COMS3000/7003

Week 13

Cloud Computing Security,
Industrial Control Systems (ICS) Security
Internet of Things (IoT) Security, Summary

David Ross

Industry Lectures Again Today

Mark McPherson, CISO, YDF

Mark is an IT specialist, with 26 years' experience, including 18 years as a security analyst, educator & manager at both of Australia's National CERTs, and senior positions advising Federal, State & Local Government agencies, national and international telecommunications providers, utilities, banks, universities and other critical infrastructure organisations.

Mark is experienced in developing and implementing critical information security management policy and organisational security culture. His roles have included National Security Policy Manager and International Training & Conferences Manager. Mark has also occupied several board & steering committee positions of international organisations collaborating on global incident response.

Tue 24/10/2017 2:09 PM

Aaron Whittaker <Aaron.Whittaker@microsoft.com>

ConsenSys Australia are launching the Summer Intern Program

To Ross, David

Hello David,
I came across this and thought one of your students may be interested. I know Peter and can give one/some of your students a great introduction.

ConsenSys Australia are launching the Summer Intern Program. Applications are closing soon, read below for more details.

ABOUT CONSENSYS

ConsenSys is a venture production studio focused on building and scaling tools and enterprise software products powered by Ethereum. Our mission is to use these solutions to power the emerging economic, social, and political operating systems of the planet. Our teams are busy at work building the future of identity, financial markets, commerce, security and infrastructure, and more.

About the role:

This paid internship (US$4.5K / month) will allow the intern to develop highly sort after skills developing in the Ethereum ecosystem. The four internships are:

- Ethereum Based Application: Contribute to an Ethereum based project, Rental dApp, a Solidity contract and React front end to manage rent for the Code Cave. It allows Cave residents to 'sign' a 'lease' for a weekly rental amount, deposit Ether, and have a fixed amount deducted from escrow each week, based on the current AUD/ETH rate (uses an Oracle). The front end shows who is up to date with payments and who is behind.
- Zero Knowledge Proof Testing: Create and contribute to the libsnark open source project a set of test vectors for the gadget primitives such as SHA256 in the libsnark library.
- Zero Knowledge Proof Use-Case Development: Create and contribute to the libsnark open source project one or more non-trivial example usages of the libsnark library.
- Quorum Testing: Create and contribute to the quorum and go-ethereum open source projects additional tests to improve the test coverage of quorum and go-ethereum.

About you:

- Pursuing a Bachelor's degree or higher degree in computer science or related field, or have graduated in the last two years.
- High level of enthusiasm and interest in the Ethereum ecosystem.
- High degree of accountability and maturity
- A minimum of ten (12) continuous weeks' availability for internship during the period November 2017 to February 2018.

If you are someone that thrives in a fast-paced environment where being self-directed, determined, and resilient are a requirement, we would love for you to join us. To be considered, please email your resume, cover letter, and a transcript of your academic record to peter.robinson@consensys.net .

Thanks,

Microsoft | Aaron Whittaker | Service Delivery Manager
Mob +61 490 074 501 | aaronw2003
awhitt@microsoft.com

Course Evaluations

If not done yet, please also comment on guest lecturers – good/bad? – more? – or less?

SECaT

Opens Monday
16th October

This email has been sent to all listed course coordinators and teaching staff for Semester 2, 2017.

WHAT HAPPENS ON MONDAY?

For the majority of courses and lecturers, students will be invited to participate in online SECaT evaluations on Monday 16 October (Week 12). In order to minimis the release of SECaTs will be staggered throughout the day between 6:00am and 7:30pm. You can download the SECaT release schedule from SECaT Release

Students will receive one email per batch with direct links to the SECaTs. Students can also access the SECaTs via the Blackboard "Have Your Say" module whic screen of Blackboard. Reminders will be sent to students who have not responded on Saturday 21 October, Thursday 26 October, and Tuesday 31 Oct, and mos November at 11:59pm.

Please note: This email has been sent to all ECP listed Course Coordinators.

Dear: Dr David Andrew Ross,

We thought you may appreciate an update on how your course SECaT responses are tracking. As at 4:00pm today (Mon 23 Oct), the response rates for your c

Course: COMS3000, Class: 60735, Response Rate: 09.4% (n=10/106)
Course: COMS7003, Class: 60729, Response Rate: 23.5% (n=4/17)

Key Information for Sem 2, 2017

For the majority of courses, the first reminder was sent to students who had not responded on Sat 17 Oct. Additional reminders will be sent to students on Thur and Tuesday 31 Oct (every 5 days). The reminder schedule can be viewed at:

http://itali.uq.edu.au/filething/get/8588/SECaT-Release-Schedule-Sem-2-2017.pdf

How can Students Access their SECaTs?

Students can access links to your SECaT survey/s via the email we send them or via the "Have Your Say" block within Blackboard at https://learn.uq.edu.au/. F this block (example below) can appear anywhere within their Blackboard homepage.

BRIDGE POINT

"SECURE NETWORKING"

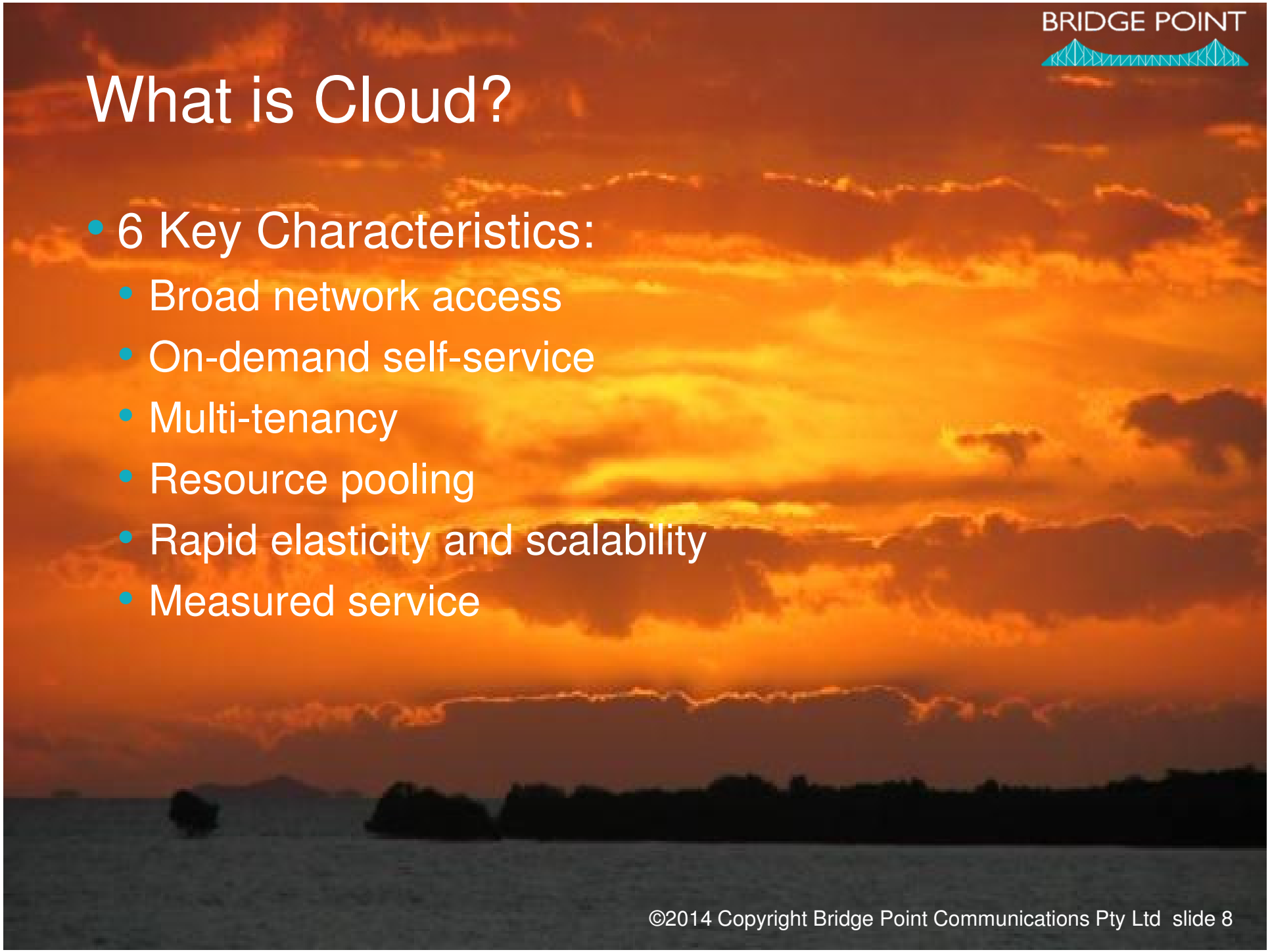
Cloud Computing

And the new ISO/IEC and ITU-T Standards

cloud computing:

- paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with on-demand self-service provisioning and administration

ISO/IEC 17788:2014 Information technology — Cloud computing — Overview and vocabulary



What is Cloud?

- 6 Key Characteristics:
  - Broad network access
  - On-demand self-service
  - Multi-tenancy
  - Resource pooling
  - Rapid elasticity and scalability
  - Measured service

Broad network access

"A feature where the physical and virtual resources are available over a network and accessed through standard mechanisms that promote use by heterogeneous client platforms.

The focus of this key characteristic is that **cloud computing** offers an increased level of convenience in that users can access physical and virtual resources from wherever they need to work, as long as it is network accessible, using a wide variety of clients including devices such as mobile phones, tablets, laptops, and workstations."

ISO/IEC 17788:2014 Information technology — Cloud computing — Overview and vocabulary

On-demand self-service

"A feature where a **cloud service customer** can provision computing capabilities, as needed, automatically or with minimal interaction with the **cloud service provider**.

The focus of this key characteristic is that **cloud computing** offers users a relative reduction in costs, time, and effort needed to take an action, since it grants the user the ability to do what they need, when they need it, without requiring additional human user interactions or overhead."

ISO/IEC 17788:2014 Information technology — Cloud computing — Overview and vocabulary

Multi-tenancy

"A feature where physical or virtual resources are allocated in such a way that multiple **tenants** and their computations and data are isolated from and inaccessible to one another. Typically, and within the context of **multi-tenancy**, the group of **cloud service users** that form a **tenant** will all belong to the same **cloud service customer** organization. There might be cases where the group of **cloud service users** involves users from multiple different customers, particularly in the case of **public cloud** and **community cloud** deployments. However, a given **cloud service customer** organization might have many different tenancies with a single **cloud service provider** representing different groups within the organization"

ISO/IEC 17788:2014 Information technology — Cloud computing – Overview and vocabulary

multi-tenancy

- multi-tenancy: allocation of physical or virtual resources such that multiple tenants and their computations and data are isolated from and inaccessible to one another
- tenant: group of cloud service users sharing access to a set of physical and virtual resources

ISO/IEC 17788:2014 Information technology — Cloud computing — Overview and vocabulary

Resource pooling

"A feature where a **cloud service provider's** physical or virtual resources can be aggregated in order to serve one or more **cloud service customers**.
The focus of this key characteristic is that **cloud service providers** can support **multi-tenancy** while at the same time using abstraction to mask the complexity of the process from the customer. From the customer's perspective, all they know is that the service works, while they generally have no control or knowledge over how the resources are being provided or where the resources are located. Even with this level of abstraction, it should be pointed out that users might still be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter)"

ISO/IEC 17788:2014 Information technology — Cloud computing — Overview and vocabulary

Rapid elasticity and scalability

"A feature where physical or virtual resources can be rapidly and elastically provisioned, in some cases automatically, to quickly increase or decrease resources. For the **cloud service customer**, the physical or virtual resources available for provisioning often appear to be unlimited and can be purchased in any quantity at any time, subject to constraints of service agreements. Therefore, the focus of this key characteristic is that **cloud computing** means that the customers no longer need to worry about limited resources and might not need to worry about capacity planning. From the customers' perspective, if new resources are needed, they are available automatically, immediately, and can appear to be infinite, subject to constraints of service agreements."

ISO/IEC 17788:2014 Information technology — Cloud computing – Overview and vocabulary

Measured Service

"A feature where the metered delivery of **cloud services** is such that usage can be monitored, controlled, reported, and billed. This is an important feature needed to optimize and validate the delivered **cloud service**.

The focus of this key characteristic is that the customer may only pay for the resources that they use.

From the customers' perspective, **cloud computing** offers the users value by enabling a switch from a low efficiency and asset utilization business model to a high efficiency one."

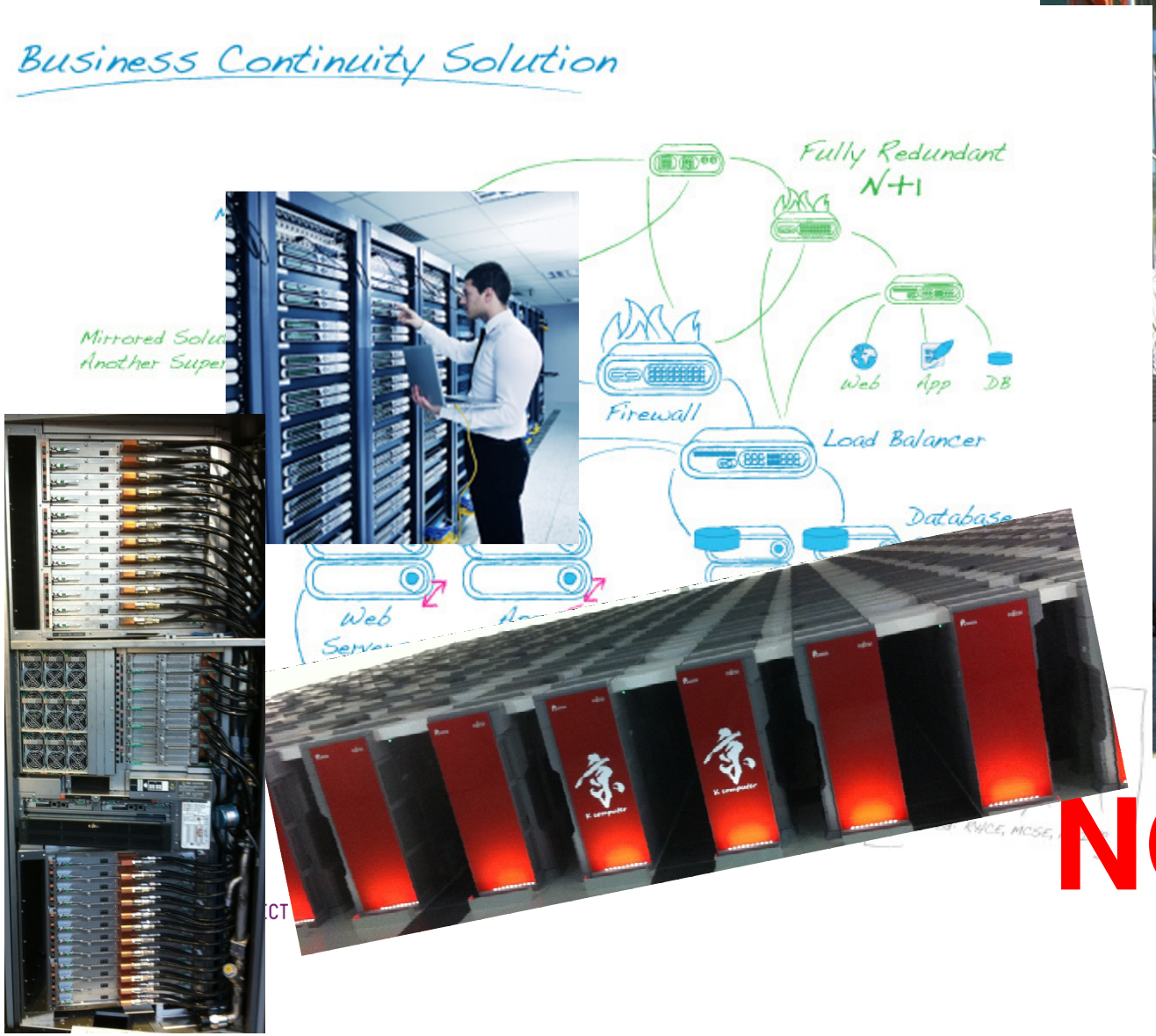
ISO/IEC 17788:2014 Information technology — Cloud computing — Overview and vocabulary

cloud service[1]:

one or more capabilities offered via **cloud computing** (3.2.4) invoked using a declared interface

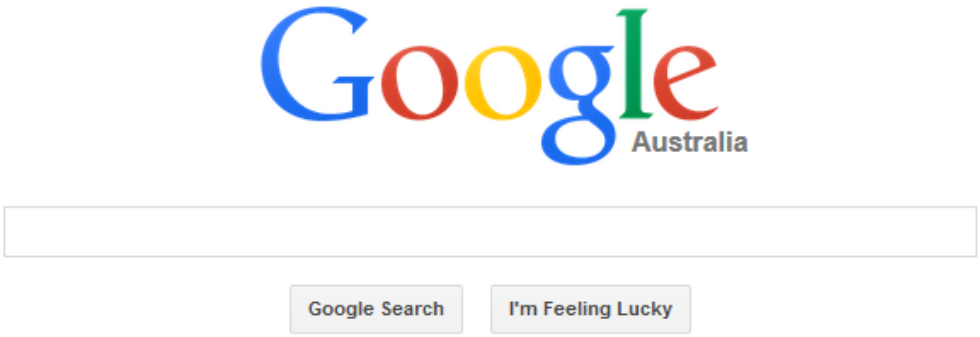
[1] ISO/IEC 17788:2014 Information technology — Cloud computing — Overview and vocabulary

Managed Services



NOT cloud

On-Demand Self-Service



CLOUD

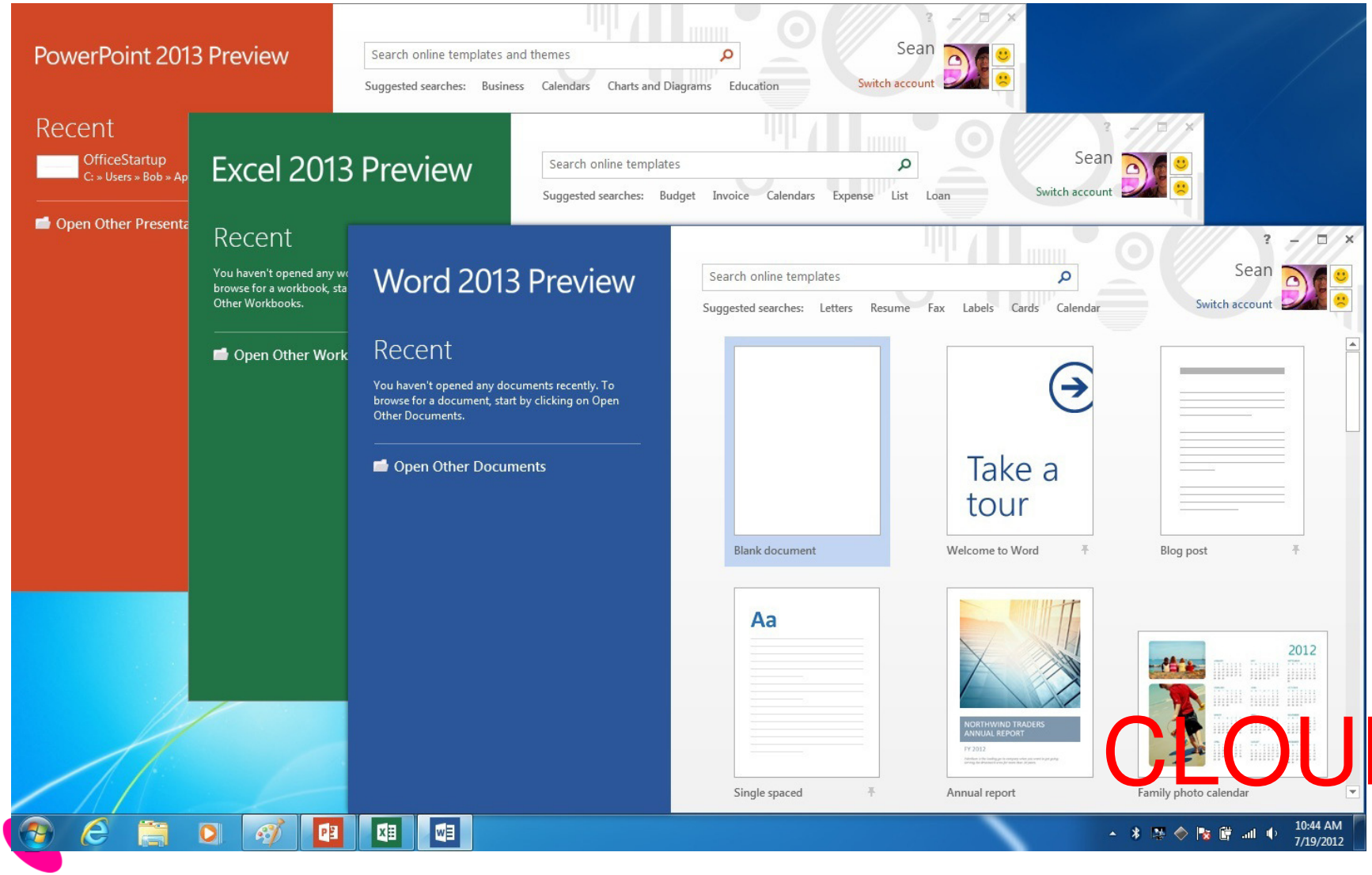
IT'S HOW
WE CONNECT

On-Demand Self-Service

CLOUD

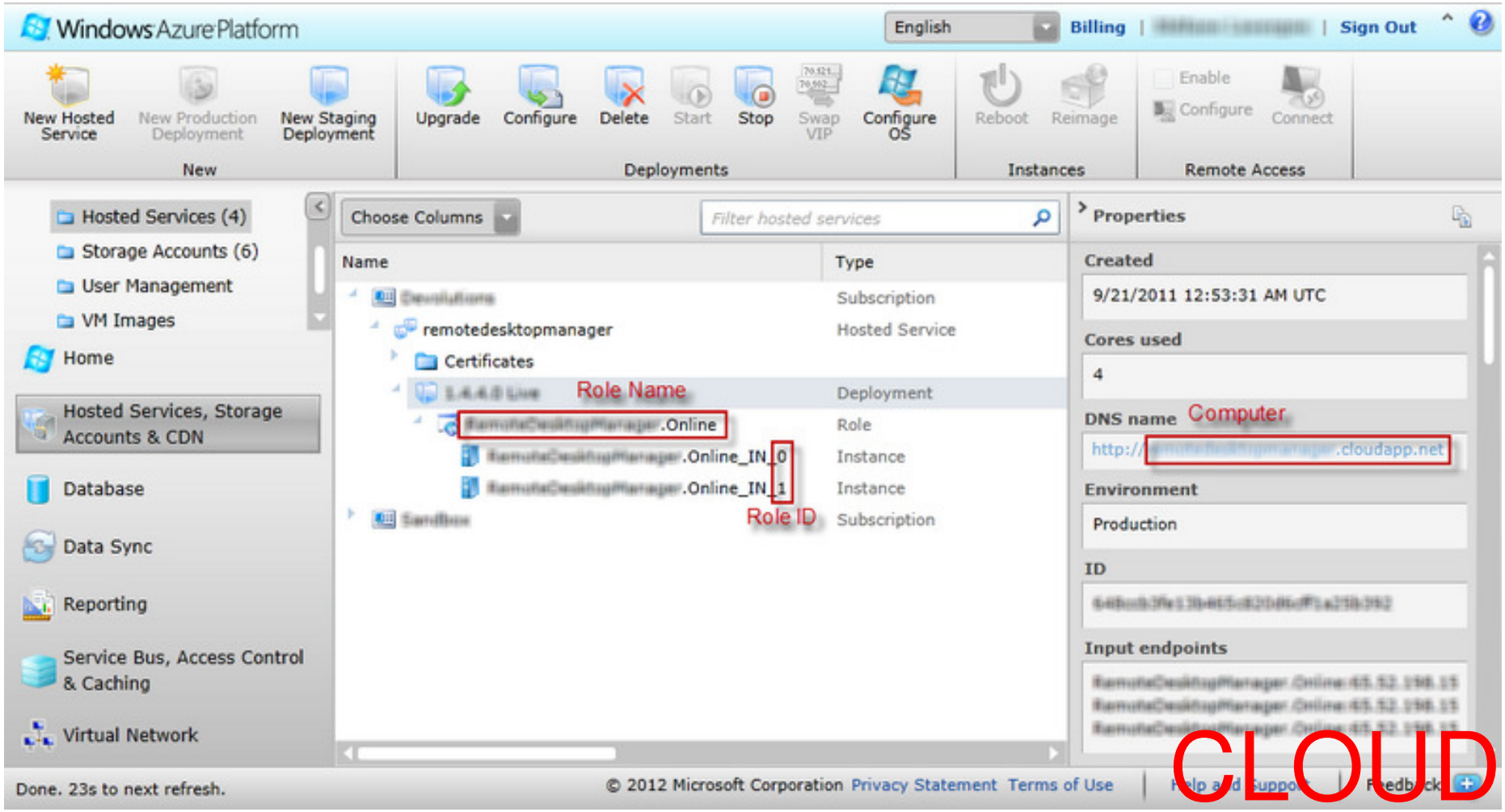
IT'S HOW
WE CONNECT

On-Demand Self-Service



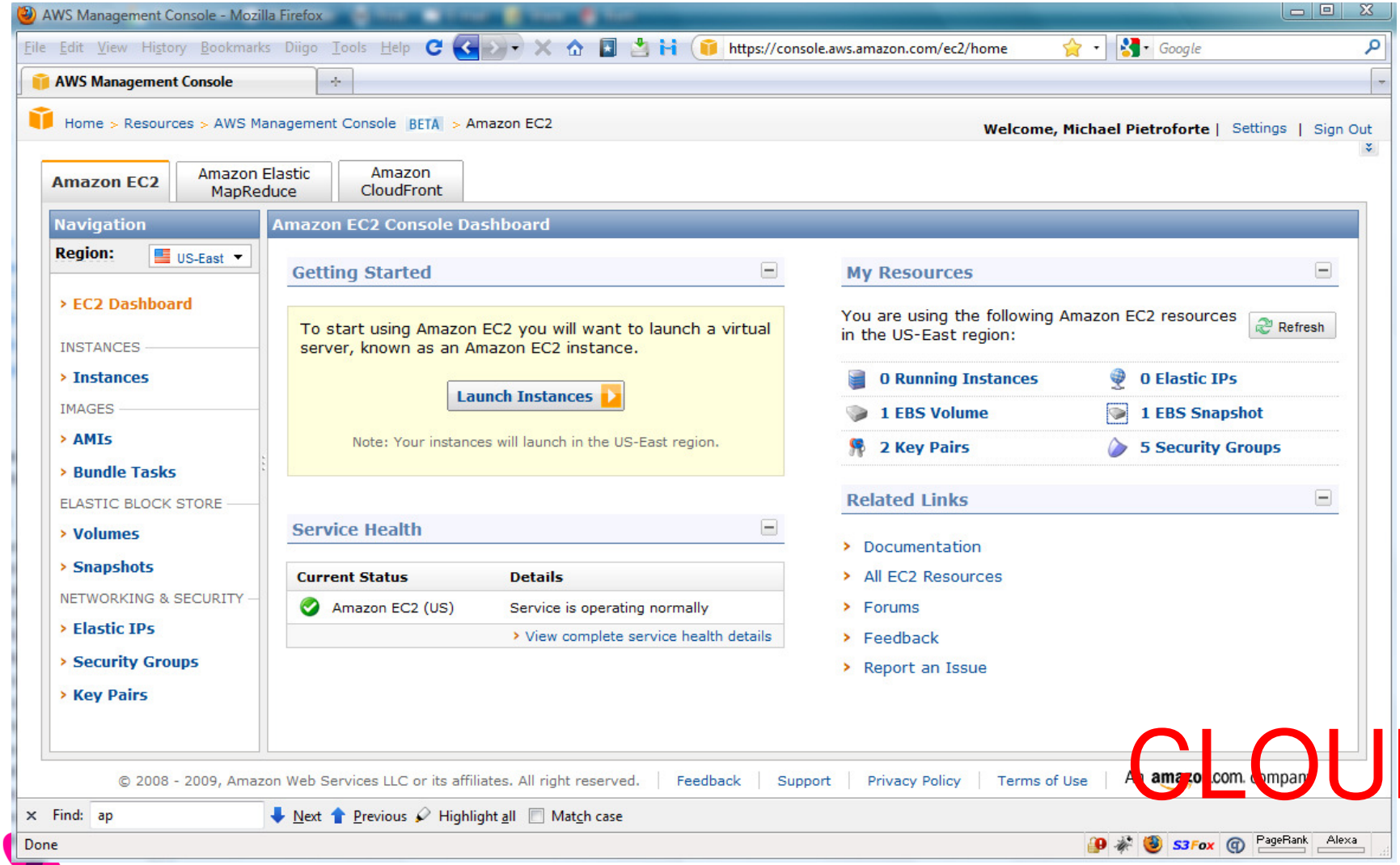
CLOUD

On-Demand Self-Service



IT'S HOW WE CONNECT

On-Demand Self-Service



CLOUD

ISO/IEC 17788 Overview & Vocabulary

- Lots of Definitions
- 6 Key Characteristics
- 4 Deployment Models
- 3 Cloud Capabilities Types

Cloud computing roles and activities

- **cloud service provider:**
  party which makes **cloud services** available
- **cloud service customer:**
  party which is in a business relationship for the purpose of using **cloud services**
- **cloud service user:** natural person, or entity acting on their behalf, associated with a **cloud service customer** that uses **cloud services**
  - NOTE – Examples of such entities include devices and applications.

ISO/IEC 17788:2014 Information technology — Cloud computing — Overview and vocabulary

4 Deployment Models

- Public Cloud
- Private Cloud
- Community Cloud
- Hybrid Cloud

3 Service Models →"Capabilities Types"

- Original 3 "Service Models" (NIST):
  - Infrastructure-as-a-Service (IaaS),
  - Platform-as-a-Service (PaaS), and
  - Software-as-a-Service (SaaS).

3 NIST Service Models → Capabilities Types

- NIST Service Models now abstracted to 2 levels:
  - A multitude of **Cloud Service Categories** are based on
    - The three core **Cloud Capabilities Types**
  - Three "Capabilities Types" (ISO 17788):
    - **Infrastructure Capabilities Type**,
    - **Platform Capabilities Type**, and
    - **Application Capabilities Type**.
  - And many "Cloud Service Categories", including:
    - Infrastructure-as-a-Service (IaaS),
    - Platform-as-a-Service (PaaS), and
    - Software-as-a-Service (SaaS).

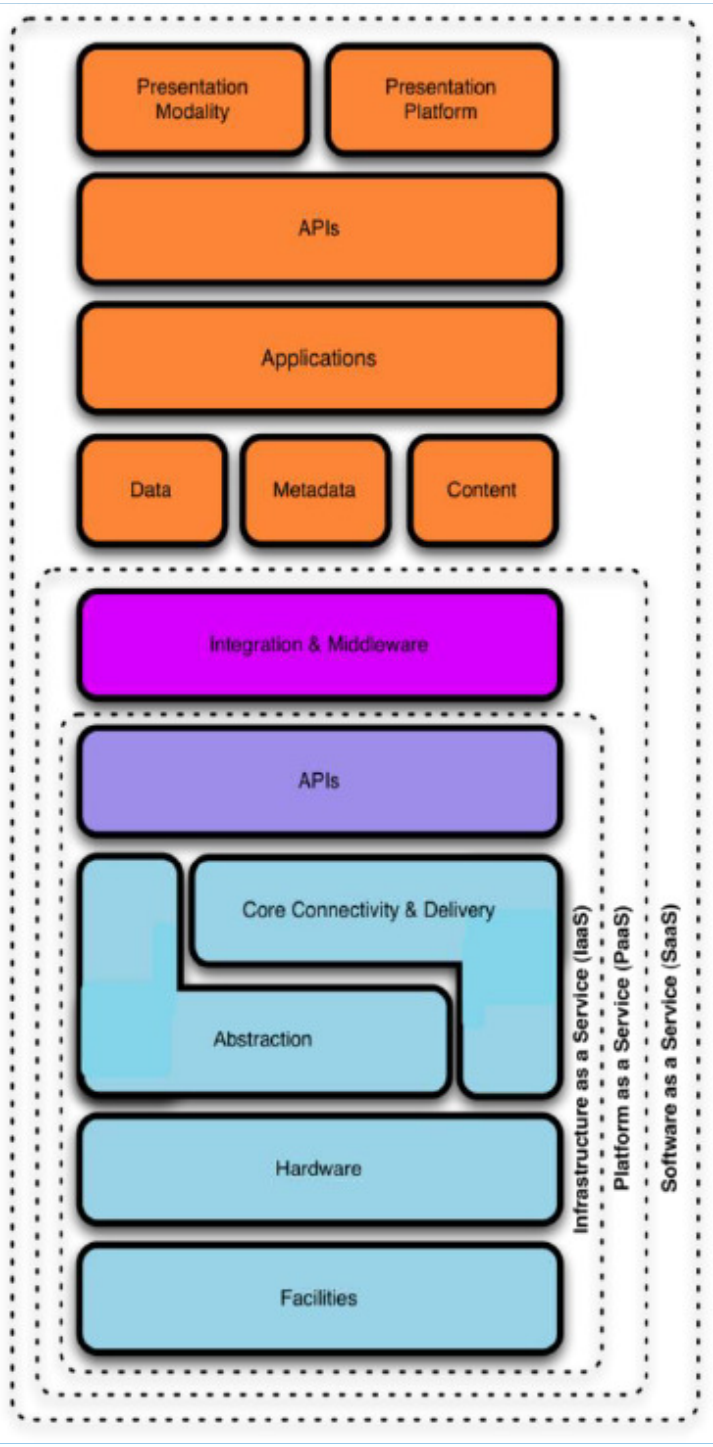
Cloud Service Categories & Cloud Capabilities

Cloud Service Categories	Cloud Capabilities Types		
	Infrastructure	Platform	Application
Software as a Service			X
Platform as a Service		X	
Infrastructure as a Service	X		
Network as a Service	X	X	X
Data Storage as a Service	X	X	X
Compute as a Service	X		
Communication as a Service		X	X

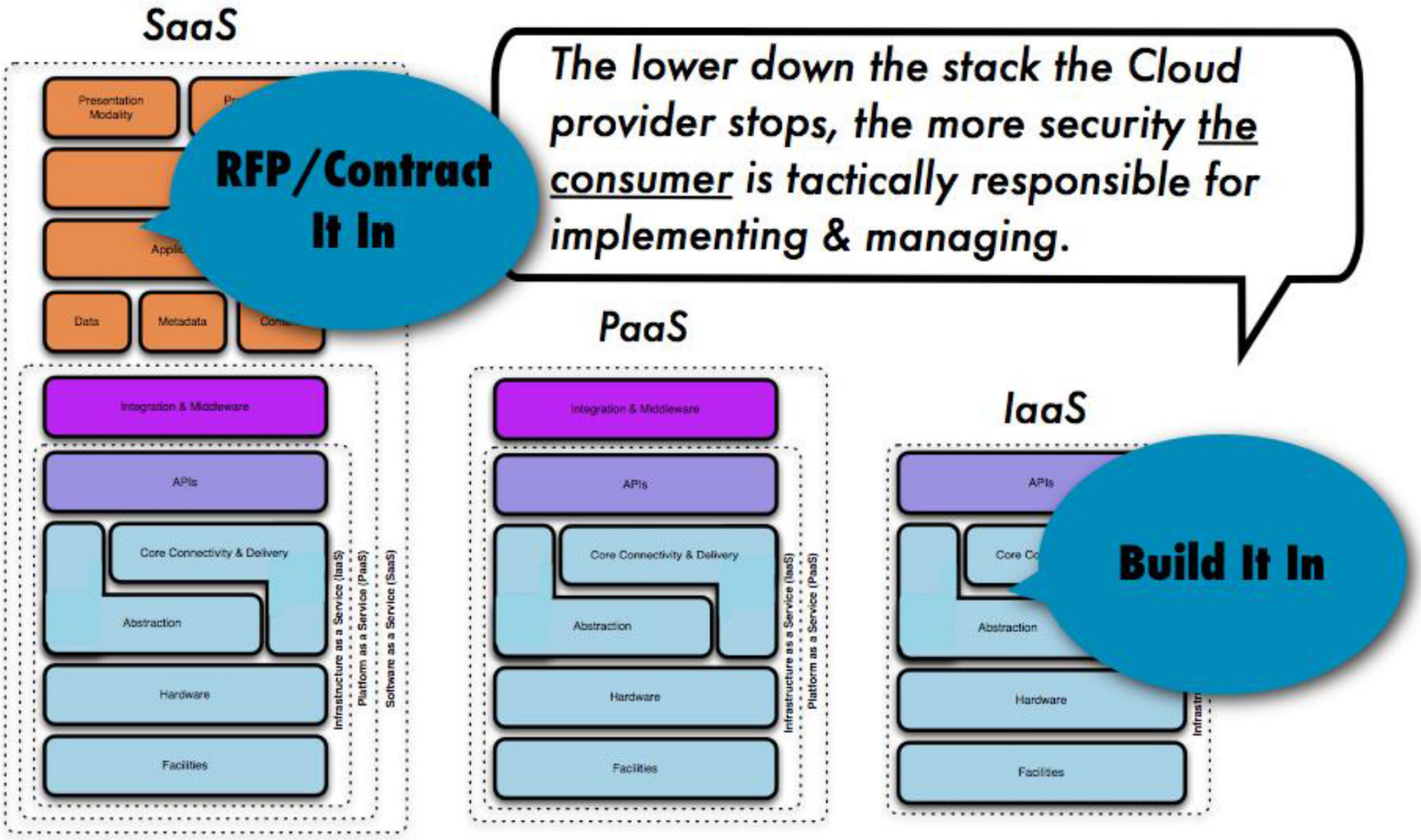
Cloud Security?

Cloud Security Alliance (CSA)

CSA Cloud Security Architecture



CSA: Security Integration



Facilities: at the base of the stack

- Recall Aaron Whittaker's lecture in week 6
  - Microsoft Azure Cloud Datacentres
  - The Three Levels of Separation
- Basic requirements to secure IaaS
  - Therefore to secure PaaS and SaaS
  - Physical security: facilities and hardware
  - Personnel security – "HR security"

Edge Computing

- Performing data processing at the edge of the network
  - Distributed, decentralised architecture
  - “Big Data on small devices”
  - “Performing analytics and knowledge generation at or near the source of the data”
  - Reduces the bandwidth needed to transfer data between the devices and the datacentre

ISO/IEC JTC/1 SC38 TR on Edge Computing Landscape

Report on the concept of Edge Computing, its relationship to Cloud Computing and IoT, and the technologies that are key to the implementation of Edge Computing.

ISO/IEC JTC/1 SC38 TR on Edge Computing Landscape

This report will explore the following topics with respect to Edge Computing:

- Concept of Edge Computing Systems
- Architectural Foundation of Edge Computing
- Edge Computing Terminology
- Software Classifications in Edge Computing – e.g. firmware, services, applicati
- Supporting technologies such as Containers, Serverless, Microservices
- Networking for edge systems, including virtual networks
- Data – data flow, data storage, data processing in edge computing
- Management – of software, of data, of networks, resources, quality of service
- Virtual placement of software and data, and metadata
- Security and Privacy
- Real Time
- Mobile Edge Computing, Mobile Devices

Any questions so far?

Industrial Networking and Critical Infrastructure

Industrial Networking

- Factory floor
- Process plant
- Control systems
- Security systems
- Wireless networks
- Integrated with company enterprise network
- Managed and unmanaged switches, routers, gateways, segment repeaters, and monitoring and configuration software

Telstra Security Services – a note on: Industrial Control Systems (ICS), The Internet of Things (IoT)

STUDENT USE ONLY – NOT APPROVED FOR PUBLIC RELEASE

David Ross

Managing Consultant – Security Practice

March 2016

IT'S HOW WE CONNECT

Industrial Controls Systems (ICS)
including
Supervisory Control And Data Acquisition (SCADA)

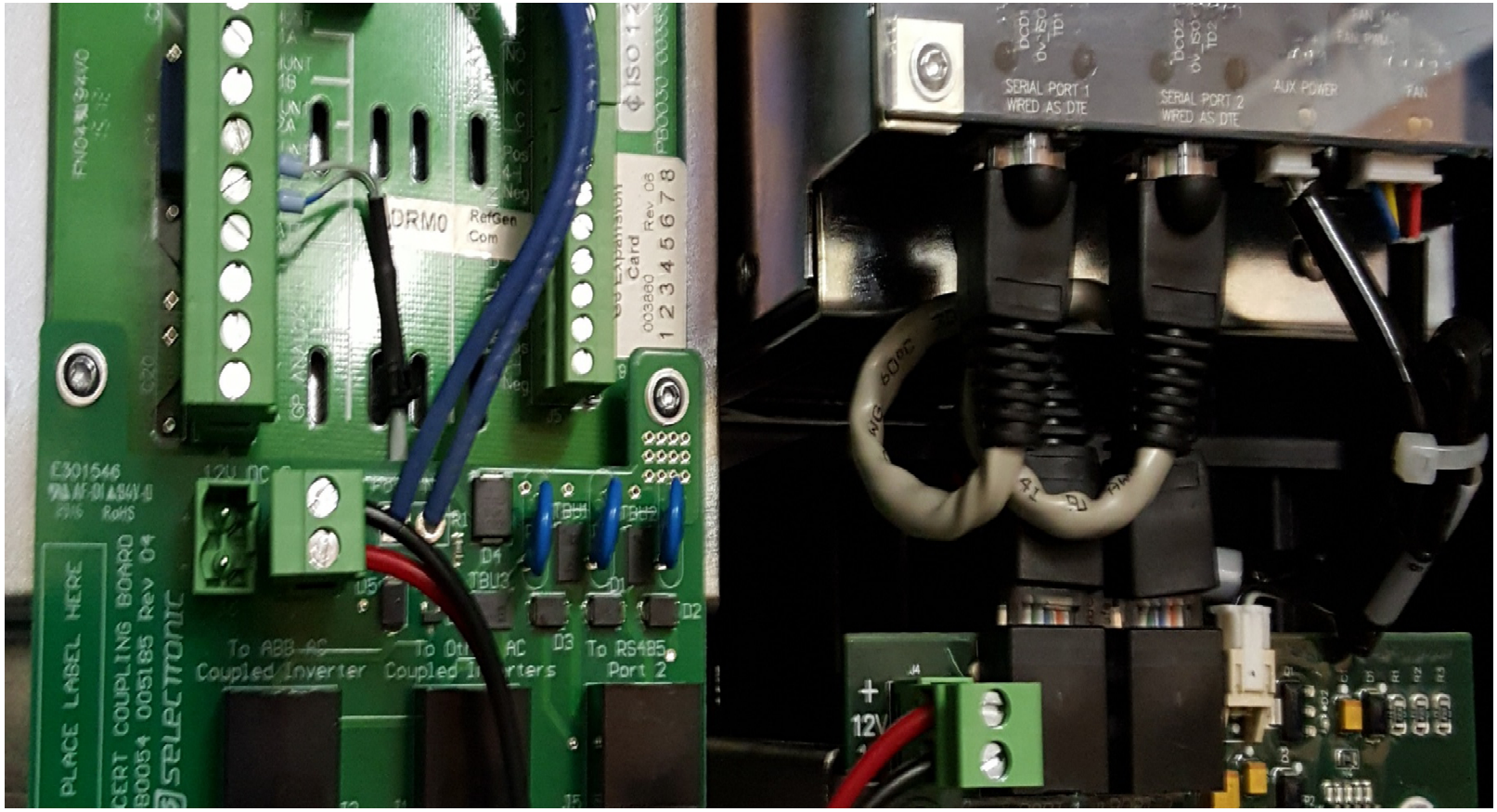
IT'S HOW
WE CONNECT

Information Security in the Dirt

or alternately … Information Security in REALLY BIG machines

IT'S HOW
WE CONNECT

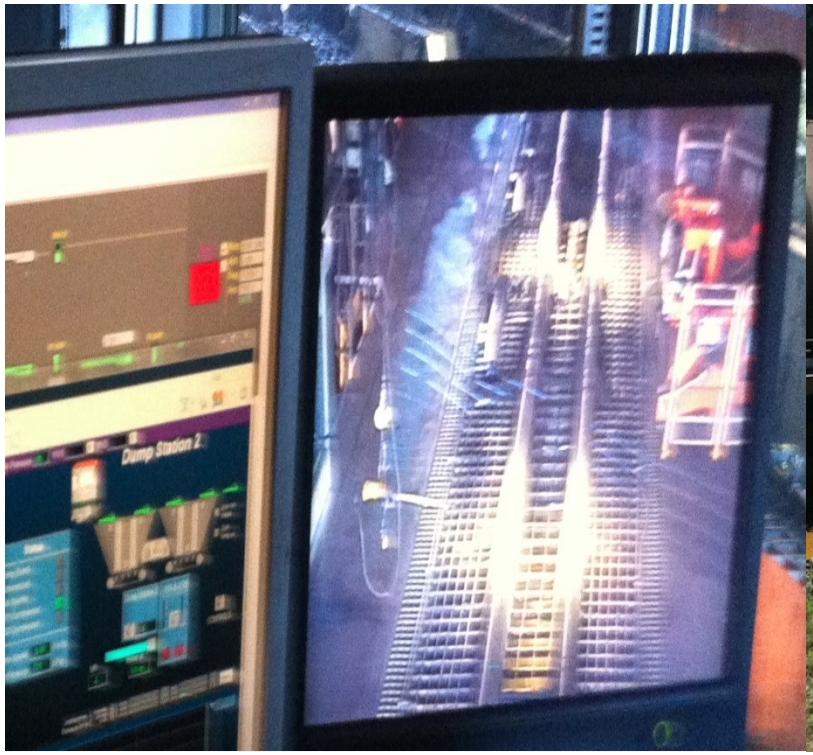
Or in the factory…



MODBUS over RS485 and over Ethernet

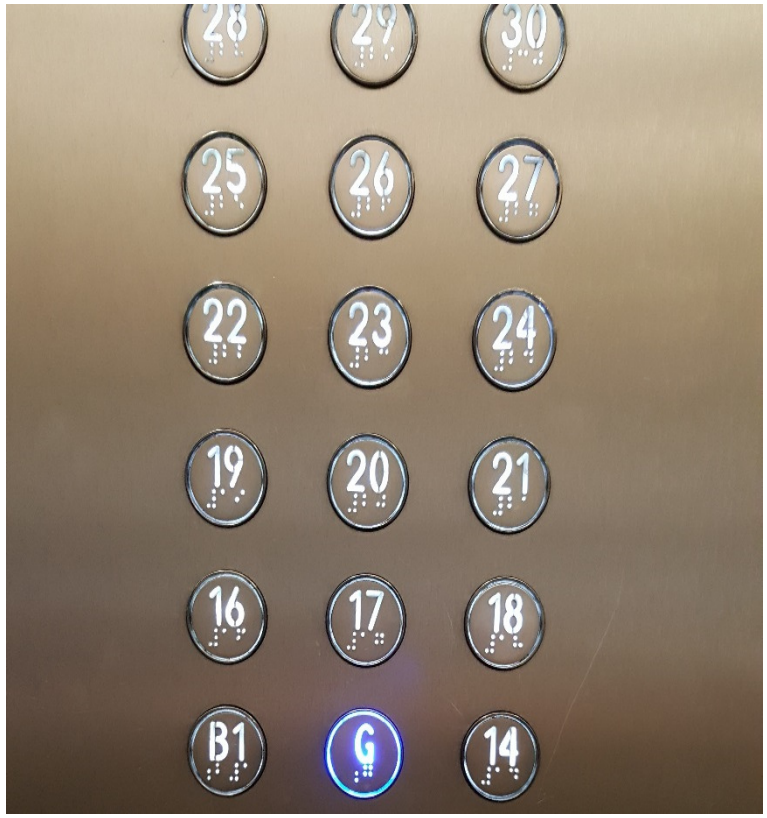
IT'S HOW WE CONNECT

Or in transport…



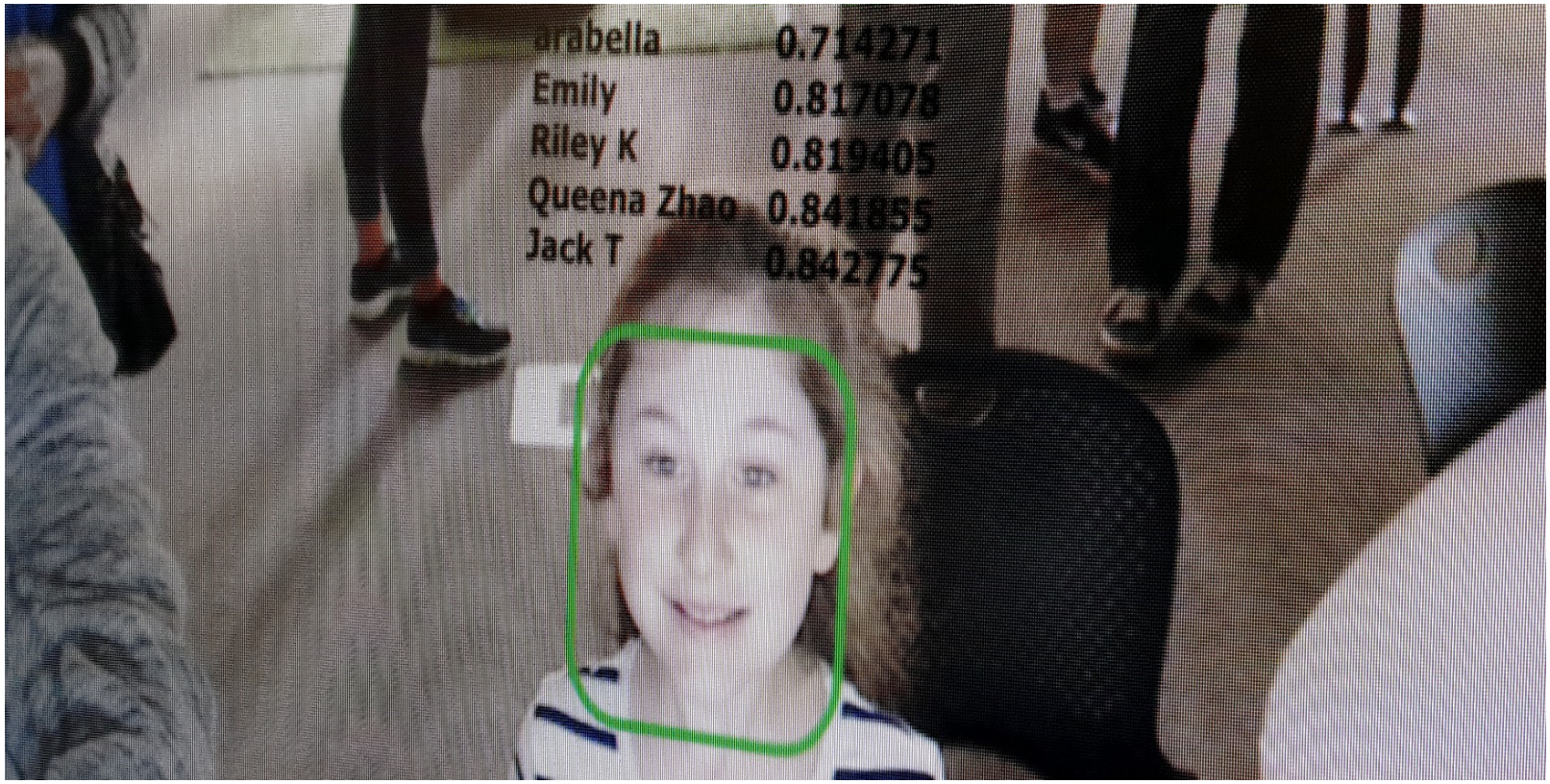
Rail and road traffic management systems

Or in your buildings



IT'S HOW
WE CONNECT

Or your security systems themselves



Draglines have many computers

And still more – a Core2Duo 1.2GHz

Our team understand the standards

IEC 62443 / ISA-99

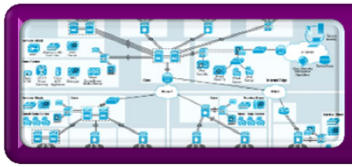
NIST SP800-53 & 82

SANS CSC

What we do

Security Architecture and Design

- IT-OT Interfaces, Business Zone, DMZ, Operations, PCN
- Enforcement zones (Purdue Model)

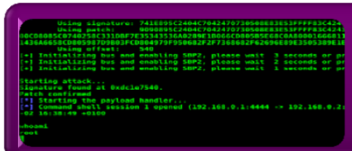


Network Design and Installation

- Networks Team
- Industrial Grade Equipment

Security Assessments

- Gap Analyses
- Compliance Audits



Vulnerability and Penetration Testing

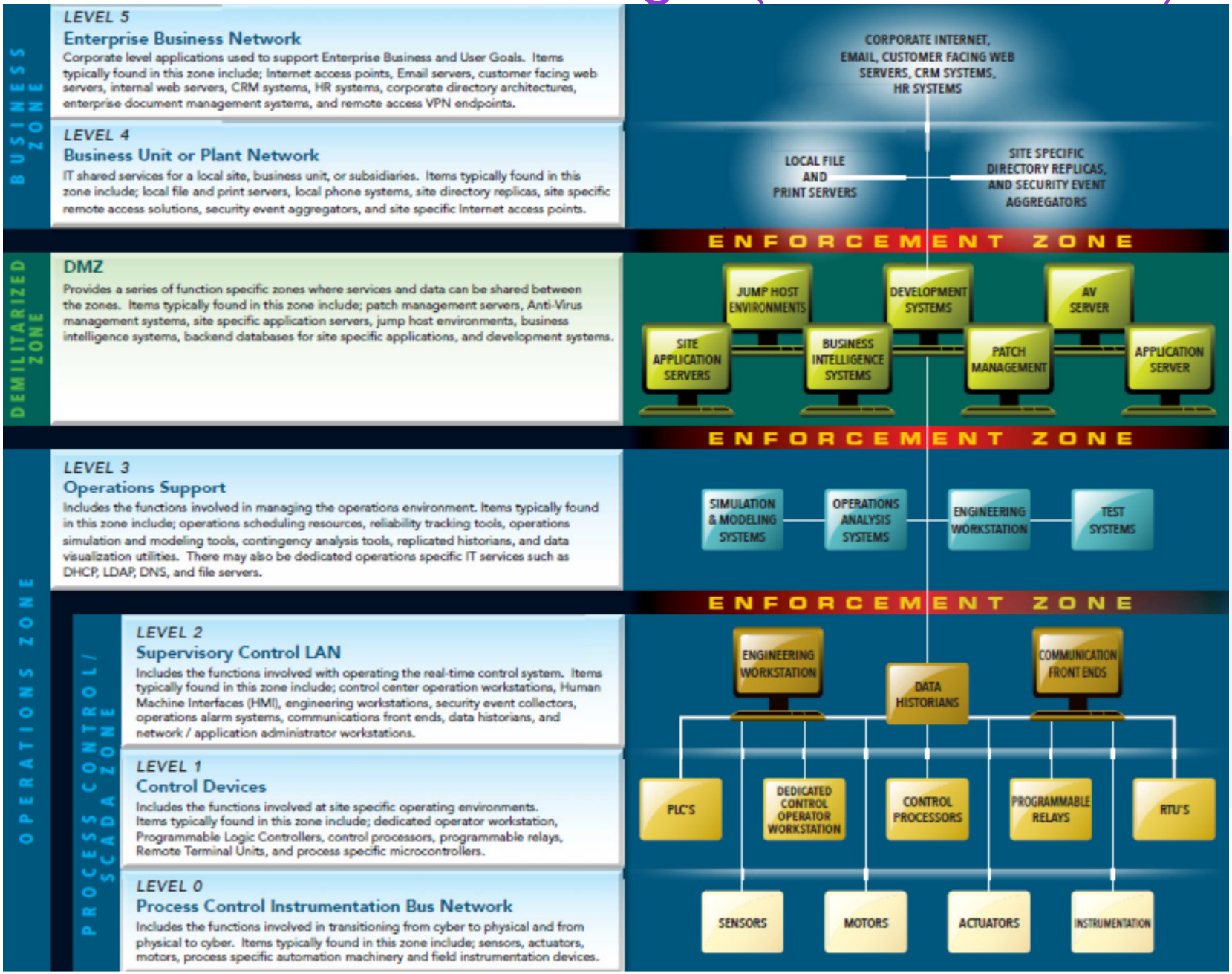
- Usually only in a Test Environment
- Use the Red Team for Detailed VPT and “Specials”

Security Remediation

- Strategy and Planning
- Review and Reporting

IT'S HOW
WE CONNECT

Archictecture and Design (Purdue Model)



Things You Need To Know

ICS – Industrial Control System

CI – “Critical Infrastructure” – small subset of ICS

SCADA – Supervisory Control And Data Acquisition – remote monitoring and control – big subset of ICS

DCS – Distributed Control System – process control – another big subset of ICS and *is not SCADA*

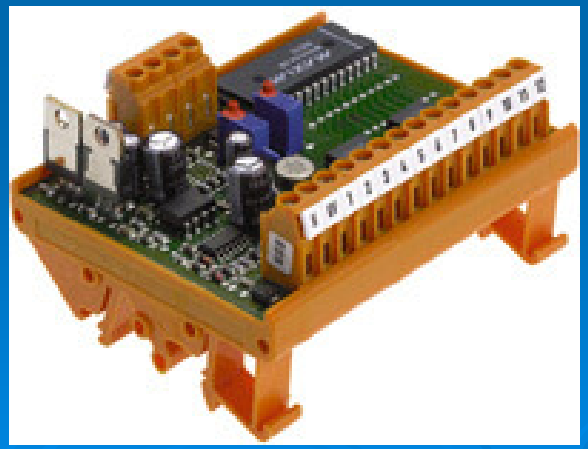
PCS – Process Control System (typically a DCS)

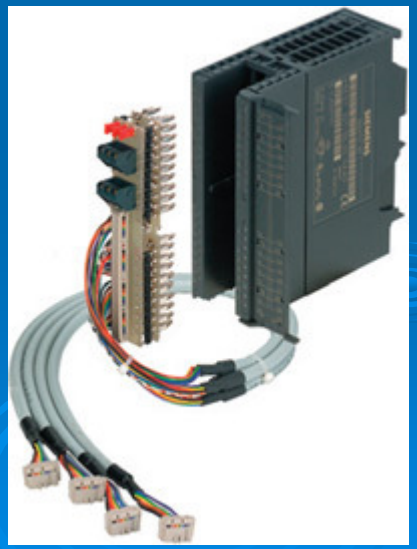
PCN – Process Control Network (has PLCs)

PLC – Programmable Logic Controller

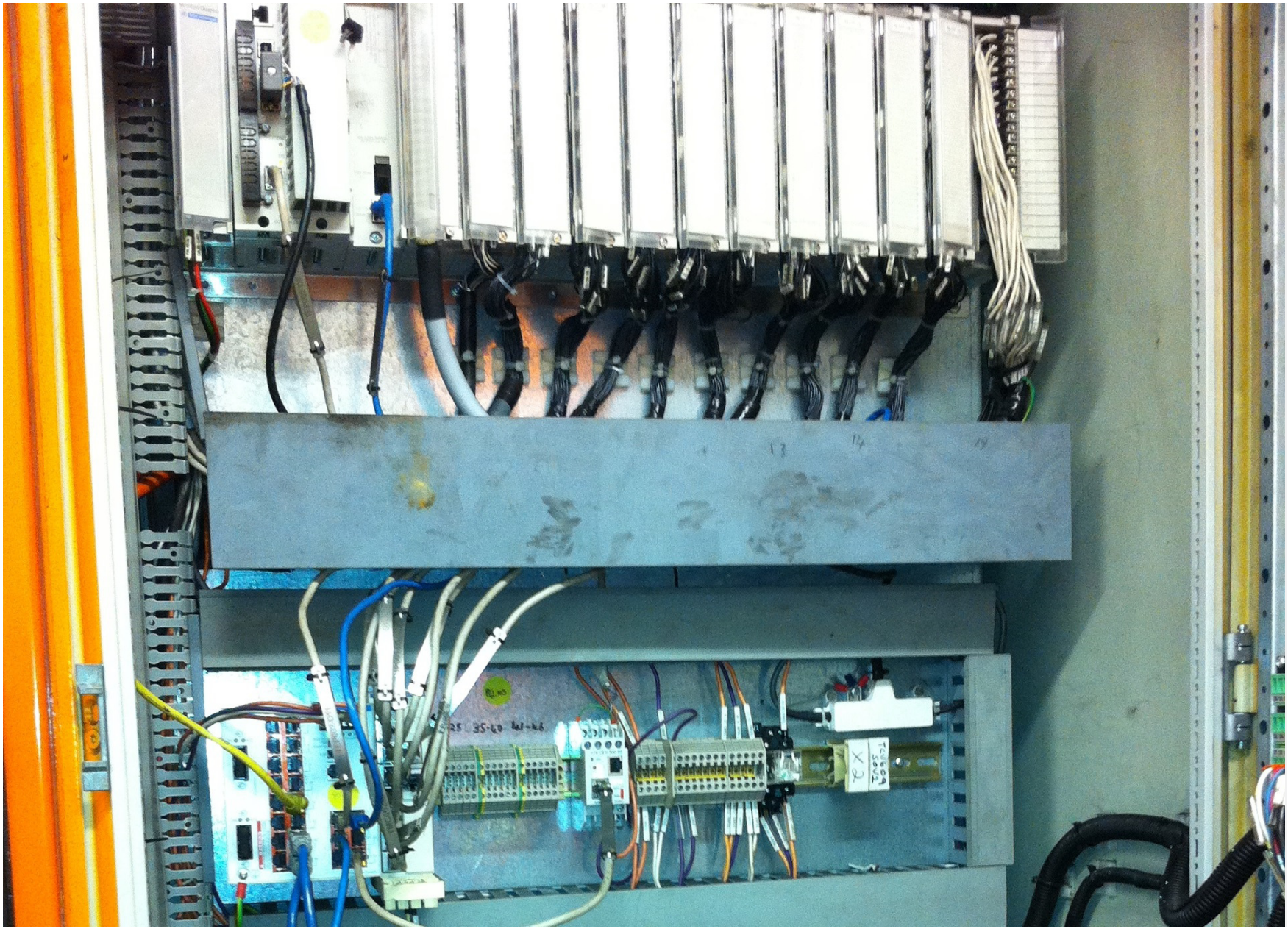
PLC LAN – a PCN

Industrial Networking Components

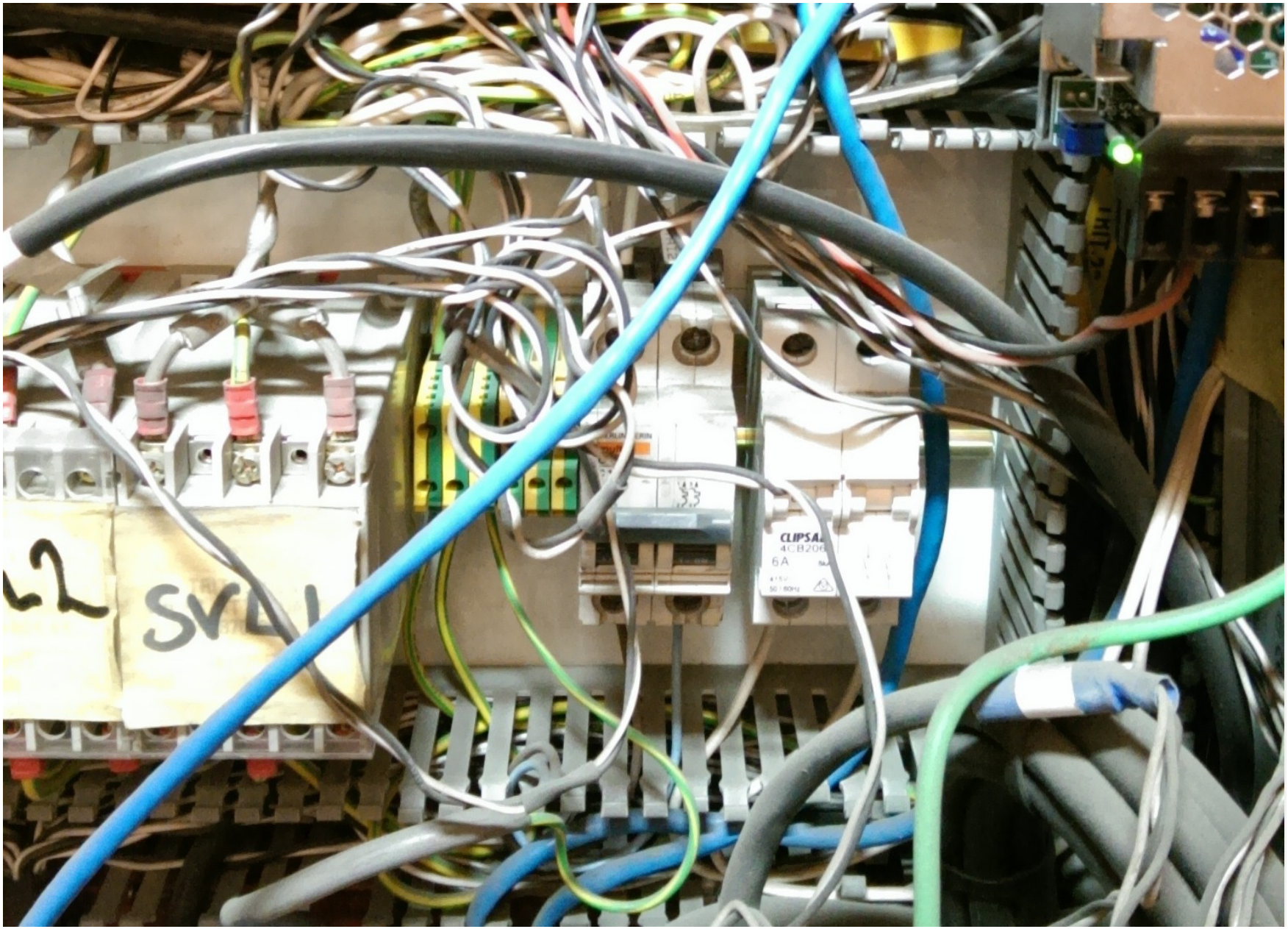




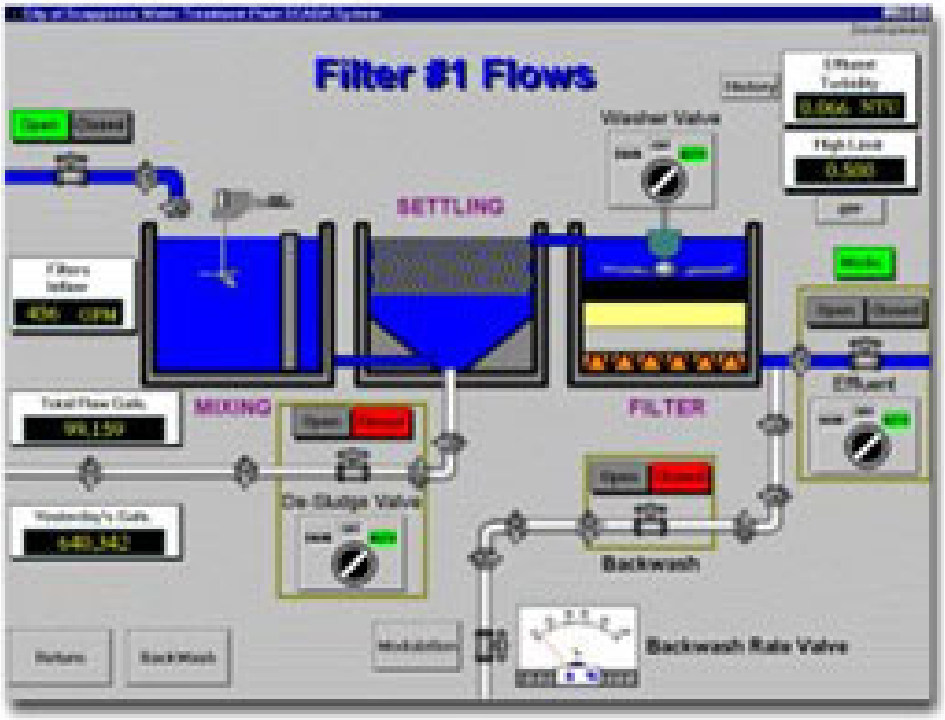
This is a typical PLC



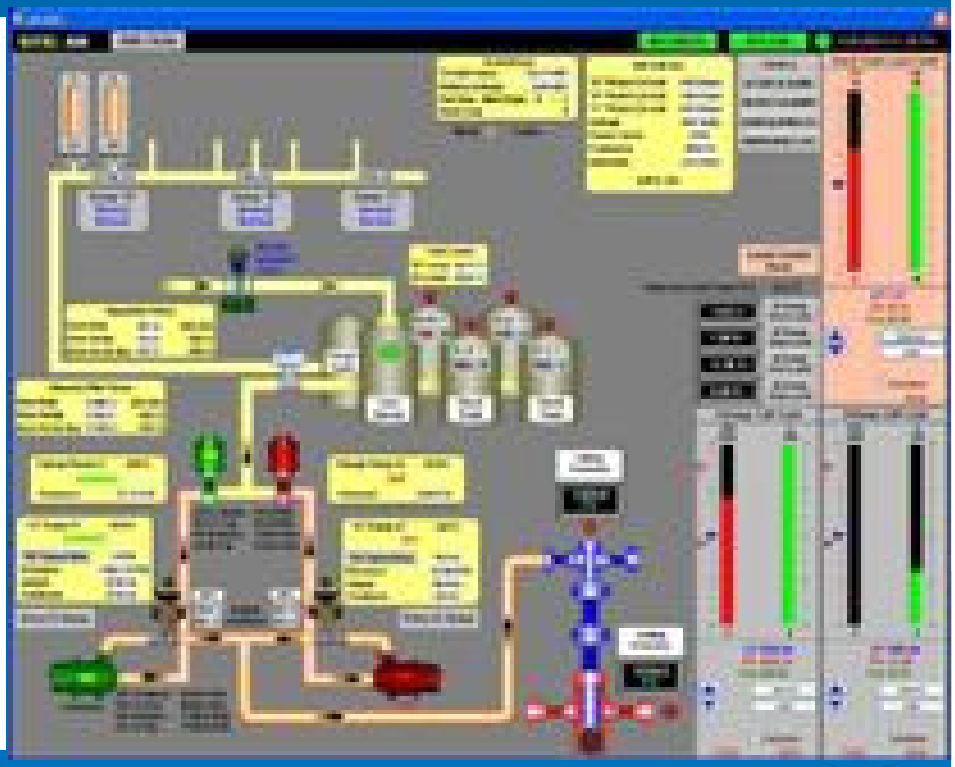
Following wires can be a challenge



MMI / HMI



Automation Technologies and Controls USA



Industrial Concepts (USA)

Industrial Networking Security

- Physical layer availability/resiliency requirements
- Segment the logical and physical topology
- Firewalls with strong ACLs
- Defence in depth
- Use managed industrial switches
- Use intrusion detection services – IDS not IPS

Critical Infrastructure

- Assets that are essential for the functioning of a society

Critical Infrastructure

Critical Infrastructure

- Airports, Bridges, Dams,
- Electricity, Fuels, Water,
- Hospitals, Lighthouses,
- Railways, Roads, Transport, Post
- Sewage, Waste Management
- Telecommunications
- National Broadband Network?

Any questions so far?

Advanced Persistent Threat

- Usually a group or a state
- Both capability and intent
- Persistently and
- Effectively
- Target a specific asset

- (Typically long-term sophisticated attacks)

Advanced

- Considerable intelligence-gathering abilities
- Access to specialist/protected knowledge
- Combine multiple tools and techniques to get to and acquire the target
- Not limited to technological resources

Persistent

- Does not mean constant attacks
- Specific target
- Typically not simply criminal gain
- Usually state political motivation
- Considerable resources
- Continuous monitoring and planned attack
- Re-acquiring of lost targets
- Maintain long-term access to targets

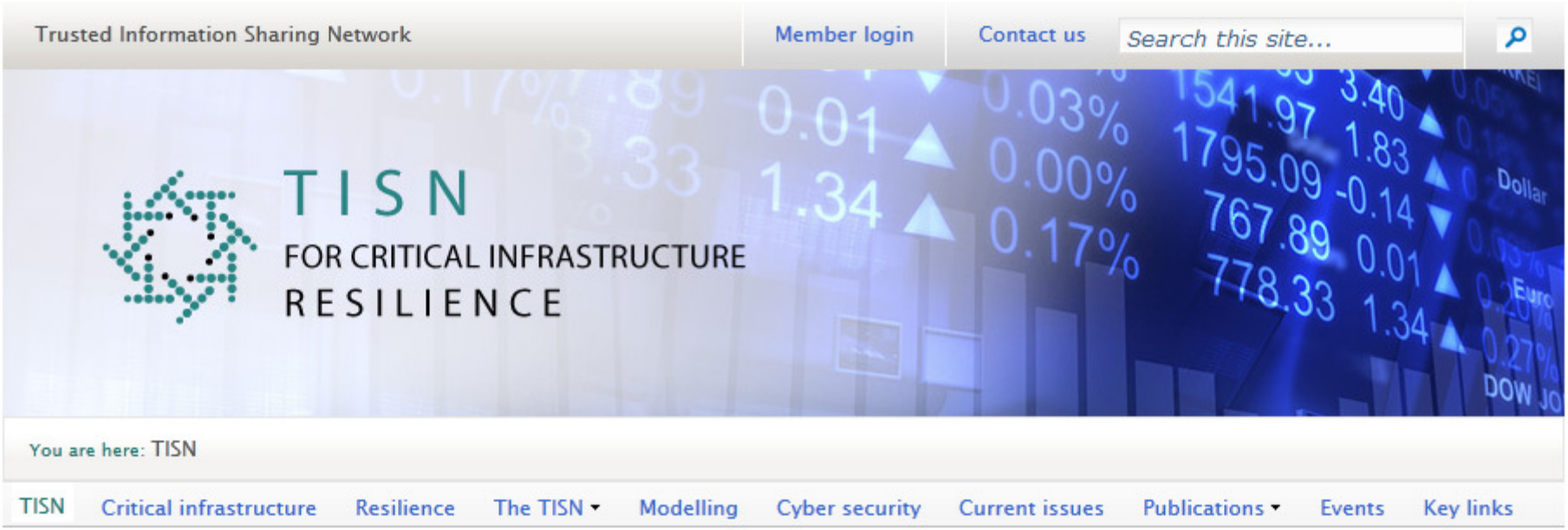
Threat

- Both capability and intent
- Motivated and well-resourced
- Effective actions
- Specific target
- Coordinated and managed (directed)

Critical Infrastructure Resilience

- Australian Government
  Critical Infrastructure Resilience Strategy
  - Effective business-government partnership
  - Organisational Resilience BoK
  - Assist owners and operators
  - Timely and high quality policy advice
  - Implement the Australian Government's Cyber Security Strategy, and
  - Support programs by States and Territories

Trusted Information Sharing Network



Stuxnet

- Discovered June 2010
- Targets Siemens “Step-7” SCADA software on Microsoft Windows
- First to include a PLC rootkit
- Different variants targeted 5 Iranian plants
  - Iranian uranium enrichment infrastructure
- Sophisticated attack
- Speculation Israel & USA may be involved
  - (vaguely acknowledged by the US President)

Stuxnet – Windows

- Four zero-day attacks
- Initially via infected USB drives
- Then peer-to-peer RPC to spread
- Rootkit capability with device drivers signed with private keys of two stolen certs
  - from JMicron and Realtek
  - both located in Taiwan
  - Now revoked by VeriSign

Stuxnet – Step 7

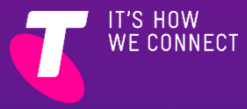
- Infects project files belonging to Siemens' WinCC/PCS 7 SCADA control (Step 7)
- Intercepts communications between WinCC and the Siemens PLC devices
- Covertly installs itself on PLC devices
- Hides itself from WinCC
- Used a zero-day (hard-coded password) exploit in the WinCC database software

Stuxnet – PLCs

- Specific slave variable-frequency drives
- Siemens S7-300 system
- Only attacks systems with drives from Vacon in Finland and Fararo Paya in Iran
- Only attacks between 807 Hz and 1210 Hz
- Installs malware and rootkit into the PLC
- Randomly 1410Hz then 2Hz then 1064Hz
- Rootkit masks the rotational speed

Any questions so far?

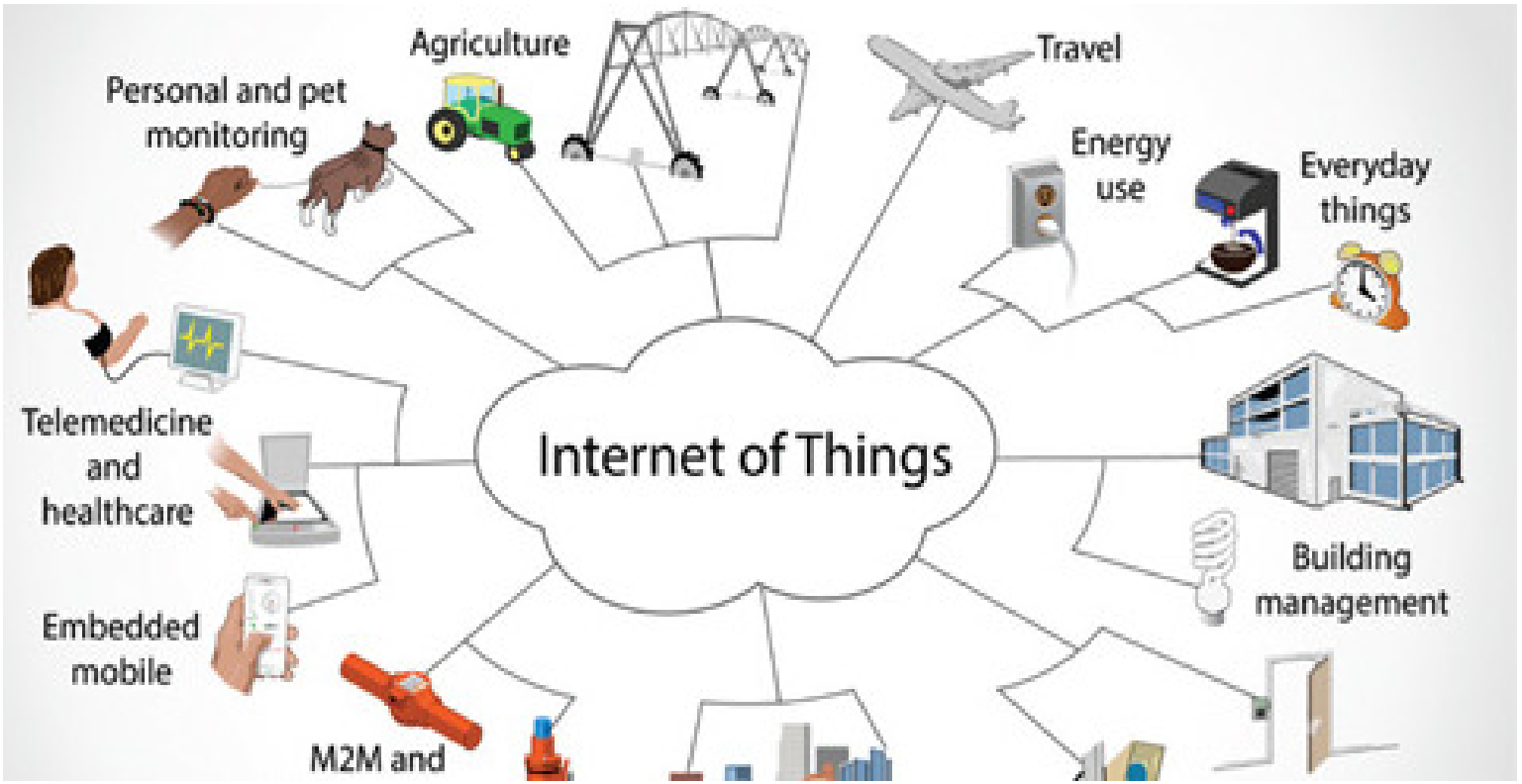
Internet of Things



Things You Need To Know

Not just ICS components – many domestic devices:

Smart Meters, Smart Homes, Smart Appliances, Devices, Vehicles, Buildings



Attack demos at RSA Conference

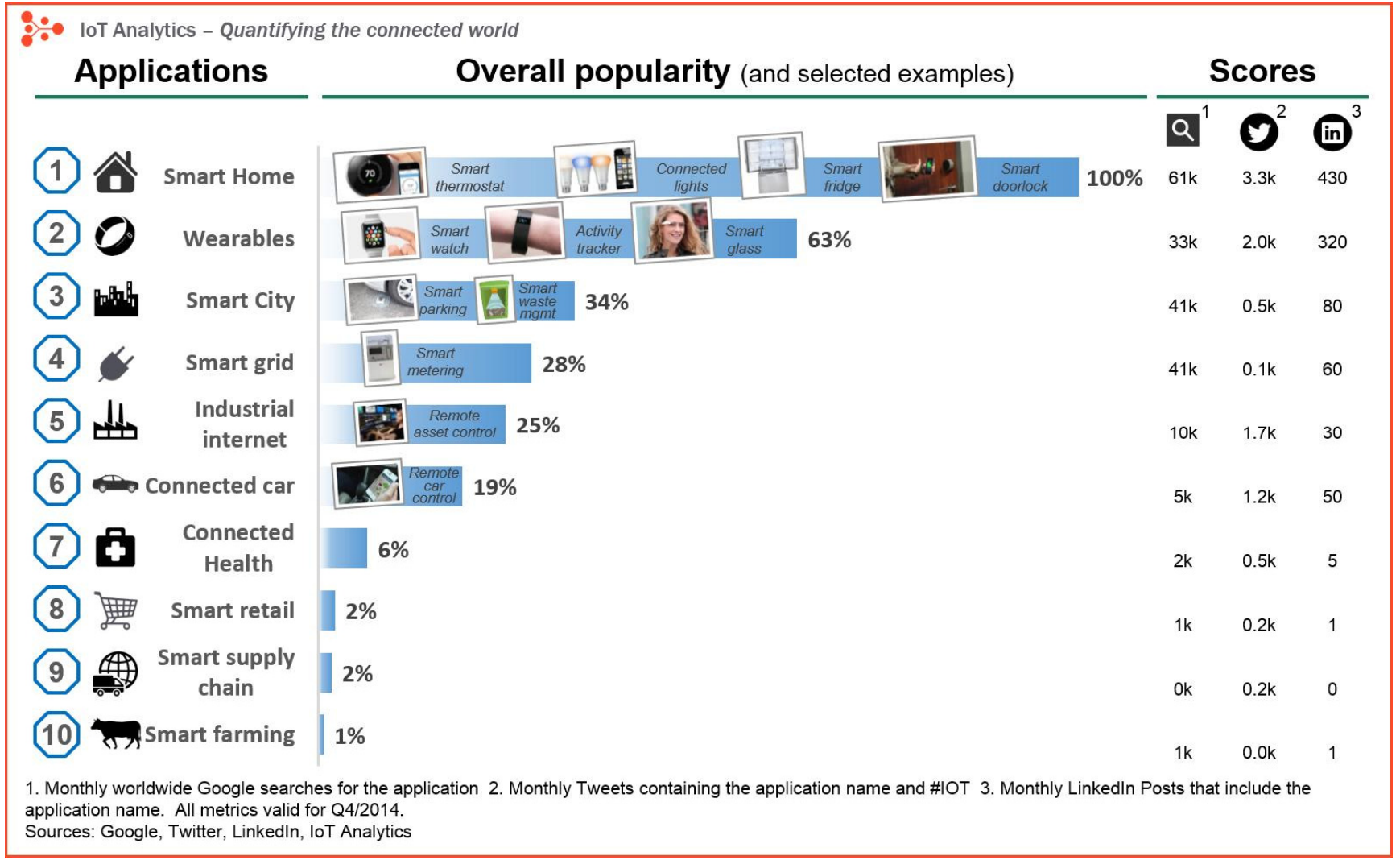
Attack demos at RSA Conference

US Federal Trade Commission

The small size and limited processing power of many connected devices could limit the use of encryption and other security measures;

it may also be difficult to patch flaws in low-cost and essentially disposable IoT devices.

https://datafloq.com/read/internet-of-things-iot-security-privacy-safety/948



Attack demos at RSA Conference

In the News (Jeremy Kirk, Information Security Media Group ISMG: Bankinfo Security)

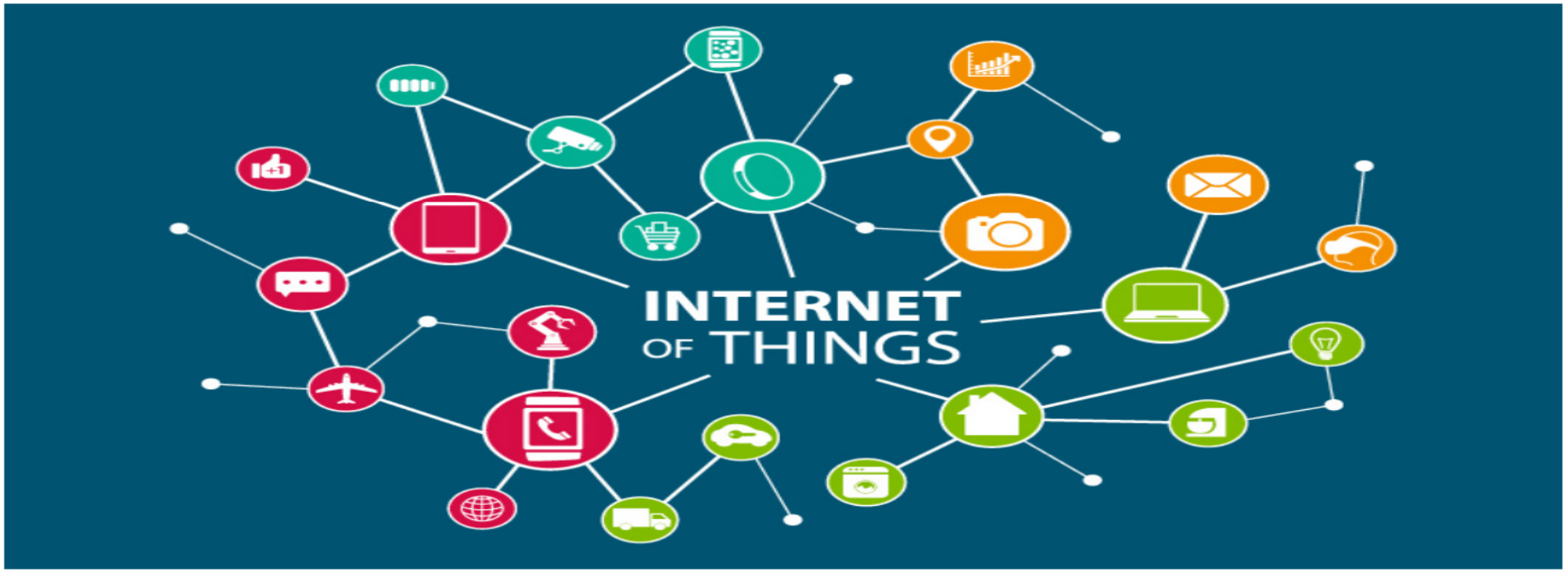
Akamai Warns of Account Takeovers Staged from Cameras, Routers

IoT Hackers Scoring Hits Using a 12-Year-Old OpenSSH Vulnerability

Jeremy Kirk (jeremy_kirk) • October 14, 2016 0 Comments

Twitter Facebook LinkedIn Credit Eligible Get Permission

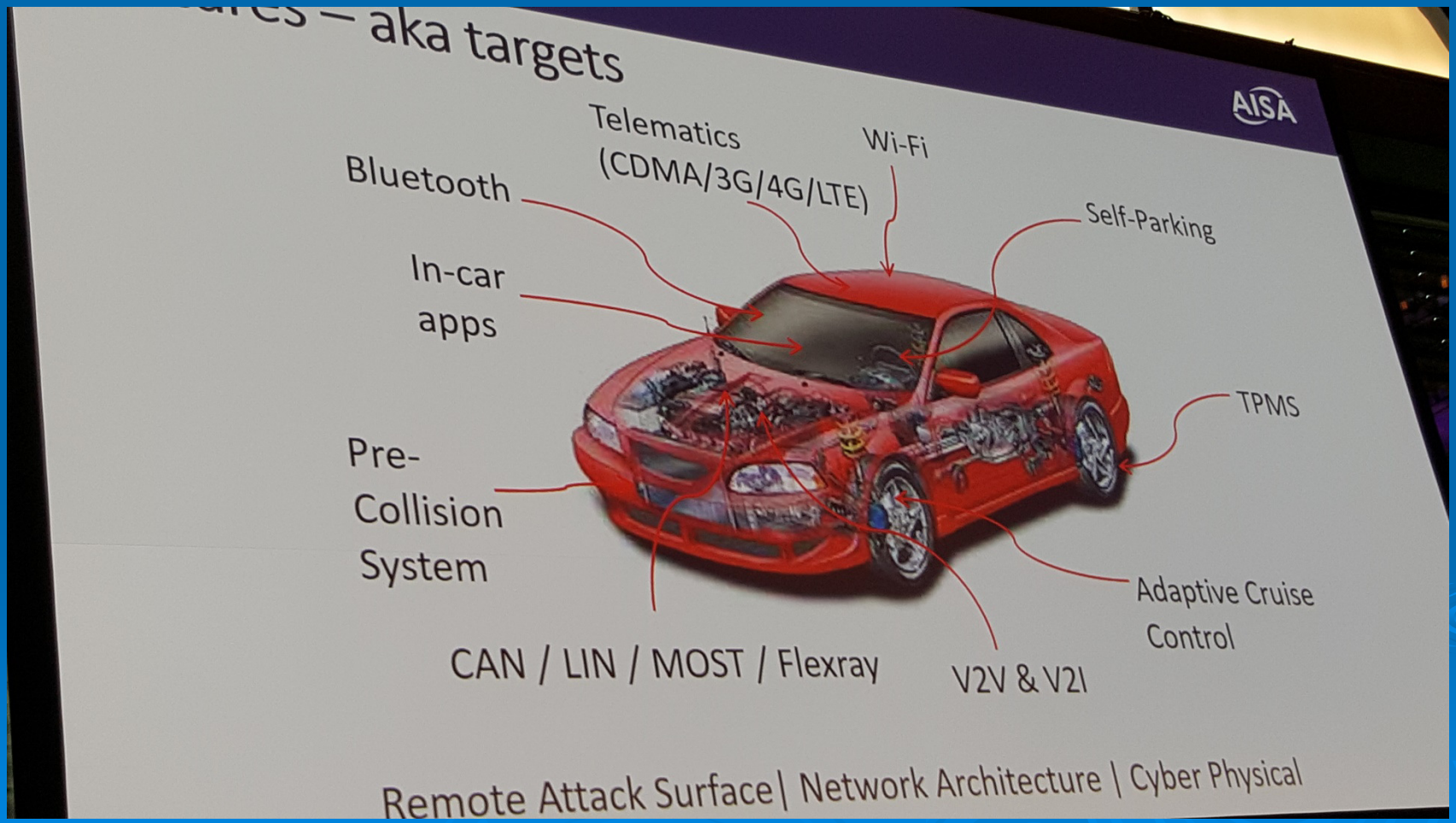
www.bankinfosecurity.com/akamai-warns-account-takeovers-staged-from-cameras-routers-a-9454



A long-known weakness in an authentication protocol shipped in millions of routers, surveillance devices and satellite antennae is being used in attempts to compromise accounts at popular web services, according to new research from Akamai.

Remember these 2 guys from the very first lecture?

Automotive ICS / IoT



Questions?

IT'S HOW
WE CONNECT

Thank you – end of examinable material

IT'S HOW
WE CONNECT

Industry Lecture Today

Mark McPherson, CISO, YDF

Mark is an IT specialist, with 26 years' experience, including 18 years as a security analyst, educator & manager at both of Australia's National CERTs, and senior positions advising Federal, State & Local Government agencies, national and international telecommunications providers, utilities, banks, universities and other critical infrastructure organisations.

Mark is experienced in developing and implementing critical information security management policy and organisational security culture. His roles have included National Security Policy Manager and International Training & Conferences Manager. Mark has also occupied several board & steering committee positions of international organisations collaborating on global incident response.

Final Exam

THE UNIVERSITY OF QUEENSLAND
AUSTRALIA

This exam paper must not be removed from the venue

Venue _____

Seat Number _____

Student Number |__|__|__|__|__|__|__|__|

Family Name _____

First Name _____

School of Information Technology and Electrical Engineering

EXAMINATION

Semester Two Final Examinations, 2017

COMS3000 Information Security

This paper is for St Lucia Campus students.

Examination Duration: 120 minutes

Reading Time: 10 minutes

For Examiner Use Only

Question Mark

Examination Duration: 120 minutes

Reading Time: 10 minutes

Exam Conditions:

This is a Central Examination

This is an Open Book Examination

During reading time - write only on the rough paper provided

This examination paper will be released to the Library

Materials Permitted In The Exam Venue:

(No electronic aids are permitted e.g. laptops, phones)

Calculators - Any calculator permitted - unrestricted

Materials To Be Supplied To Students:

1 x 14 Page Answer Booklet

Instructions To Students:

Additional exam materials (eg. answer booklets, rough paper) will be provided upon request.

For Examiner Use Only

Question	Mark

Final Exam

- 15 QUESTIONS
- 60 MARKS
- 120 minutes

- Do the math → 2 minutes per mark
  - 1 mark = 2 minutes
  - 10 marks = 20 minutes

Final Exam Marks

- Q1 – 7 marks
- Q2 – 7 marks
- Q3 – 1 marks
- Q4 – 3 marks
- Q5 – 2 marks
- Q6 – 2 marks
- Q7 – 3 marks
- Q8 – 1 mark
- Q9 – 10 marks
- Q10 – 4 marks
- Q11 – 1 marks
- Q12 – 4 marks
- Q13 – 2 marks
- Q14 – 7 marks
- Q15 – 6 marks

Final Exam(s)

- Week 1: Information Security, Risk Mgt
- Week 2: Trust, Access Control, Authentication, Authorisation, Cryptographic hashes
- Week 3: MFA, Biometrics
- Week 4: Biometrics, PCI
- Week 5: Malware (guest)
- Week 6: Datacentre (cloud) security (guest)
- Week 7: Access Control Security Models, Information Theory
- Week 8: Cryptography,
- Symmetric Cryptography
- Week 10: Discrete Logs, Asymmetric Cryptography
- Week 11: Network Monitoring (guest)
- Week 12: Network Security
- Week 13: Cloud Computing

Final Exam

- Typically questions want you to "Demonstrate…", "Describe…", "Compare…", "Show how…", "Give an example…", etc.
- So a final numerical result for calculations will only be worth 1 mark
- You MUST demonstrate, describe, etc – i.e. show your working / how you got the answer – to get the rest of the marks.

Final Exam

- E.g. 4 marks:
  "Demonstrate how to calculate the Shannon Information in this coding system"
- Correct formula – 1 mark
- Correct values into formula – 1 mark
- Correct working – 1 mark
- Correct answer – 1 mark

Final Exam

- The exam requires you to UNDERSTAND
- Some questions will be similar to tutorials but with additional marks in complexity or unfamiliar components, so that you have to apply the principles from the tutorial, but in a new way or to an additional component.

Final Exam

- It is designed for open-book:
  - There is no “draw diagram X from the lecture notes”
  - No point asking anything directly from the lecture notes because it is open book
  - It is time-limited:
    - You DO NOT have time to look up everything you don’t know
    - Your notes are for the occasional thing you need to check – you cannot learn each topic in the exam!

Final Exam

- Last year's **average** mark was 39.8 (out of 60, including both course codes)
- The lowest was **16.5** / 60
- The highest was **56** / 60
- Should be easy for most to get 30 (pass)
- Should be harder to get >40 (credit '5')
- Should be quite hard to get >45 distinction
- Should be very hard to get >50 high dist. 7

Thank you

I wish you success in all your studies!

IT'S HOW
WE CONNECT