a unique attack (zeroday) that has never been seen before, the dissimilarity of the attacks to those that were previously known (created in order to intentionally evade) will lead to the defeat of today's A.I.
- A much smarter A.I. will be needed - one that can understand the attacker's intent, his objectives and the way he thinks.
- However, as such advanced A.I. is not yet operationally available, the fall-back is to leverage a human-machine team to manage something that is radically different from what was known previously.

Examples of Wrong Detection (Sitting)







Auto Pilot (Tesla Accident)

https://www.theregister.co.uk/2017/06/20/tesla_death_crash_accident_report_ntsb/

7th May 2016

- Fatal motorway collision between a Tesla Model S and a truck, confirming Tesla's earlier statement that its autopilot failed to notice the truck blocking the car's path.
- The accident, which happened in May last year on US Highway 27A in Florida's Levy County, left the 40-year-old driver, Joshua Brown, a US Navy Seal turned networking hardware company owner, dead after the collision.
- The car issued six audible warning alerts that he'd spent too long with his hands off the wheel.
- But then a truck slowly pulled out of a side road onto the highway, and the Tesla smashed into its trailer and passed underneath "in a cloud" of debris, according to the report. The trailer lacked side guards that would have stopped the car from going under and Brown suffered fatal head injuries.
- The vision system had likely mistaken the trailer to be part of "the road with sky/cloud"; i.e. failed to recognise "the white side of the tractor trailer against a brightly lit sky".

DJI Drone Case – A.I. Malfunction

Safe to land

Unsafe

- The drone's A.I. chip supports a Safe Landing mode, using a down facing camera.
- When triggered to land on a grassy patch, the drone descended and at low level, went berserk and flew across the field to the other side of the road, almost hitting a person.
- Suspect: the drone's vision system sees different things at different heights. Upon descend, it decided that grass was unsafe to land on and sought a non grass area in a dangerous fashion.

Poisoning the A.I. Model

- With the emergence of fast paced improvements in predictive models, we will become better at detecting cyber attacks over time. Hackers will then look for ways to confuse our models, e.g. via adversarial A.I.
- Bad actors will study how the underlying models work and find evasion techniques and ways to circumvent our new A.I. defences. E.g. force the defender to recalibrate the model by flooding it with false positives (tantamount to getting your intrusion alarm to go off all the time, until you get so frustrated, you turn it off altogether). That would then be the perfect opportunity to break in.
- In a gist, cyber attacks will be preceded by an attack that will first create samples or behaviour that look malicious, but are in fact benign. By pushing the defender to deal with a flood of false positives, it will result in automatic recalibration from its new unsupervised learning.

certis

But A.I. is Great when it Helps Security Automation

Why do we need automation?

- Save cost and reduce reliance on manpower and resources
- With the influx of attack attempts, human beings just can't keep up
- Double Gain: By remediating fast, the damage is reduced and the cost of repairs will be considerably contained

While still in its infancy, with most vendors just a year or two old, there are already some promising technologies:

- A.I. Deep Learning to empower Attacks and log analysis
- Software Defined Perimeter/Protection
- Automated Intelligence Monitoring and Threat Hunting
- Automated Pentesting and Report Remediation
- Automated Forensic Analysis

certis

A.I. is One of Many New Cyber Security Innovations that We Need to Pursue

- A.I. is like precision surgery
- For wellbeing and holistic healthcare, many more components would be needed, e.g. Deception, Security by Design
- We need to take a strategic approach that will embed A.I. as a key enabler

Security by Design is Strategic

Continuous Monitoring/ Audit,
Security Integration (Big Data),
AI Security Automation

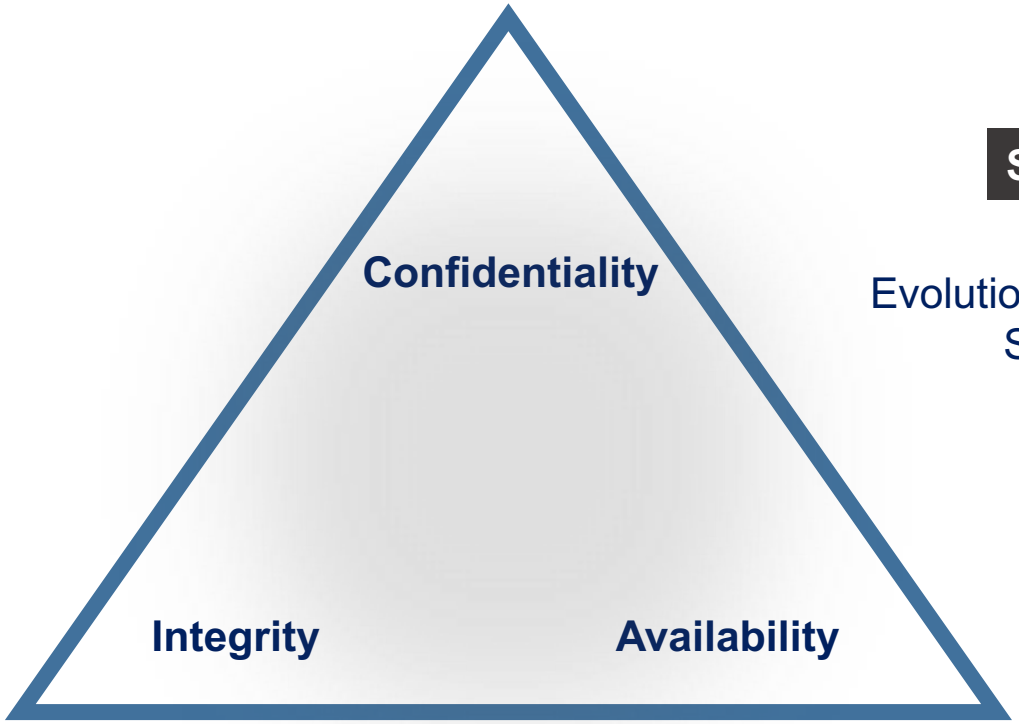
Security by Design

Automated Testing, e.g. A.I. fuzzing,
Deception/Honeynets,
Self defending models,
Autonomous Object Security

Security by Learning

Security by Construction

Zero Knowledge (ZK),
MultiPartyComputation,
Tokenisation,
Trustzone Intel SGX



Evolutionary Discovery e.g. Chaos Monkey,
Software Defined Constructs,
Resilient Cloud

Privacy by Design

Resiliency by Design

Conclusion

Cyber Security A.I. is not going to bring us Nirvana

- A.I. is going through “teething” pains.
- It takes time to get the right data to train A.I. systems well.
- A.I. requires a highly advanced and modern infrastructure for its optimal Big Data deployment. This will have to come first.
- The best that we can manage today is side-by-side operations with humans and therefore, a new type of interface for Cyber Security Operations Centre would be needed. This is still work in progress.
- For the security industry to get the most out of A.I., we need to recognise what machines do best and what people do best.

Conclusion

- Today’s narrow AI can make mistakes, leading to very serious and fatal safety and security issues.
- Thus, there is a need for new standards to manage embedded AI.