Big Data and Maritime Cyber Security

Mr Adrian Venables

Lancaster University

Introduction – Adrian Venables

- Phd researcher at Lancaster University, UK
  - ‘The changing character of power projection and maritime security in a digital age’
- 24 years service in Royal Navy
  - Communications, Electronic Warfare and Intelligence officer
- Commander, Royal Naval Reserve
  - Communications, Intelligence and Cyber Operations
  - Researcher at the UK Defence Cyber School
- Self employed cyber security consultant
  - Government and industry clients

Lancaster University

Outline

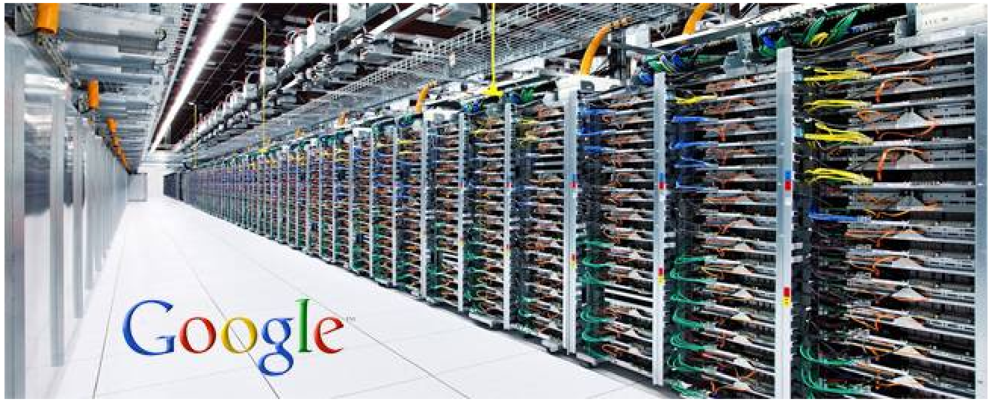
- What is Big Data and the security issue?
  - How your data is collected?
  - How is your data processed and stored?
- Using Big Data to secure your organisation

Outline

- What is Big Data and the security issue?
  - How your data is collected?
  - How is your data processed and stored?
- Using Big Data to secure your organisation

Characteristics of Big Data

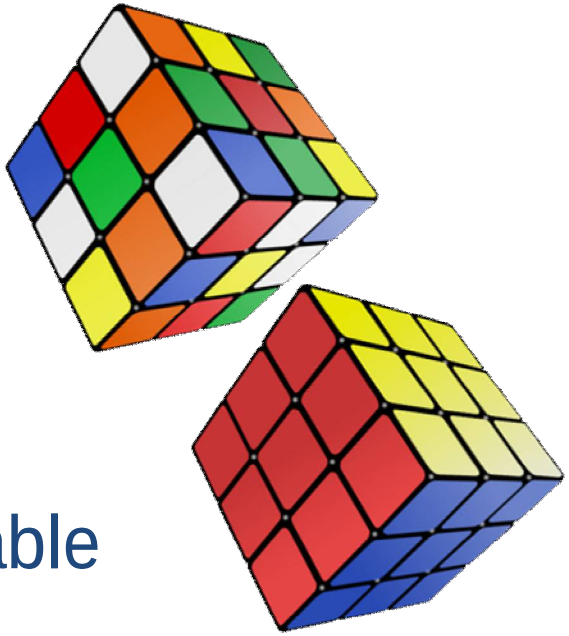
- What is 'Big Data'?
- Defined by IBM as
  - – Volume – most companies have at least 100 Tb
  - – Velocity – modern cars have around 100 sensors
  - – Variety – text, numeric, static or transient
  - – Veracity – accurate, approximate or false



http://www.ibmbigdatahub.com/sites/default/files/infographic_file/4-Vs-of-big-data.jpg

Characteristics of Big Data

- Unstructured – unorganised
  - Text, dates, facts
  - Designed for humans
  - Semantic issues over interpretation and meaning
  - Cultural and linguistic differences
- Structured – organised
  - Stored in databases, readily searchable
  - Designed for computers to process
  - Easily and accurately processed



The benefits of Big Data

- New levels of automation
  - More efficient
  - More economical
- Remote access and monitoring
  - Quicker response times to failures & defects
  - Lower infrastructure costs
- Dig data collection
  - Understand the enterprise
  - Reduce wastage
  - Faster diagnosis of faults

The Big Data security issues

- Security of data collection devices
  - – Are they hackable?
- Security of data transportation
  - – Can it be intercepted or altered?
- Securing of storage
  - – Who else is benefitting from your data?
- Security of processing
  - – Are your algorithms protected?

www.learningtree.com

Lancaster University

Outline

- What is Big Data and the security issue?
  - How your data is collected?
  - How is your data processed and stored?
- Using Big Data to secure your organisation

The Issue for the maritime industry

- Traditionally the maritime industry was low data
  - Analogue, mechanical systems
  - Low bandwidth with little or no data communications
- Digitization has led to increased data flows
  - 90% of data in world created in last two years*
  - Every day 2.5 quintillion bytes created (2.5 x 10^{18})
  - More devices connected by the ‘Internet of Things’
    - 20 – 40 billion devices by 2020
- This presents new opportunities and challenges

Lancaster University

Maritime Big Data – where it comes from

- Remote monitoring of systems
- Condition-based maintenance
- System performance monitoring & optimisation
- Fuel consumption information
- Crew data – business and personal
- Navigational information
  - PNT / AIS / VDR
- Data analytics (meta data)
  - Data about data

The risks with data collection

- Data collection devices may be vulnerable
- Organisations rarely redesign their infrastructures
  - Rely on legacy systems not designed to be connected
  - Previously unexploited vulnerabilities become exposed
- New monitoring devices can be rushed to market
  - Security implications not considered
  - Little understanding of risks they bring
  - Risks may vary depending on how used
  - Security is another cost, so is often avoided

The risks with data collection

- Monitoring devices may be cheap with little memory
  - Less code scrutiny for security considerations
- Minimal computing power & energy consumption
  - Cannot process security algorithms
- Not designed to be updated
  - Vulnerabilities remain unpatched
- Can data collection devices be accessed from within or outside your network?

Lancaster University

Maritime Big Data – what you do with it

- Your data is valuable, both to you and adversaries
  - Competitors for market advantage
  - Criminals for financial gain
- It can also potentially improve your profitability
- It can also reveal your vulnerabilities
- You need to protect it as a valued resource

www.itsecurityguru.org

www.learningtree.com

Lancaster University

Maritime Cyber Security

- The core issues are the same as any other industry
  - No need to reinvent the cyber security industry
- However, there are specific maritime issues that we need to be aware of in your collection devices
  - Outdated hardware / software updates and patching
  - Anti virus software
  - Backups in multiple locations including offline
  - Bandwidth
  - Crew rotation

www.touchstore.ie

Lancaster University

Outline

- What is Big Data and the security issue?
  - How your data is collected?
  - How is your data processed and stored?
- Using Big Data to secure your organisation

Maritime Big Data – where does it go?

- Where is your data stored and who has access?
- In your organisation
  - – Read/write access to data
  - – Read/write access to processing algorithms
  - – Read/write access to output
- In a ‘cloud storage’ provider
  - – What does the contract say?
  - – Have you audited them?

zipcloud
box
justcloud.com
bitcasa INFINITE STORAGE
Dropbox
OneDrive
IDrive
Google Drive
MediaFire
iCloud

Maritime Big Data – where does it go?

- What do your suppliers do with your data?
- Your ships and their sub systems
  - Who owns it?
  - Who has access to it?
  - Is it identifiable?
  - Is it properly secured?
  - Is it used for your analytics?
  - Wider industry trends?

www.korolit.com

Who wants your data?

- State actors seeking international advantage
- Competitors seeking local advantage
- Criminals wanting to make money
- Hacktivists wanting to embarrass you
  - Political/religious/ideological
- Terrorists intent on disrupting your business
- ‘Script Kiddies’ testing their skills
- Insiders or former employees wanting revenge

The insider threat

- 28% of all cyber attacks and 38% of targeted attacks involve insider malicious activity
- Insiders may be
  - Self motivated – unhappy, disgruntled, poorly led
  - Blackmailed through personal behaviour or weakness
  - Incentivised by money
  - Unintentional
- Insiders can be targeted through open sources, social media or compromised databases

To encrypt or not to encrypt

- Encrypting data at rest protects from physical theft
  - – Will not protect from those inside your networks
- Encryption in transit presents issues
  - – Protects from Man in the middle attacks
  - – Prevents network monitoring
  - – Adds to processing overhead

Big Data classification

- Knowledge of data ownership vital
- Data classification depends on
  - Assignment of a level of sensitivity to data
  - Value or importance of the data
  - Results in the specification of controls for each level
- Distinguish between
  - Commercial
  - Personnel
  - Personal
  - Compliance issues

Information and Data

- Information and Data are not the same
- Information is processed data
  - Basis for Business Intelligence
  - Can be more valuable than unprocessed data
  - Therefore should be classified higher

Outline

- What is Big Data and the security issue?
  - How your data is collected?
  - How is your data processed and stored?
- Using Big Data to secure your organisation

Lancaster University

Big Data and cyber security

- How to secure your information?
  - Keeping your data safe at rest
  - Secure data collection and transit
  - Identifying threats
- Using Big Data to analyse and predict security incidents

www.digipaypolutions.com

Lancaster University

Big Data and cyber security

- Conventional methods
  - Threat intelligence to identify areas of risk
  - Intruder Prevention Systems (IPS) to halt attack
    - Firewalls
  - Intruder Detection Systems (IDS) to identify attack
    - Log analysis tools
  - Security Incident and Event Management (SIEM)
  - Use of Cyber Security Operations Centres (CSOC)
    - Coordinated security with dedicated teams

Big Data to improve security

- Dig data can supplement or replace traditional measures by using the information available
- Analysis from multiple sources gives greater advanced warning of incidents
- Big Data shows what is ‘normal’
  - Enables better indication of abnormal
- Can identify anomalies using pattern analysis for detecting
  - Fraud
  - Advanced Persistent Threats

Lancaster University

Big Data to improve security

- Not all SIEM can cope with Big Data input
  - Quantity and range of information types too great
  - Around a million new types of malware annually
  - 300 000 malicious files reported to SophosLabs daily
  - Some tools do not scale well
- Apache Hadoop commonly used platform
  - Open Source framework for processing Big Data sets

Final thoughts

- Big Data can provide the maritime industry with
  - Improved performance and optimisation
    - Savings and profit
  - Improved overall security
- Big Data does have overhead though
  - Collection, transmission and storage needs
  - In house or outsourcing analysis
  - Security of raw data, processed information & its business implications must be considered as part of overall business case

Thank you for listening

https://www.stickermule.com/marketplace/3442-there-is-no-cloud

Adrian Venables. e-mail: a.venables2@Lancaster.ac.uk

Lancaster University