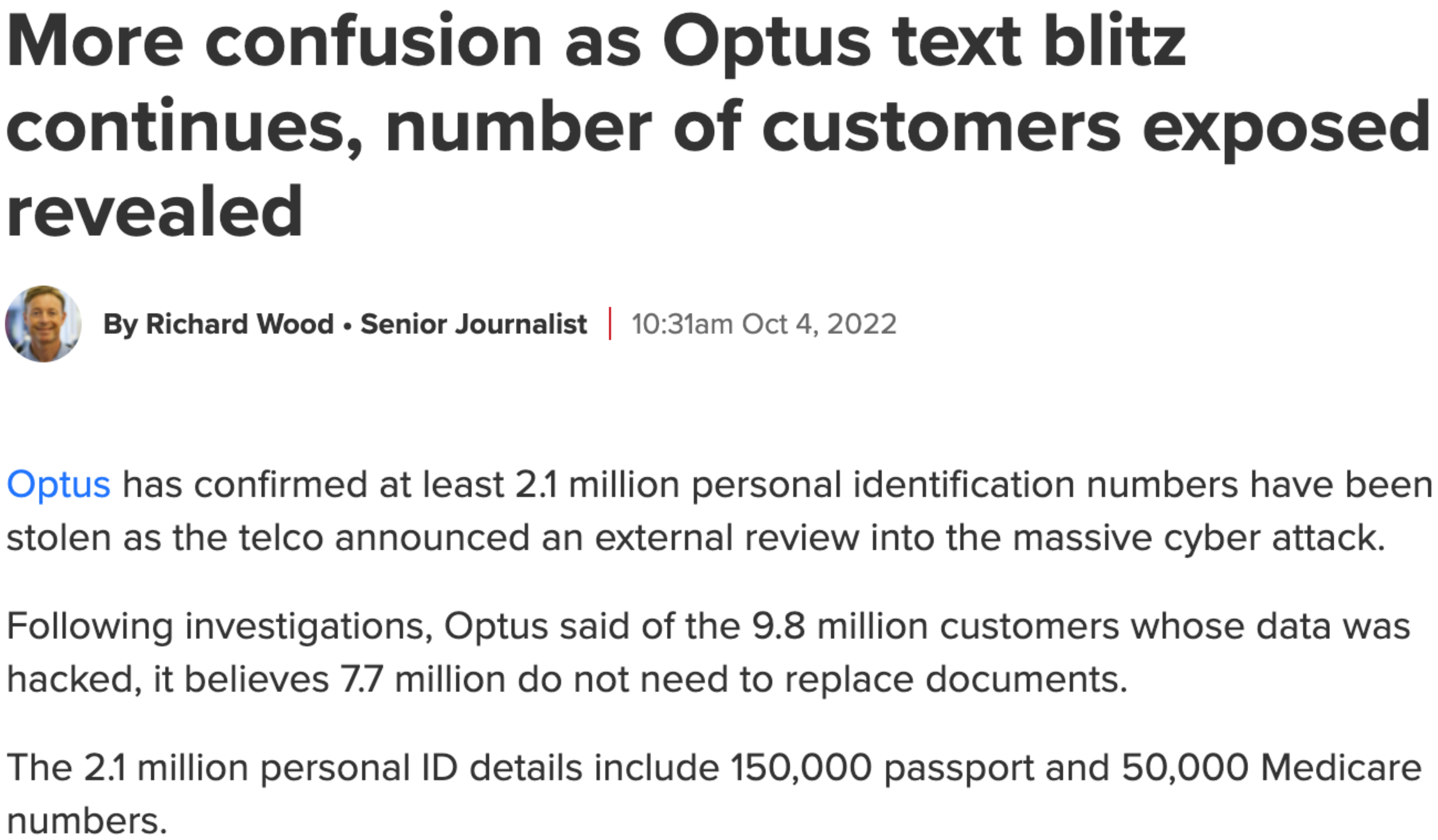
Security and Privacy for Pervasive Systems

COMP5047 – Lecture 12

Anusha Withana
Security slides are adapted from **Dr Kanchana Thilakarathna**

The School of Computer Science
The University of Sydney

Why care about security/Privacy?



More confusion as Optus text blitz continues, number of customers exposed revealed

By Richard Wood • Senior Journalist | 10:31am Oct 4, 2022

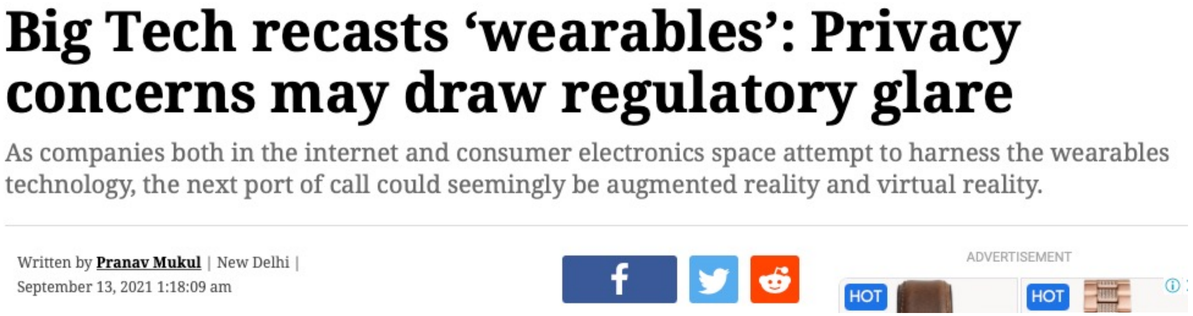
Optus has confirmed at least 2.1 million personal identification numbers have been stolen as the telco announced an external review into the massive cyber attack.

Following investigations, Optus said of the 9.8 million customers whose data was hacked, it believes 7.7 million do not need to replace documents.

The 2.1 million personal ID details include 150,000 passport and 50,000 Medicare numbers.

https://www.9news.com.au/national/optus-data-breach-update-more-than-two-million-customer-identity-details-exposed/b92b17d9-fc77-430b-94ca-21def7fea61d

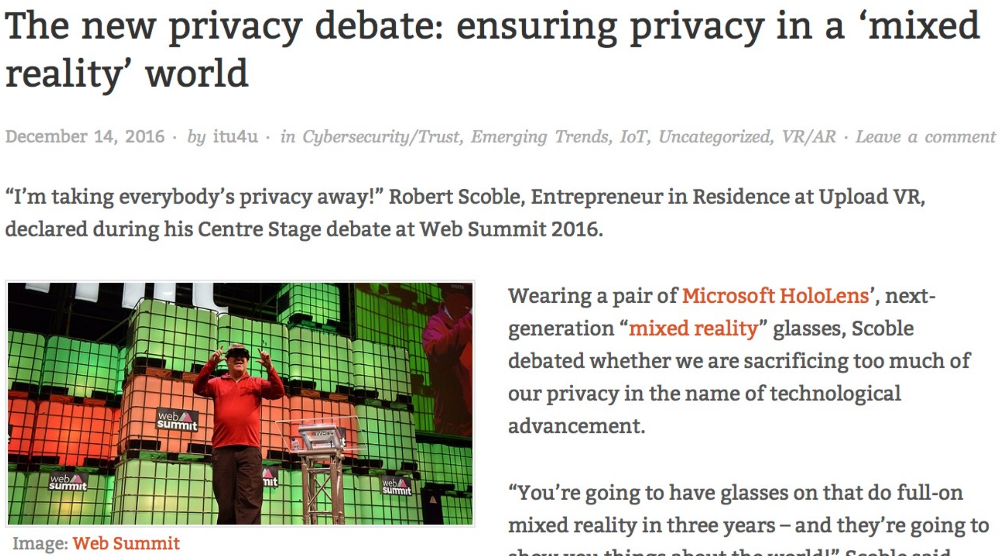
Why care about security/Privacy?



Big Tech recasts ‘wearables’: Privacy concerns may draw regulatory glare

As companies both in the internet and consumer electronics space attempt to harness the wearables technology, the next port of call could seemingly be augmented reality and virtual reality.

Written by **Pranav Mukul** | New Delhi |
September 13, 2021 1:18:09 am



The new privacy debate: ensuring privacy in a ‘mixed reality’ world

December 14, 2016 · *by* itu4u · *in Cybersecurity/Trust, Emerging Trends, IoT, Uncategorized, VR/AR* · *Leave a comment*

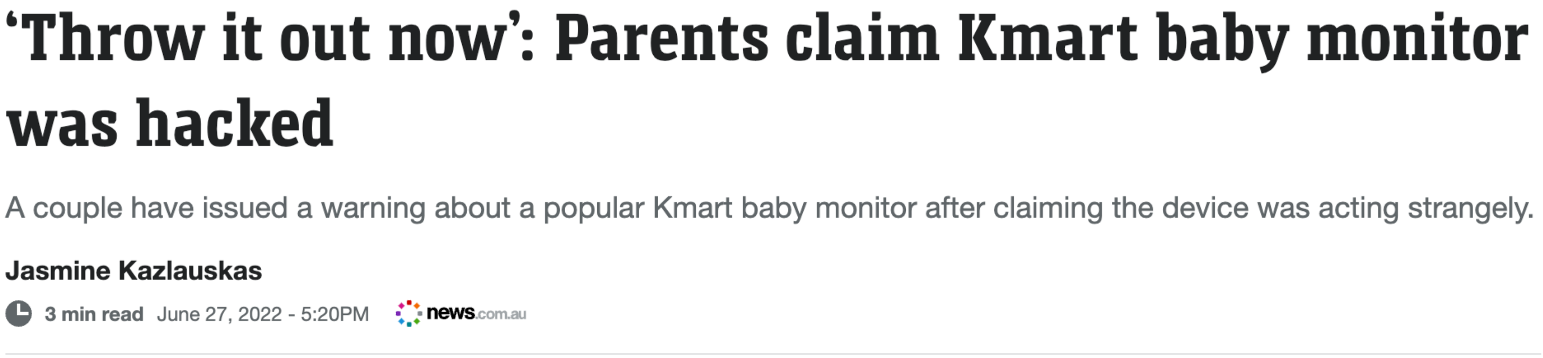
“I’m taking everybody’s privacy away!” Robert Scoble, Entrepreneur in Residence at Upload VR, declared during his Centre Stage debate at Web Summit 2016.

Image: Web Summit

Wearing a pair of Microsoft HoloLens’, next-generation “mixed reality” glasses, Scoble debated whether we are sacrificing too much of our privacy in the name of technological advancement.

“You’re going to have glasses on that do full-on mixed reality in three years – and they’re going to show you things about the world!” Scoble said.

Why care about security/Privacy?



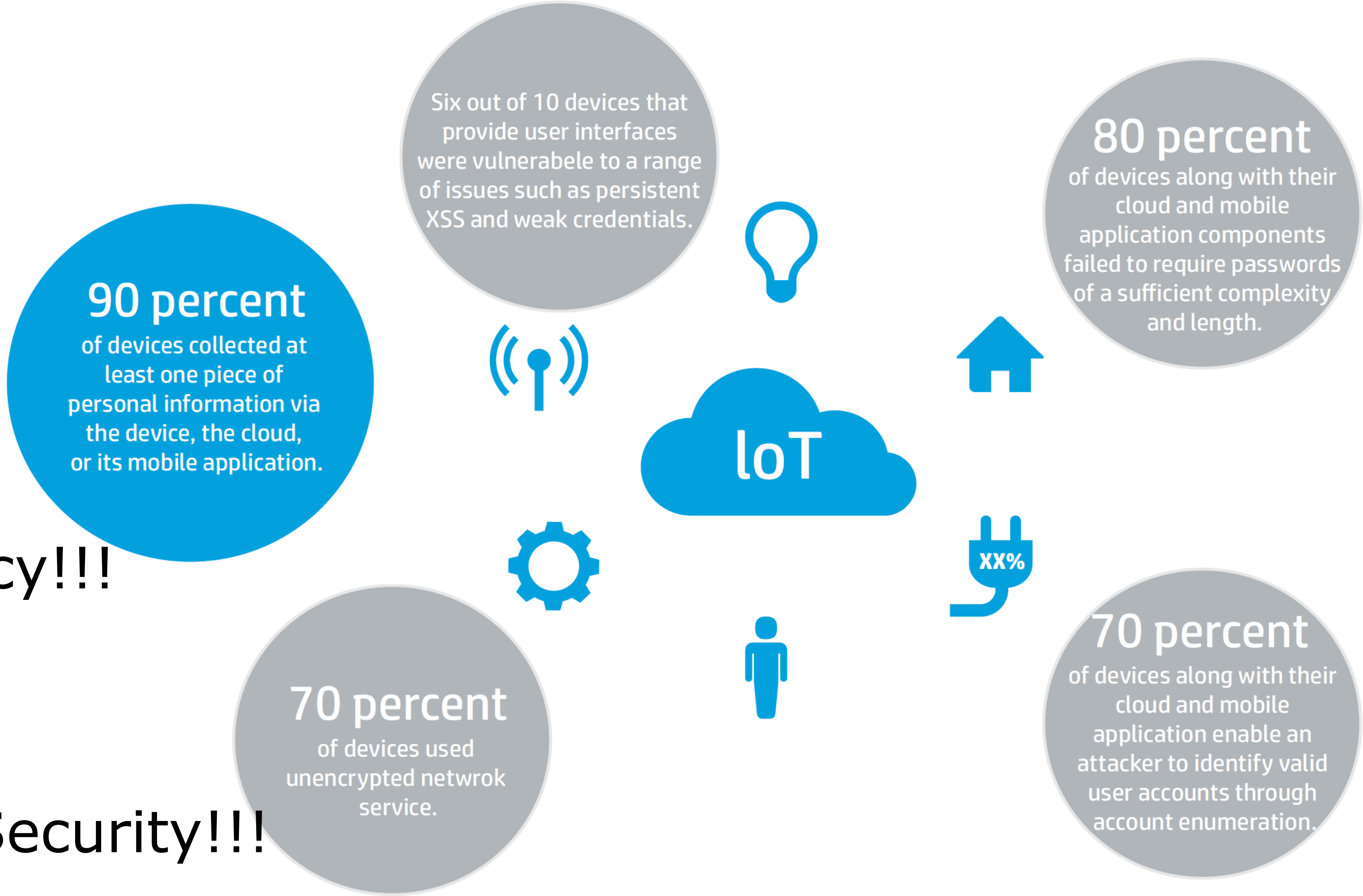
‘Throw it out now’: Parents claim Kmart baby monitor was hacked

A couple have issued a warning about a popular Kmart baby monitor after claiming the device was acting strangely.

Jasmine Kazlauskas

3 min read June 27, 2022 - 5:20PM news.com.au

https://www.news.com.au/lifestyle/real-life/news-life/throw-it-out-now-parents-claim-kmart-baby-monitor-was-hacked/news-story/980ef5d3d243e675d053da6a93c79f6f



Six out of 10 devices that provide user interfaces were vulnerabele to a range of issues such as persistent XSS and weak credentials.

80 percent of devices along with their cloud and mobile application components failed to require passwords of a sufficient complexity and length.

90 percent of devices collected at least one piece of personal information via the device, the cloud, or its mobile application.

Privacy!!!

70 percent of devices used unencrypted netwrok service.

Security!!!

70 percent of devices along with their cloud and mobile application enable an attacker to identify valid user accounts through account enumeration.

HP Security Research. *Internet of Things Research Study*. s.l. : HP, 2014.

Three Security Goals

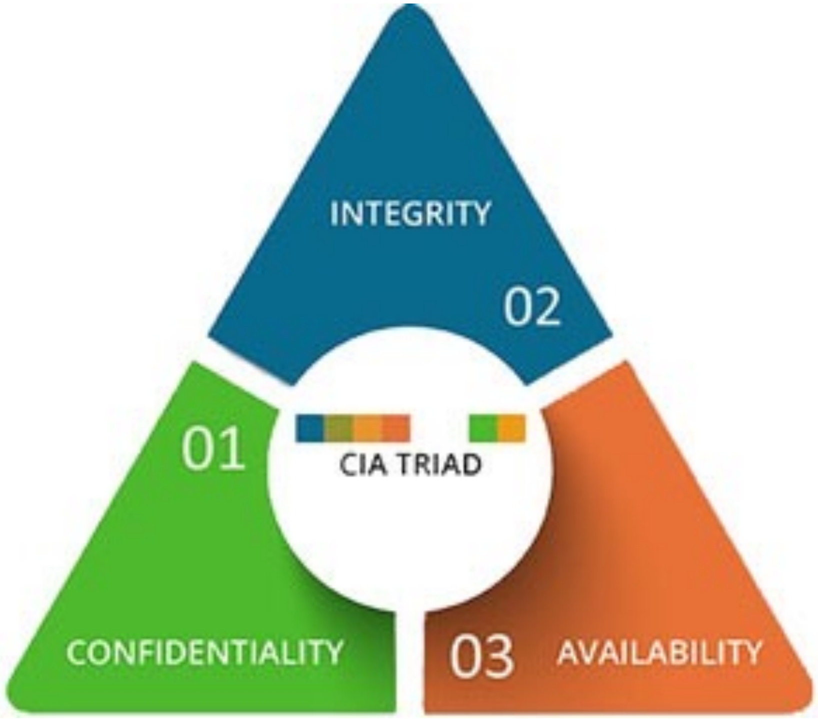


Image source: https://www.lbmc.com/blog/three-tenets-of-information-security/

CIA Triad

- Confidentiality
  - Privacy / Protect data
    - Prevent unauthorised access
- Integrity
  - Data is valid and accurate
    - Prevent unauthorised modification
- Availability
  - Accessible and modifiable by people with right access level in a timely manner

https://www.javatpoint.com/cyber-security-goals

Confidentiality - tools

- Encryption
    - Unreadable by any unwanted entity
- Authentication
    - Confirmation of a user's identity
- Authorization
    - Level of access
- Physical Security

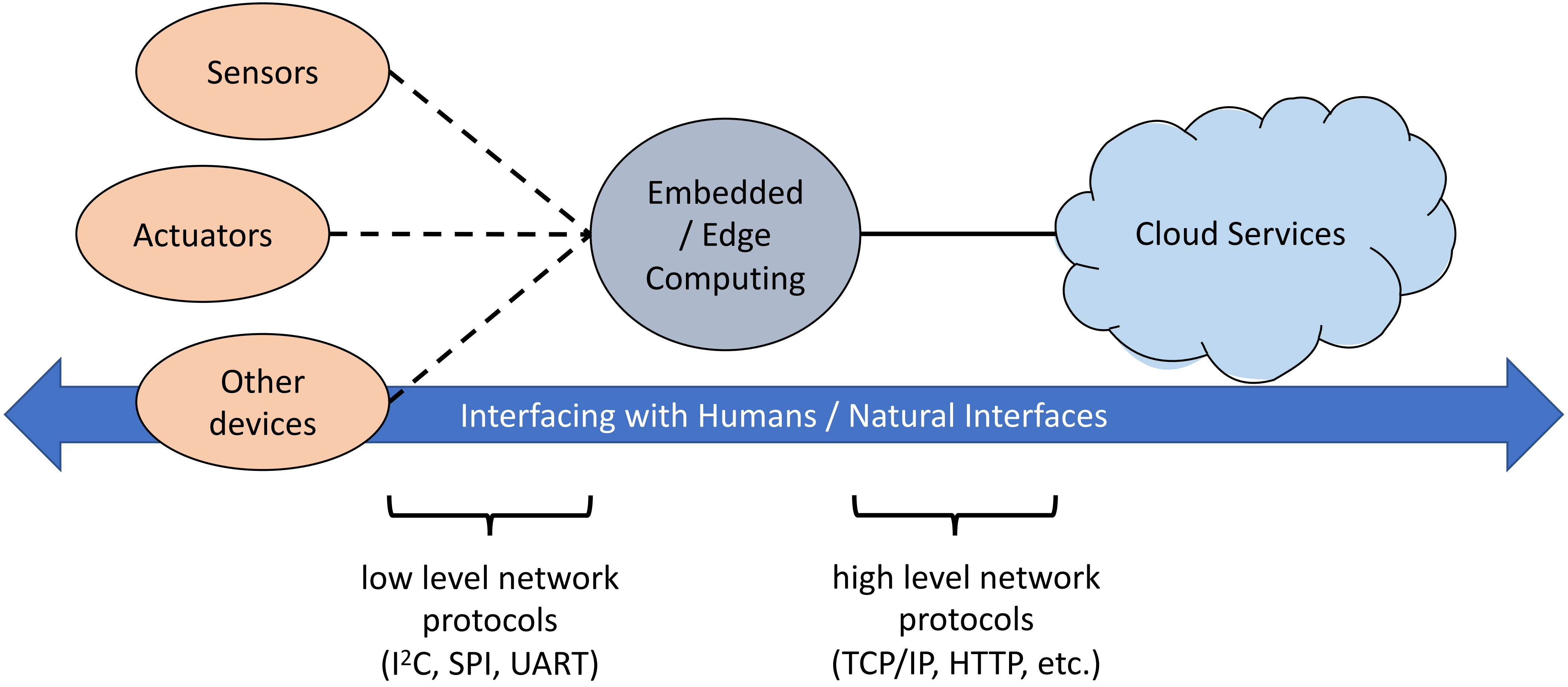
Integrity - tools

- Backups
- Checksums
  - Check integrity
- Data Correcting Codes
  - Correct data issues
- Physical Security

Availability - tools

- Network security solutions
  - E.g. Firewalls, intrusion detection
  - Protects against Denial of Service (DoS) attacks
- Physical Protections
- Computational Redundancies
  - Data stores, servers, even sensors

Where are the concerns?


Sensors
Actuators
Other devices
Embedded / Edge Computing
Cloud Services
Interfacing with Humans / Natural Interfaces
low level network protocols (I^2C, SPI, UART)
high level network protocols (TCP/IP, HTTP, etc.)

Sensors, Actuators, etc.

- Physical security is very important
  - Sensors can be manipulated
  - Interfaces like I2C, SPI are easy to hack into

https://weheartit.com/entry/121340615

Embedded Computing

- Firmware Confidentiality
  - Can be read by unauthorised people
- Reverse Engineering an Arduino Application
  - https://github.com/thomasbbrunner/arduino-reverse-engineering
- They will manage to read your private information
  - Eg. Wifi settings, usernames, etc.

Embedded Computing

- Firmware Integrity
  - Can be changed by unauthorised people
- MCUboot
  - secure bootloader solution
  - fail-safe firmware authentication
  - secure firmware update

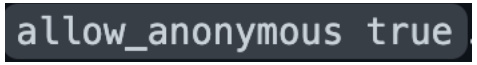
Introducing the Arduino secure boot

MCUboot-based bootloader solution offering fail-safe firmware authentication and update

arduino.cc/pro

Cloud Computing

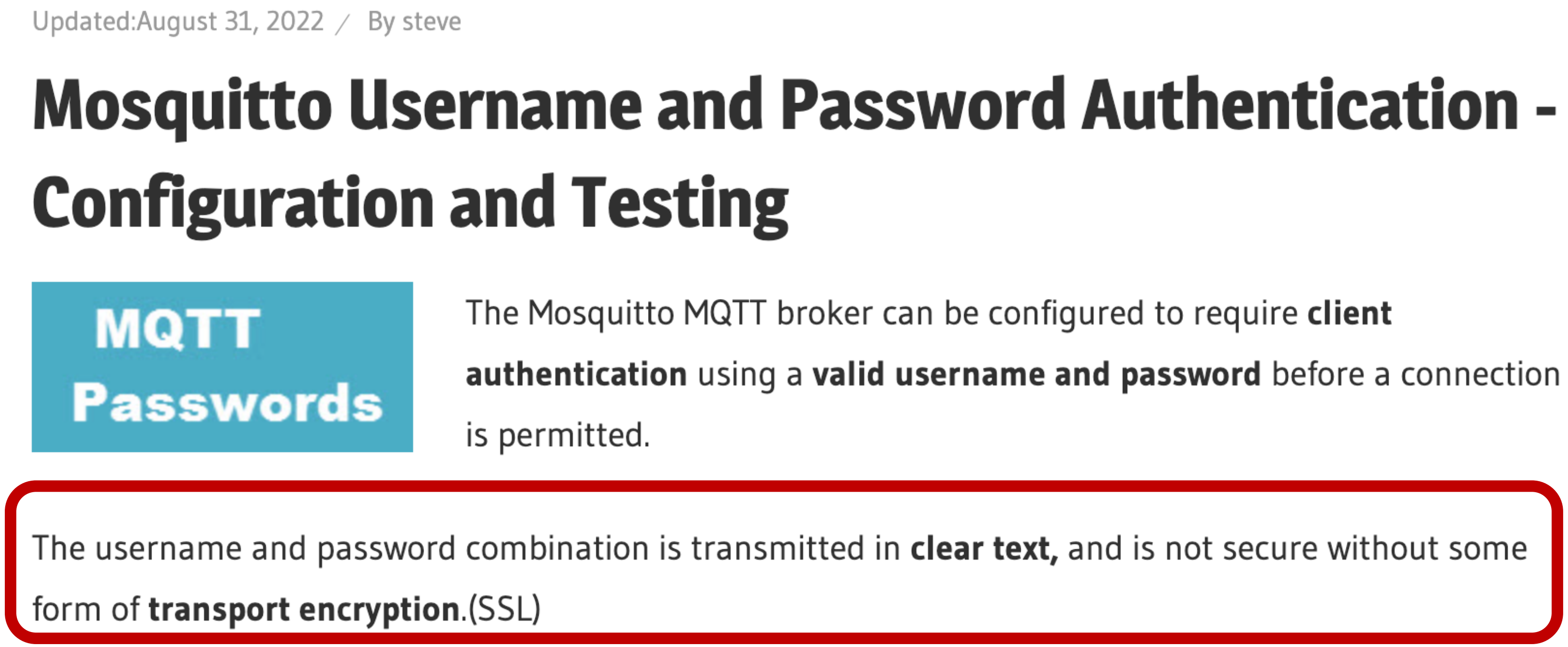
- Confidentiality
  - Authentication
  - Authorization



```
allow_anonymous true
```

- Anyone can post/subscribe

MQTT



Updated:August 31, 2022 ⁄ By steve

Mosquitto Username and Password Authentication - Configuration and Testing

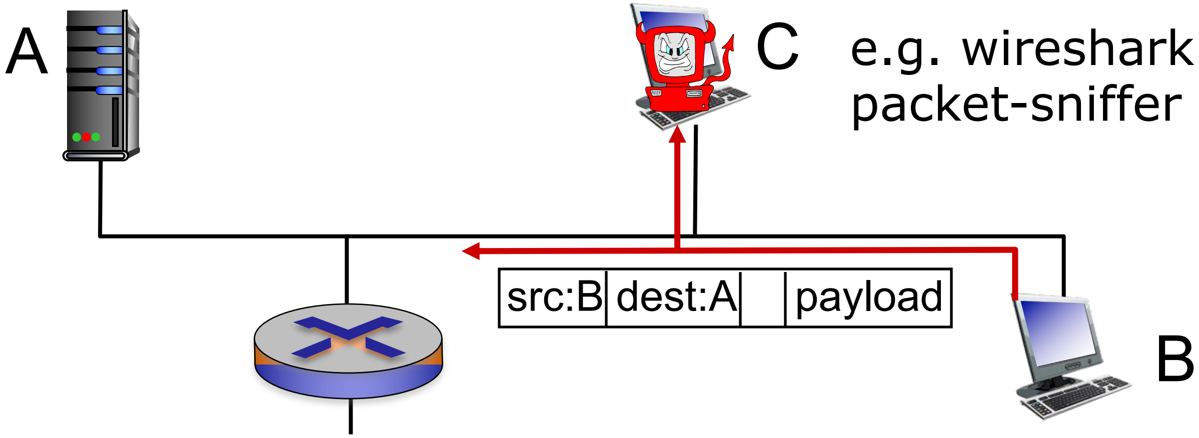
The Mosquitto MQTT broker can be configured to require **client authentication** using a **valid username and password** before a connection is permitted.

The username and password combination is transmitted in **clear text,** and is not secure without some form of **transport encryption**.(SSL)

http://www.steves-internet-guide.com/mqtt-username-password-example

Data Encryption

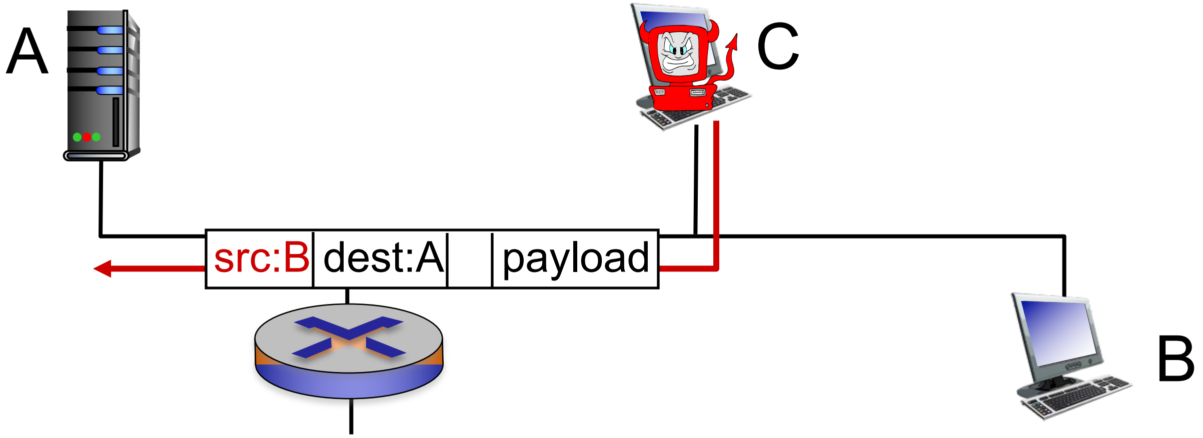
- If data is transmitted through network as plain text
  - There can be **packet sniffing**
    - broadcast media (shared Ethernet, wireless)
    - promiscuous network interface reads/records all packets (e.g., including passwords!) passing by



e.g. wireshark software is a (free) packet-sniffer

Data Encryption

- If identities are not verified
  - There can be **IP spoofing**
    - send data with false source address



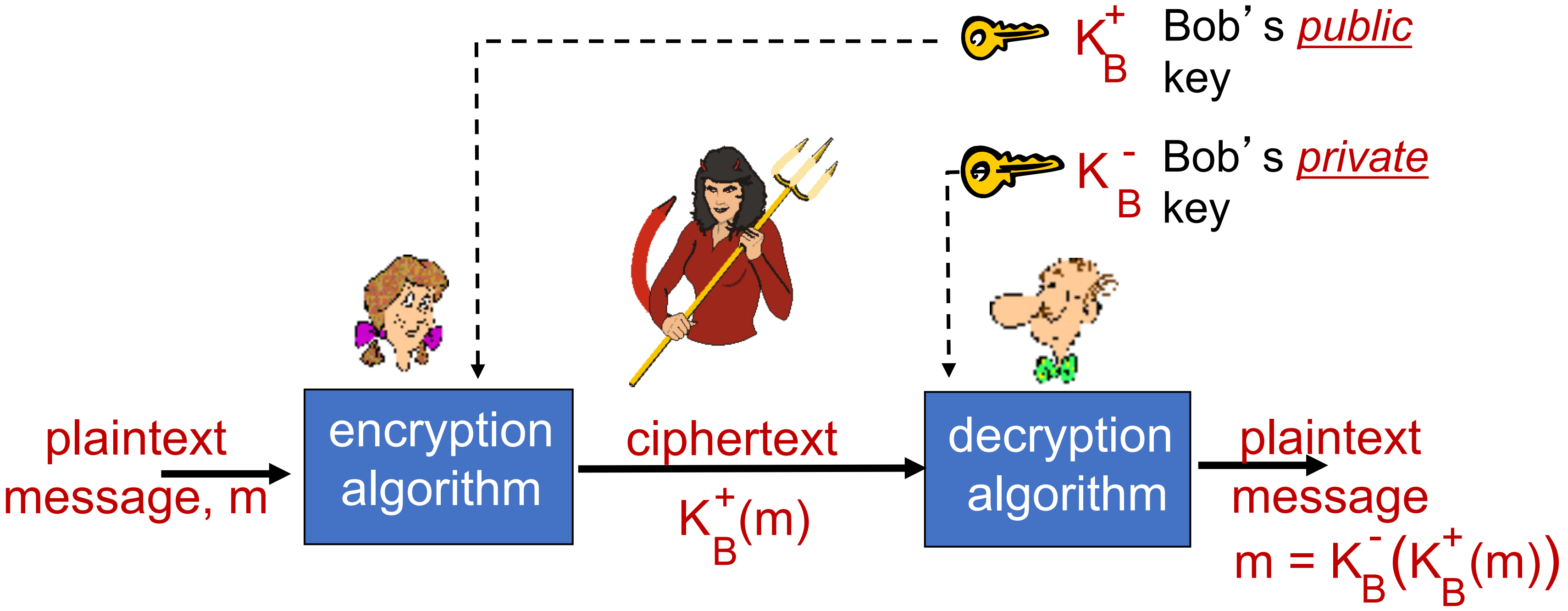
Data Encryption

- We have to encrypt data and include entity identification
- ***Encryption*** - Conversion of messages from a comprehensible form into an incomprehensible one and back again at the other end, rendering it unreadable by interceptors or eavesdroppers without secret knowledge
- ***Cryptography*** uses the processes of ***Encryption*** and ***Decryption***. The system it uses is called ***Cryptosystem***

Data Encryption

- Most of the network systems we used today use encryption
  - *Find out if following networks use encryption*
    - *I2C, SPI, Bluetooth LE, WiFi, LoRa*
- Most of the applications use application layer encryption
  - HTTP vs HTTPS

Public key cryptography



m plaintext message - a comprehensible form

K^+ key – public knowledge

$K^+(m)$ ciphertext, encrypted with key - an incomprehensible form

K^- key – secret knowledge

Public key encryption algorithms

requirements:

1. need $K_B^+(\cdot)$ and $K_B^-(\cdot)$ such that

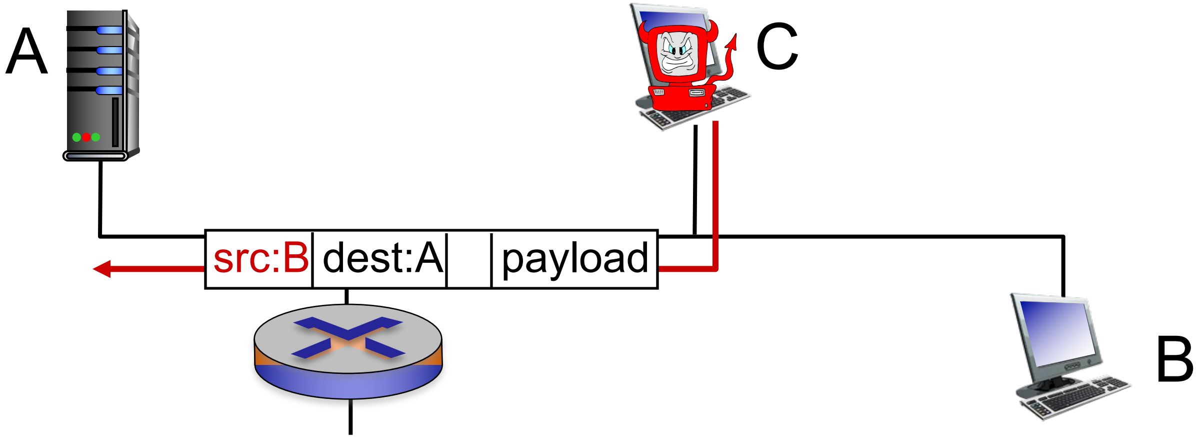
$$K_B^-(K_B^+(m)) = m$$

2. given public key K_B^+, it should be impossible to compute private key K_B^-

RSA: Rivest, Shamir, Adelson algorithm

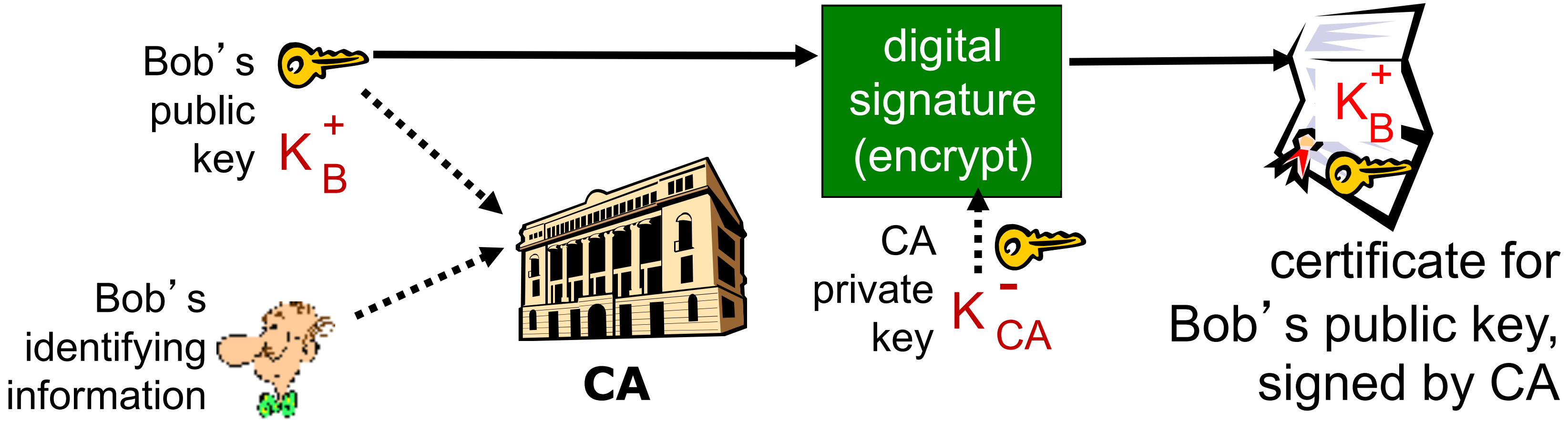
What about server identity?

- How do we know the MQTT server we are connecting to is not spoofing?

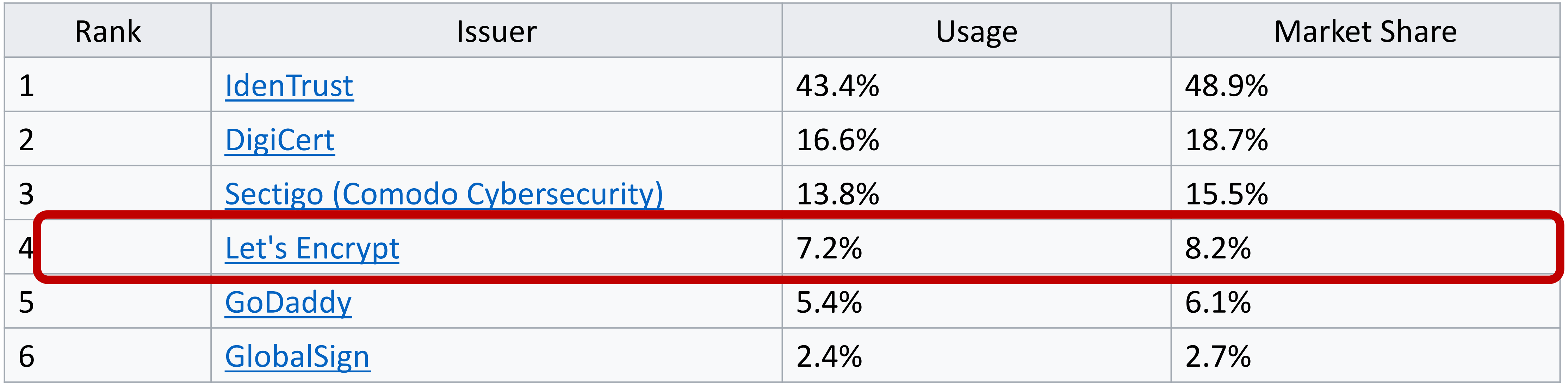


Certification Authorities (CA)

- Binds public key to particular entity, E.
- E (server, person, router, sensor) registers its public key with CA.
  - E provides "proof of identity" to CA.
  - CA creates certificate binding E to its public key.
  - certificate containing E's public key digitally signed by CA – CA says "this is E's public key"


Bob's public key K_B^+
Bob's identifying information
CA
digital signature (encrypt)
CA private key K_{CA}^-
K_B^+
certificate for Bob's public key, signed by CA

Certification Authorities (CA)



Rank	Issuer	Usage	Market Share
1	IdenTrust	43.4%	48.9%
2	DigiCert	16.6%	18.7%
3	Sectigo (Comodo Cybersecurity)	13.8%	15.5%
4	Let's Encrypt	7.2%	8.2%
5	GoDaddy	5.4%	6.1%
6	GlobalSign	2.4%	2.7%

https://en.wikipedia.org/wiki/Certificate_authority

MQTT Encryption

- http://www.steves-internet-guide.com/mosquitto-tls/
  - Will not be asked in the exam/quizzes to do this

Can a system be 100% secure?

- **No!**
- There are a lot of cool research about this
  - If interested in security research, contact

Dr Kanchana Thilakarathna

kanchana.thilakarathna@sydney.edu.au

Summary

- Understand why security is important
- CIA Triad and different tools
- Vulnerabilities at different components and possible solutions