The Insecurity of Things

OR…

"The unexpected security consequences of cats, flaps and programming mishaps"

Leigh Chase, IBM Emerging Tech.

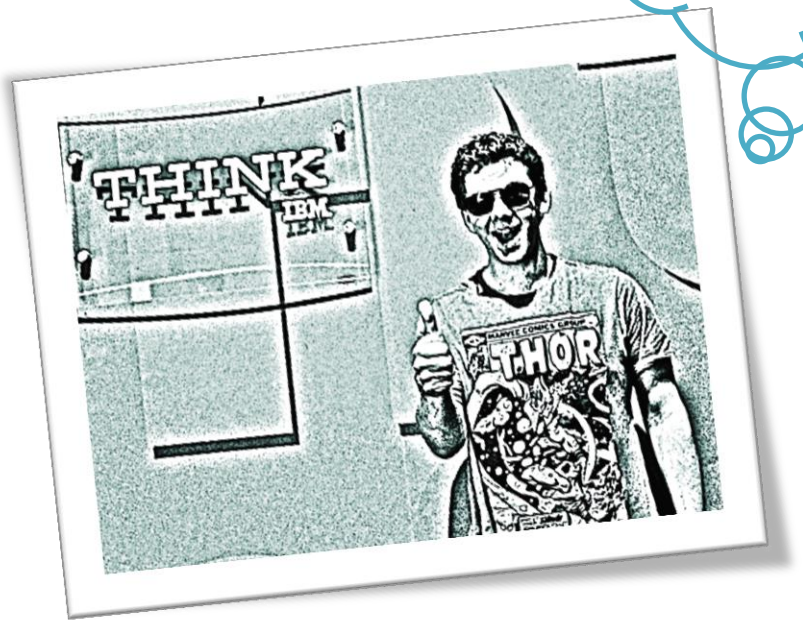
Hursley House

24th March 2017

I’m here to tell you a story

- “Schrödinger's cat flap and the unlikely case of the IBM Q”
- We will see how IoT computing can lead to some highly unexpected ‘security outcomes’
- We’re going to show how IoT provides ‘Security Agency’ and a cat can quantum compute

A story has to have characters…

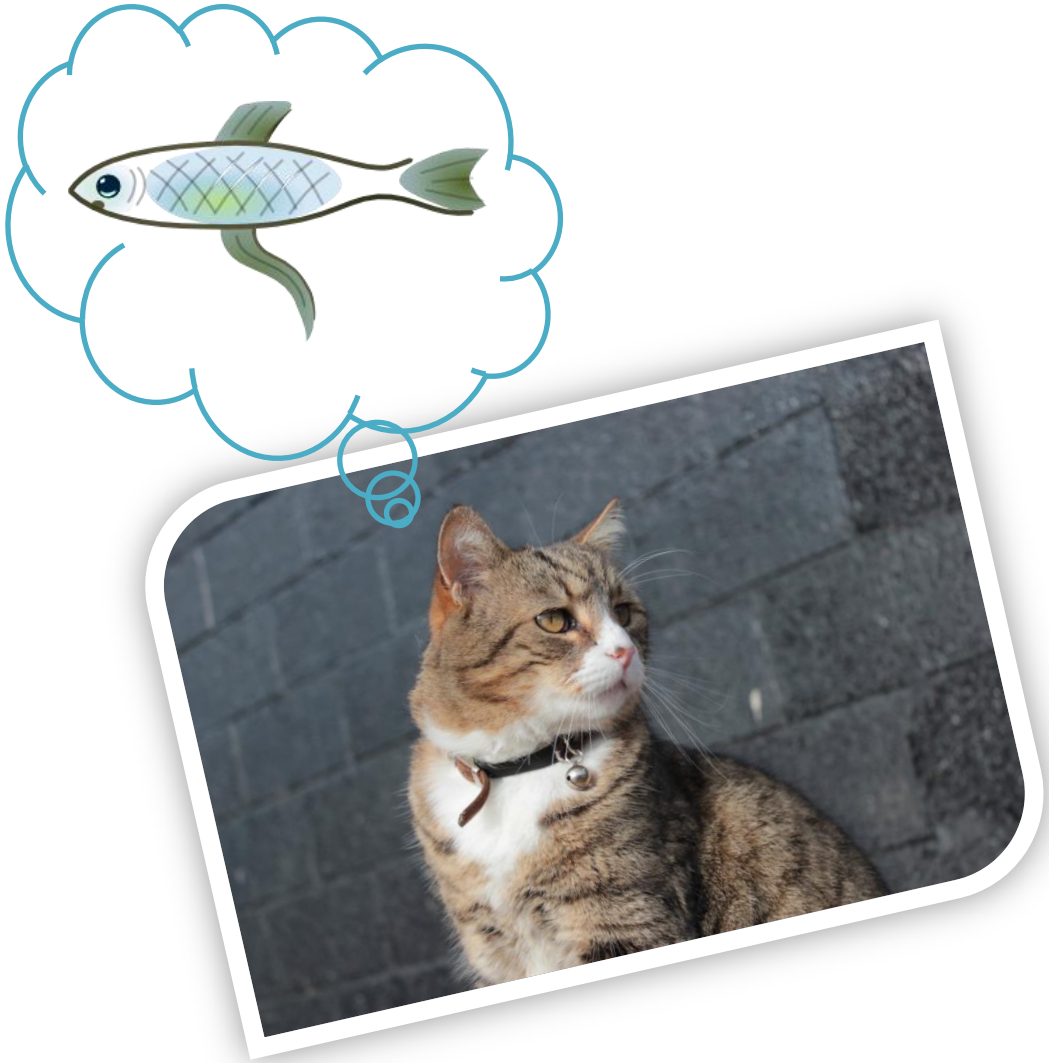


P=NP?

Leigh

IBMer, Computer Scientist

Emerging Technology



Elgar

Felis Catus (Cat)

Own agenda

Cookie

Felis Catus (Cat)

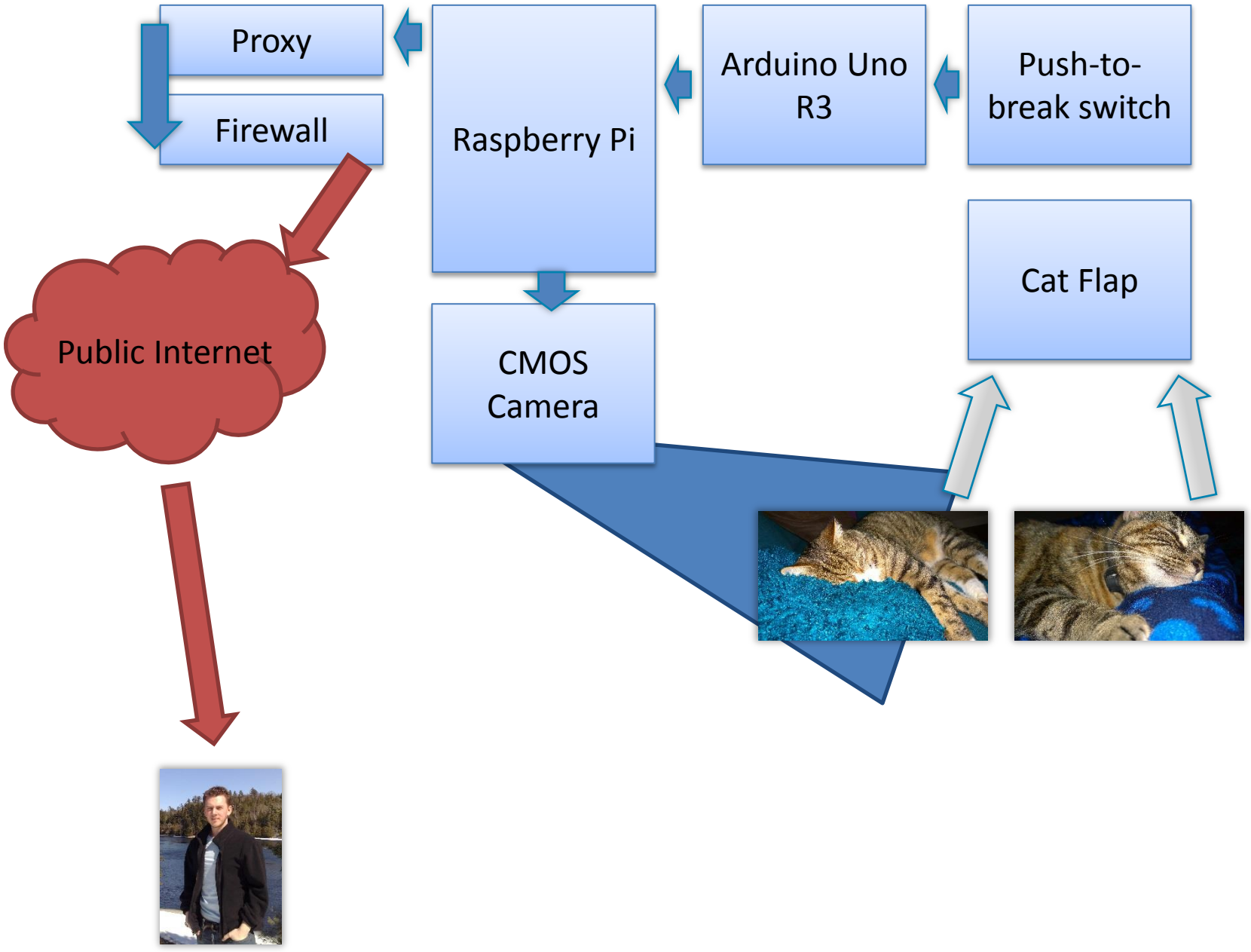
Stares at walls

And so our story begins…

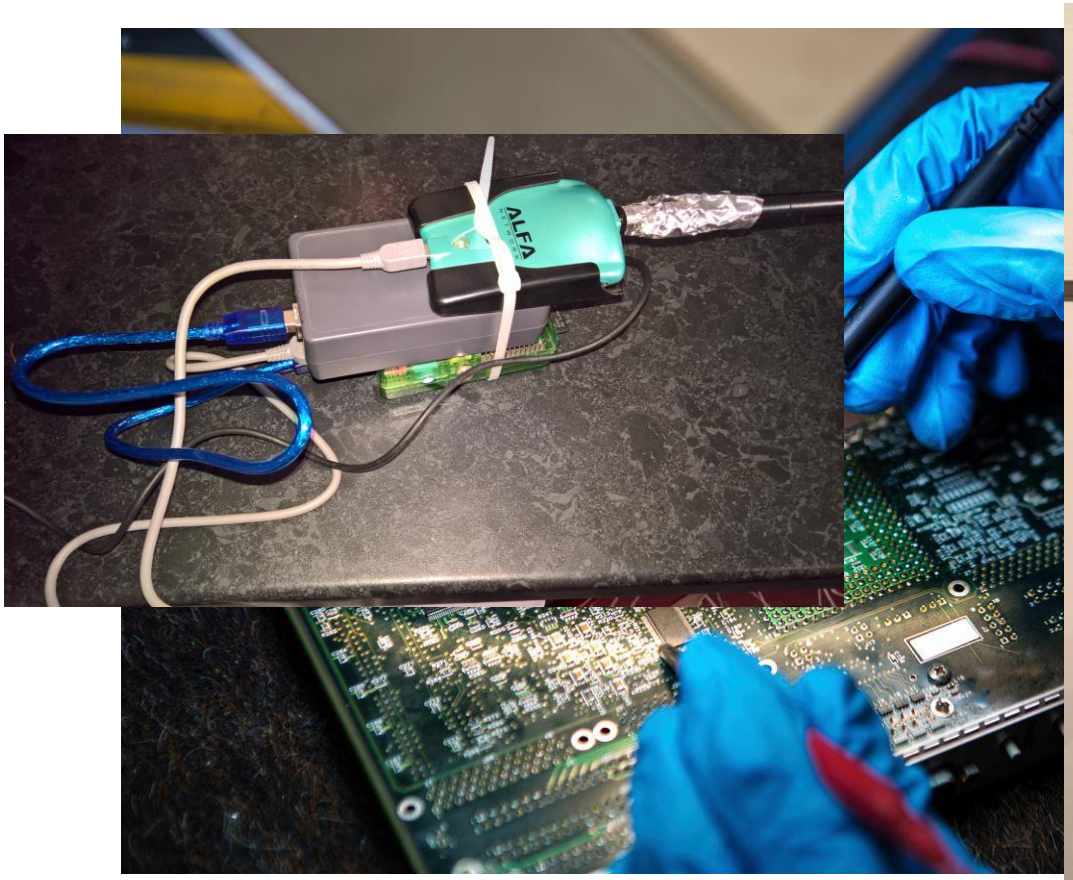
Feline Intrusion Detection System

- Cats invade houses like unwelcome packets within a network
- So in essence, this is really just a network intrusion detection problem
- Isn't it?

The Mk1


Proxy
Firewall
Raspberry Pi
Arduino Uno R3
Push-to-break switch
Cat Flap
Public Internet
CMOS Camera

Rapid ~~Engineering~~ Prototyping



Wiring it all together

- The sheer inventiveness and creativity of the IoT sector is phenomenal
- Within just a few years the area has seen rapid developments in
  - Sensor networking
  - Decision making
  - Modular computing
- With applications in all market sectors

However

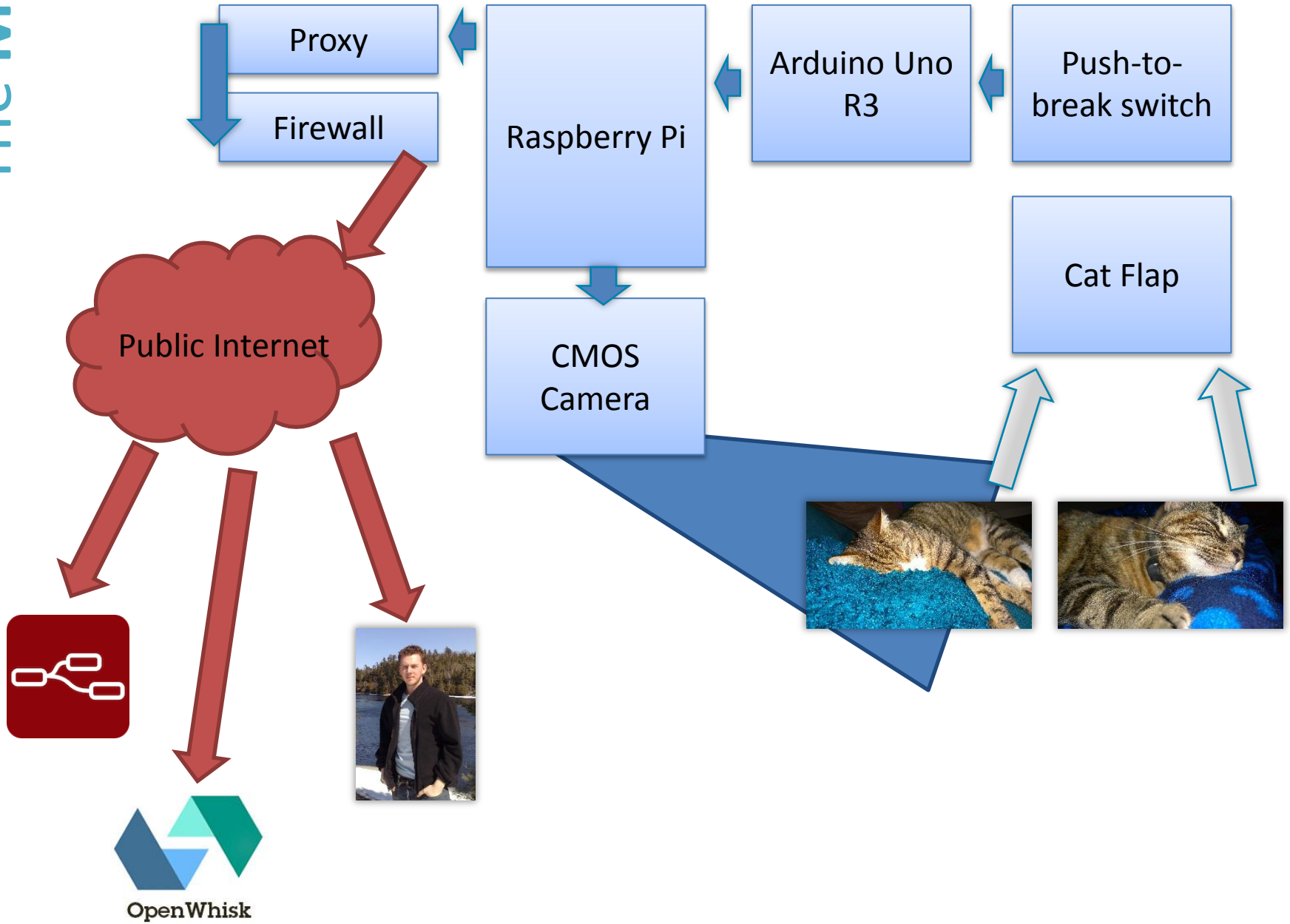
- With great power…
- IoT clearly requires us to think differently about security – specifically data-centric models and moving away from decades of assumptions generated by monolithic IT

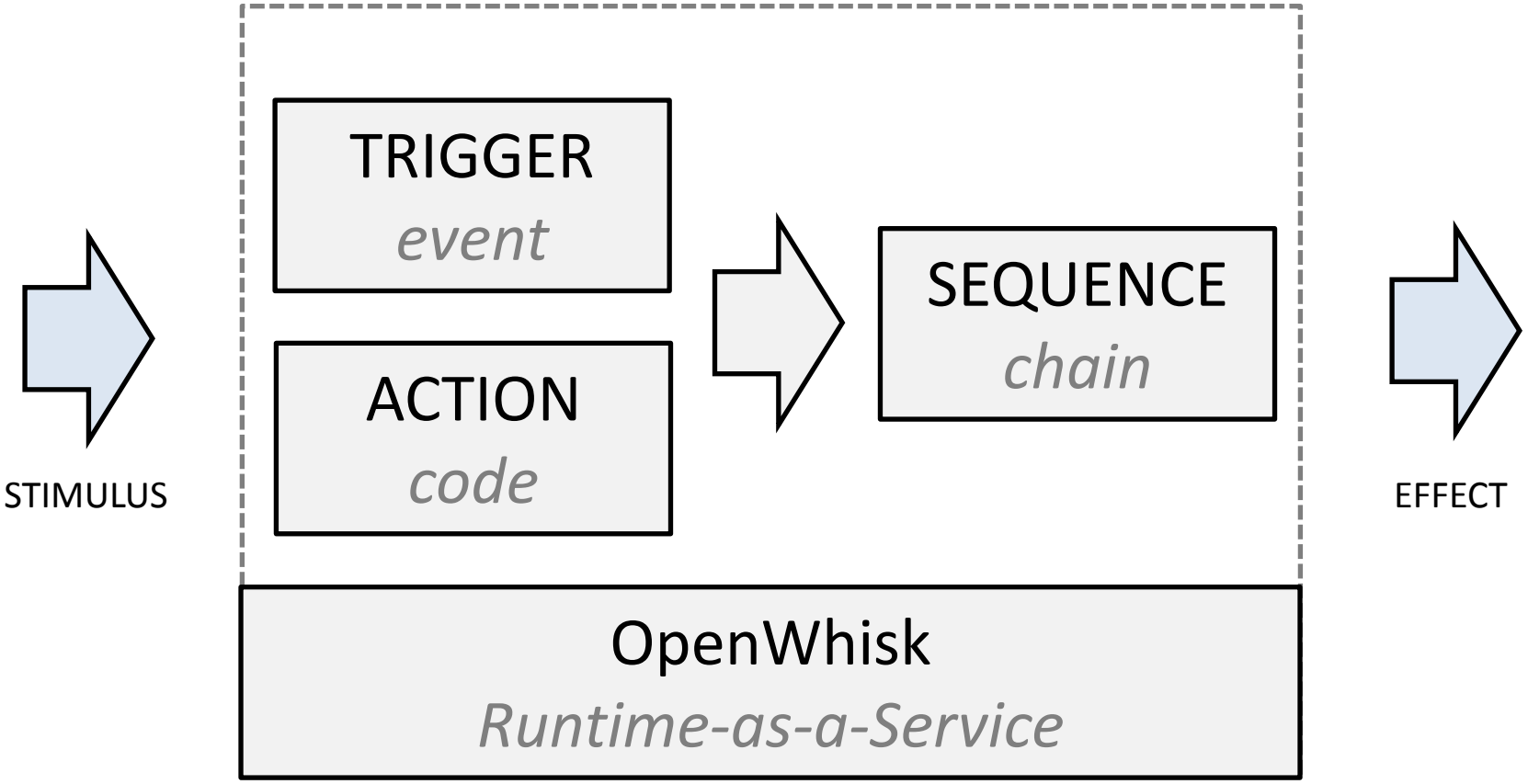
Inspiration strikes…

IoT for Event-Driven Security

- Using IoT-inspired sensor networks, we can blend physical-world events and interactions with logical-world effects and outcomes
- Applications in cyber-physical systems, digital forensics, network security, security automation, intelligence acquisition and management, distributed security policies…
- '**Security Agency**' through instrumentation

The Mk2


Proxy
Firewall
Raspberry Pi
Arduino Uno R3
Push-to-break switch
Cat Flap
Public Internet
CMOS Camera
OpenWhisk


TRIGGER
event
ACTION
code
SEQUENCE
chain
STIMULUS
EFFECT
OpenWhisk
Runtime-as-a-Service

IoT for Event-Driven Security

```
var request = require('request');

function main(params) {
   var location = params.location || 'Winchester';
   var url = 'https://query.yahooapis.com/v1/public/yql?q=select item.condition from weather.forecast where
woeid in (select woeid from geo.places(1) where text="' + location + '")&format=json';

   return new Promise(function(resolve, reject) {
      request.get(url, function(error, response, body) {
         if (error) {
            reject(error);
         }
         else {
            var condition = JSON.parse(body).query.results.channel.item.condition;
            var text = condition.text;
            var temperature = condition.temp;
            var output = 'It is ' + temperature + ' degrees in ' + location + ' and ' + text;
            resolve({msg: output});
         }
      });
   });
}
```

Harnessing the Power of Serverless and RESTful APIs

- It was doing this that I broke my router…
  - *and* kernel panicked the Pi
  - *and* made snort light up (like ‘Vegas)
  - *and* upset my Squid web proxy

Back to the Notepad…

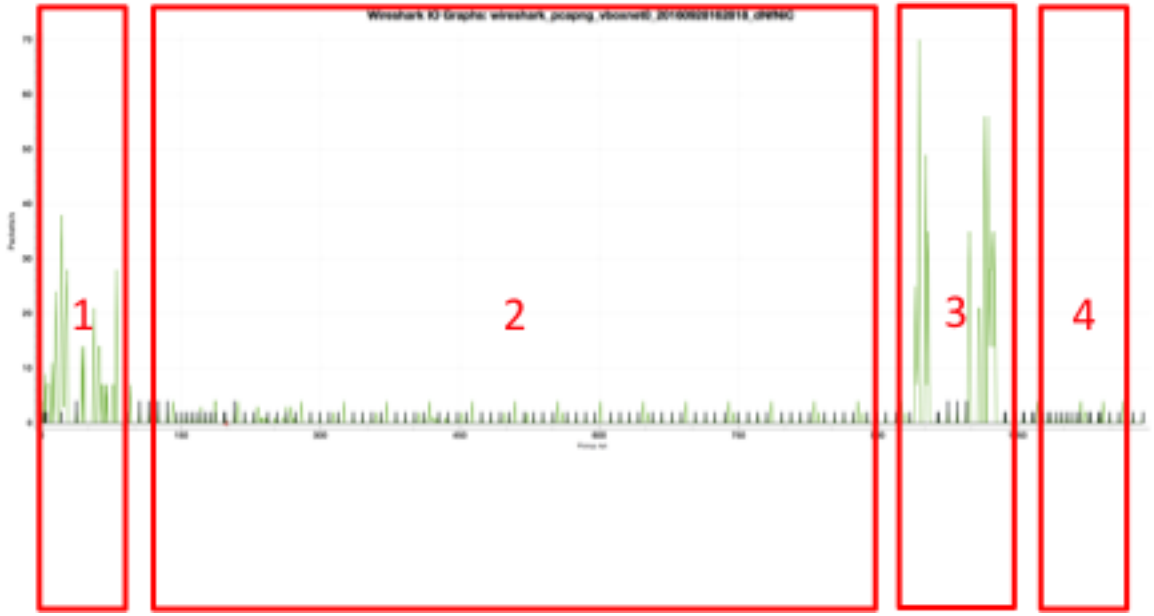
- Managing scale and demand
- Understanding the system's telemetry up-front
- Handling errors and input properly (ish)
- Proper third-party service integration

Thinking it Through (doing it properly, ish)

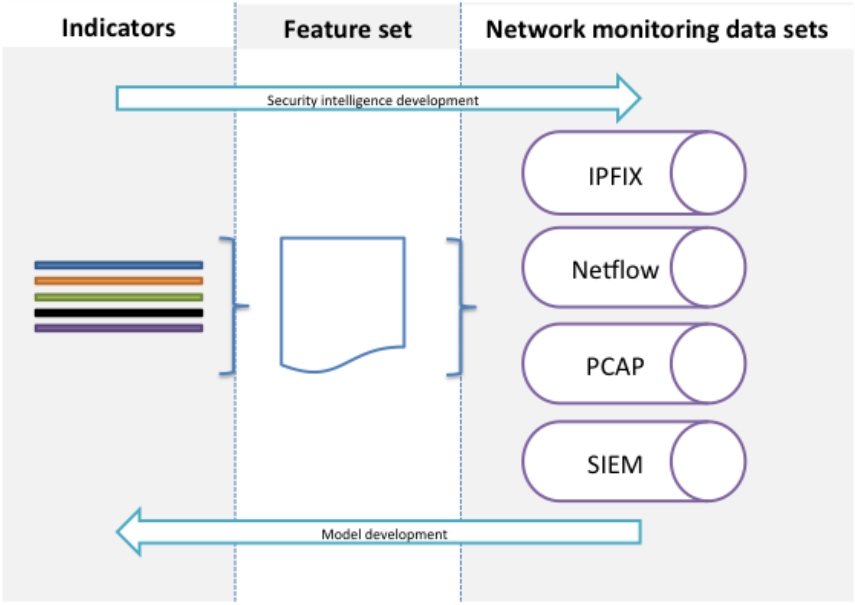
- The flexibility of IoT platforms promises much for *proper* security use-cases
- Extending this approach, we can integrate complex security systems – such as the X-Force Information Exchange
- However we also see the risks and challenges

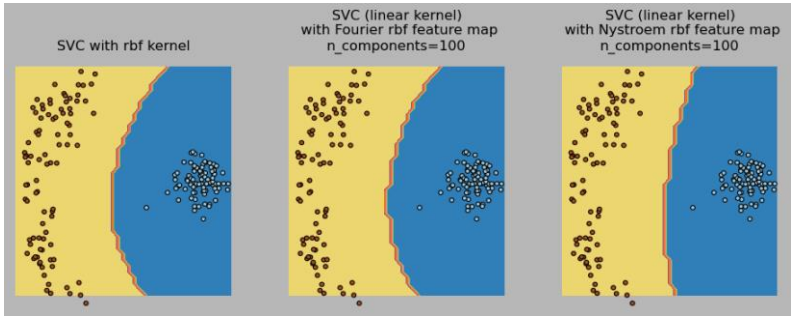
IoT for the (security) Win

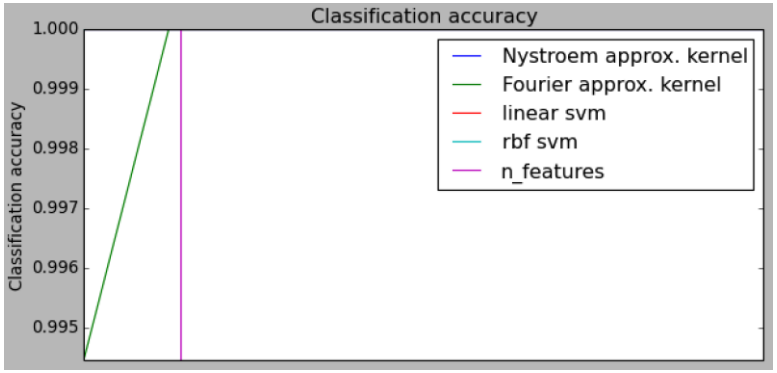
- Using some IBM ET prior art, we can use this same approach to fix another kind of intrusion-case



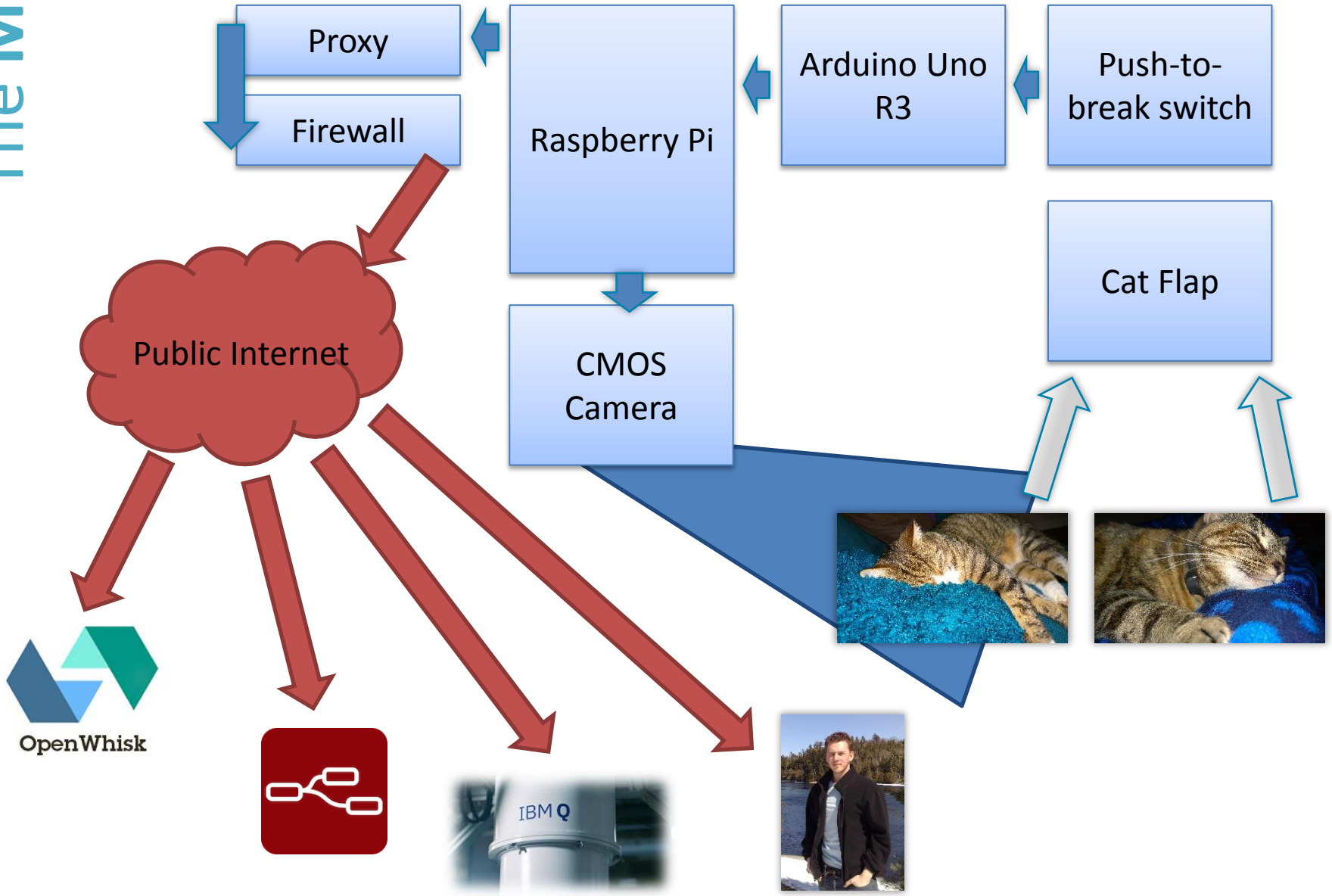
IoT for the (security) Win

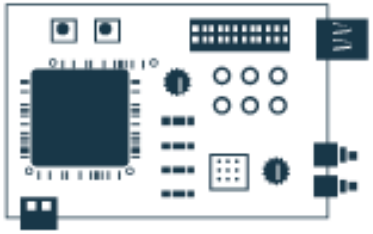






The Mk3


Proxy
Firewall
Raspberry Pi
Arduino Uno R3
Push-to-break switch
Cat Flap
Public Internet
CMOS Camera
OpenWhisk
IBM Q



Your device or gateway

We start with your device, be it a sensor, a gateway or something else.
To find out how to get it connected, search our recipes.

MQTT

Your device data is sent securely up to the cloud using the open, lightweight MQTT messaging protocol.

IBM Internet of Things Foundation

This is the hub of all things IBM IoT. This is where you can setup and manage your connected devices so that your apps can access their live and historical data.

REST & Real-time APIs

Use our secure APIs to connect your apps with the data coming from your devices.

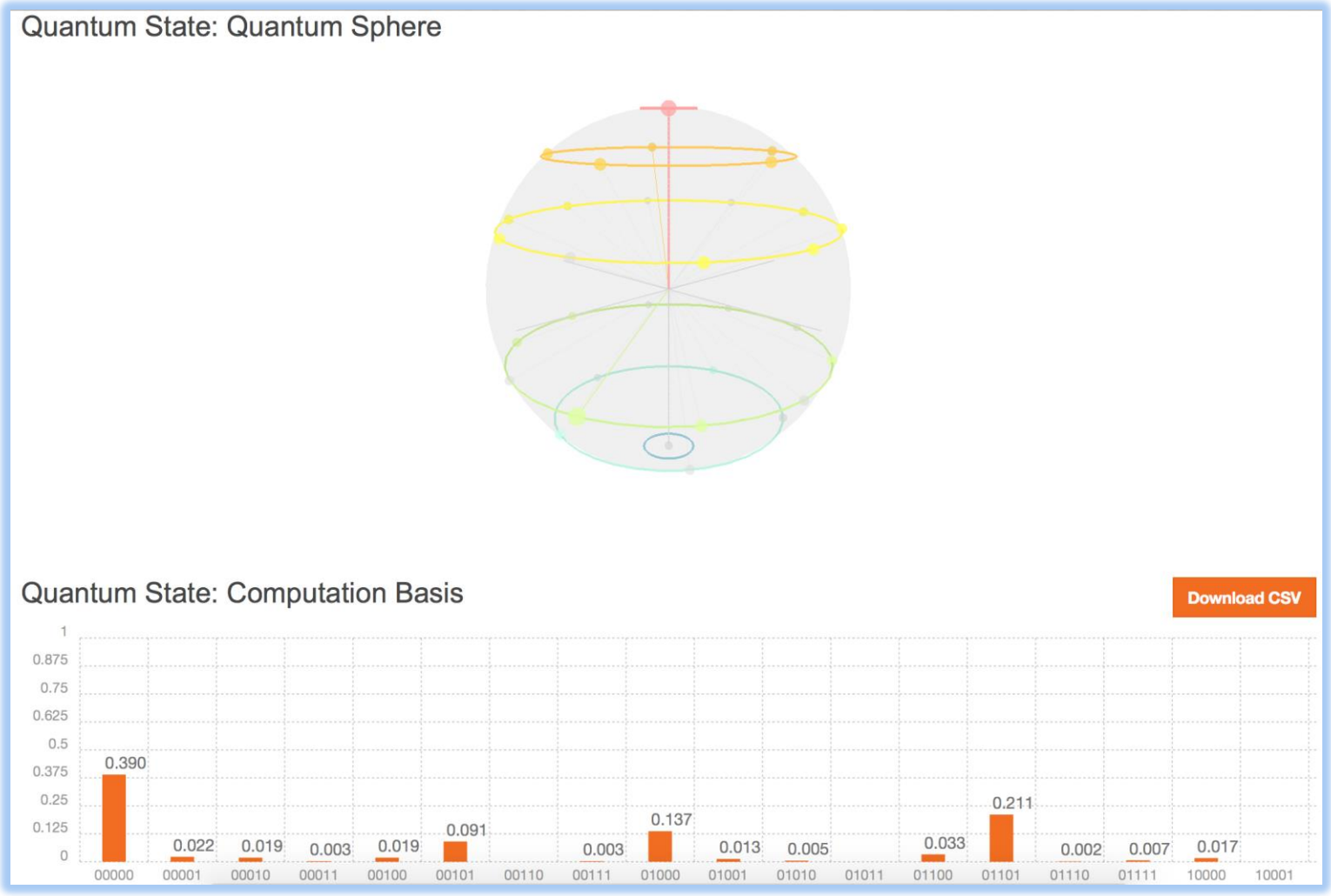
Your application and analytics

Create applications within IBM Bluemix, another cloud,
or your own servers to interpret the data you now have access to!

Cat-driven Quantum Computing

- The final extension is integration with the IBM Q – a 5-qubit universal Quantum Computer
- From a security standpoint, this is about as experimental as it gets
  - Untested, rapidly prototyped code
  - Cheap, distributed IoT kit
  - Bleeding-edge non-von Neumann machine architectures
  - Under developed use-case…

When Elgar met Shor



In conclusion?

- Using IoT devices, serverless computing and APIs we combined physical and logical events to create specific outcomes

- IoT techniques have massive potential within cyber security – specifically through exploitation of the event-driven paradigm

In conclusion?

- We see the potential for breaking things in new and original ways
- Security models for IoT will need to be different – cyber physical systems and Security Agency
- Oh… and we detected unauthorised feline guests

Alfie

```
(!=Elgar && !=Cookie)
```