GRAD Driving Innovation for Safer Maritime Navigation

Maritime Cyber-Security…

What is the problem and what can be done about it?

G Wimpenny, J Šafář, A Grant, M Bransby

General Lighthouse Authorities of the UK and Ireland, Research and Development

The Royal Institute of Navigation's, International Navigation Conference, 20 November 2019 – Edinburgh, UK

Cyber-Security

GRAD Driving Innovation for Safer Maritime Navigation

- Protect computers, programs, communications networks and data from attack, damage or unauthorised access.

- Affects us all in all walks of life.

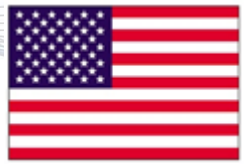
- **Maritime** Cyber-Security has lagged behind,
  but guidance has been published in recent years, such as:

IMO Guidelines on cybersecurity on board ships (MSC 96/4/1)

- International Maritime Organisation February 2016

Code of Practice Cyber Security for Ports and Port Systems

- UK Department for Transport (commissioned by) August 2016



The Application of Cybersecurity Principles to Marine and Offshore Operations *- American Bureau of Shipping February 2016*

Maritime Cyber Threats

GRAD Driving Innovation for Safer Maritime Navigation

Image Credit: Wikimedia Commons

"A cyber-threat is expected to cause a loss of life at sea"

– Admiral Lord West

Many attacks aren't high profile, but cause disruption and financial loss on a daily basis

"The insurance industry may come to regard a vessel as unseaworthy if appropriate cyber-security measures are not taken"

– Legal panel discussion, Maritime Cyber Risk Conference, London 2016

Understanding the problem - IT and OT

GRAD Driving Innovation for Safer Maritime Navigation

IT: Information Technology
Used for manipulation of data

OT: Operational Technology
Used to control physical processes

Understanding the problem - a generic example

GRAD Driving Innovation for Safer Maritime Navigation

Control Room

IT: Risks Addressed?

TCP/IP Link

IT: Risks Addressed?

Out Station

OT: Vulnerable?

Radio Link

RF: Vulnerable?

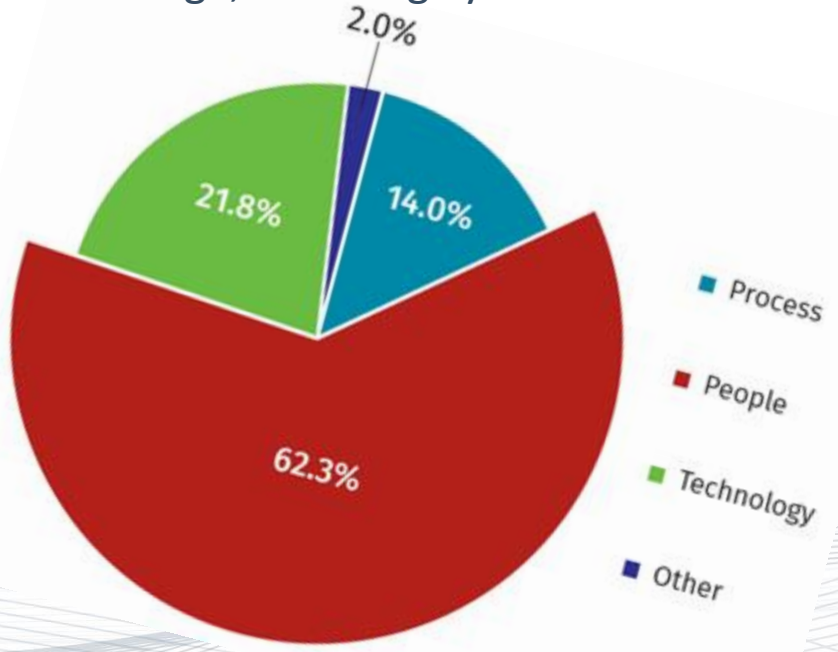
End User

Understanding the problem - how & why attacks occur

GRAD Driving Innovation for Safer Maritime Navigation

- Many attacks are untargeted (automated scripts)
  - You are at risk, even if you think you are not!
- More sophisticated targeted attacks may be conducted for many reasons
  - *Inter alia*, extortion, theft, industrial espionage or to cause disruption and damage, including cyber-warfare.

"What element do you consider to be at the greatest risk for compromise to your Operational Technology / control systems?"



SANS State of ICS Security Survey 2019

OT and IT Integration - a very human problem

- OT increasingly
  - has remote (internet) access
  - uses ‘standard’ IT operating systems, hardware and software

…this makes OT systems increasingly vulnerable to ‘IT like’ attacks

However….

OT and IT staff have differing backgrounds, priorities and training which are unlikely to foster an understanding of each others roles and responsibilities…

Defending Against OT Attack

- Government OT security guidance available to protect critical national infrastructure….. published by:
  - UK National Cyber-Security Centre (NCSC)
  - French Network and Security Agency (ANSSI)
  - Swedish Civil Contingencies Agency (MSB)

- Technical advice to protect, detect and respond to cyber-attack
- The human problem:
  - Procedural and managerial advice: physical locks
  - Overcoming the OT / IT staff barrier:
    Embed staff in each others departments for a period

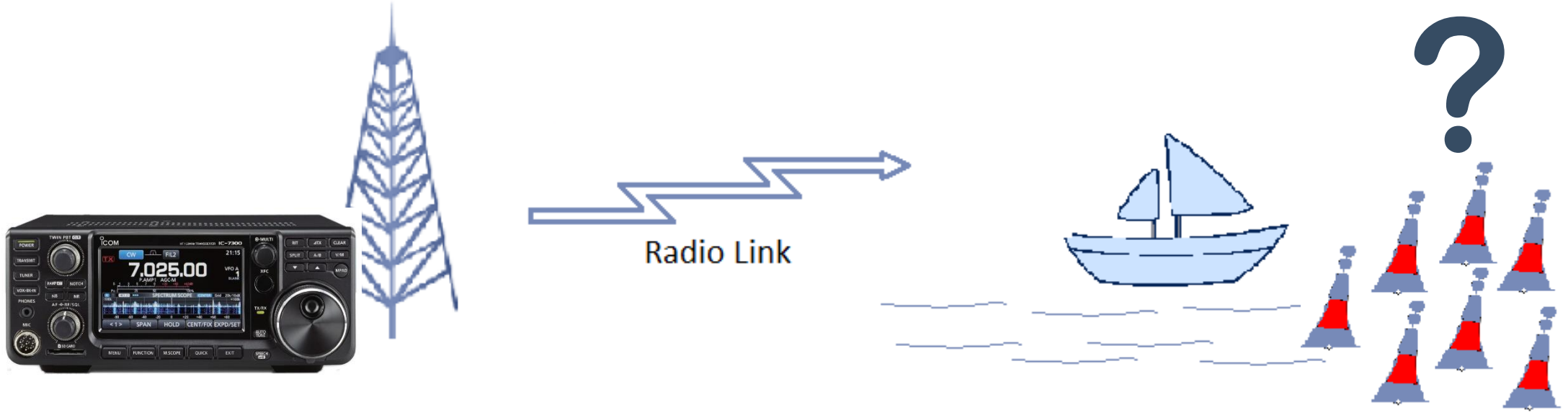
The Human Problem

Encourage a culture of cyber-security
the same way we encourage a culture of safety

- Cyber-Risk assessments before working.
- Take immediate action if poor cyber-security is identified
  ….don’t ignore it or leave it to someone else
- Report security breaches and near misses ….make it easy to report
- Give staff confidence concerns will be listened to and acted on
- Encourage staff to seek advice if unsure
- Be responsible for your own and others cyber-security
- Consider a ‘permit to work’ scheme

Unauthenticated Communications

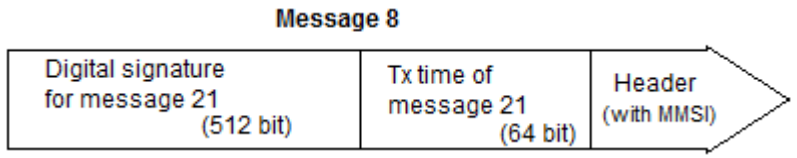
GRAD Driving Innovation for Safer Maritime Navigation

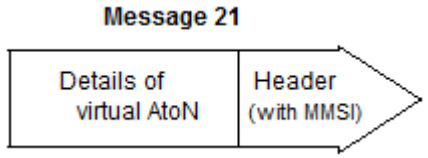


- Many data links not authenticated and vulnerable to spoofing
- Includes AIS
  - Allows spoofing of vessels (AIS Message 1,2,3)
  - Allows spoofing of Virtual Aids to Navigation (AIS Message 21)
  - Allows spoofing of differential GNSS corrections (AIS Message 17)

AIS Authentication

GRAD Driving Innovation for Safer Maritime Navigation





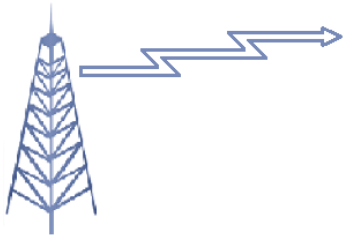
- Signature ensures message integrity and authenticity
  - Use the ECDSA cryptographic algorithm with a 256-bit public key and SHA-256 hash function
- Timestamp links messages and prevents replay attacks

PUBLIC KEY AUTHENTICATION FOR AIS AND THE VHF DATA EXCHANGE SYSTEM (VDES)
G. Wimpenny, J. Šafář, A. Grant, M Bransby & N. Ward (ION GNSS 2018)

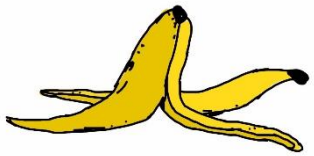
Conclusions

GRAD Driving Innovation for Safer Maritime Navigation

- Operational Technology (OT) is vulnerable to cyber-attack
  - A poor understanding and culture clash exists between IT and OT staff
  - Government advice is available to secure OT



- All data communications need to be authenticated
  - GRAD has proposed a technique to authenticate AIS and VDES



- Security is human problem, not just a technical problem
  - Encourage a cyber security culture
  - Encourage it the same way we promote a safety culture (cyber-risk assessments)

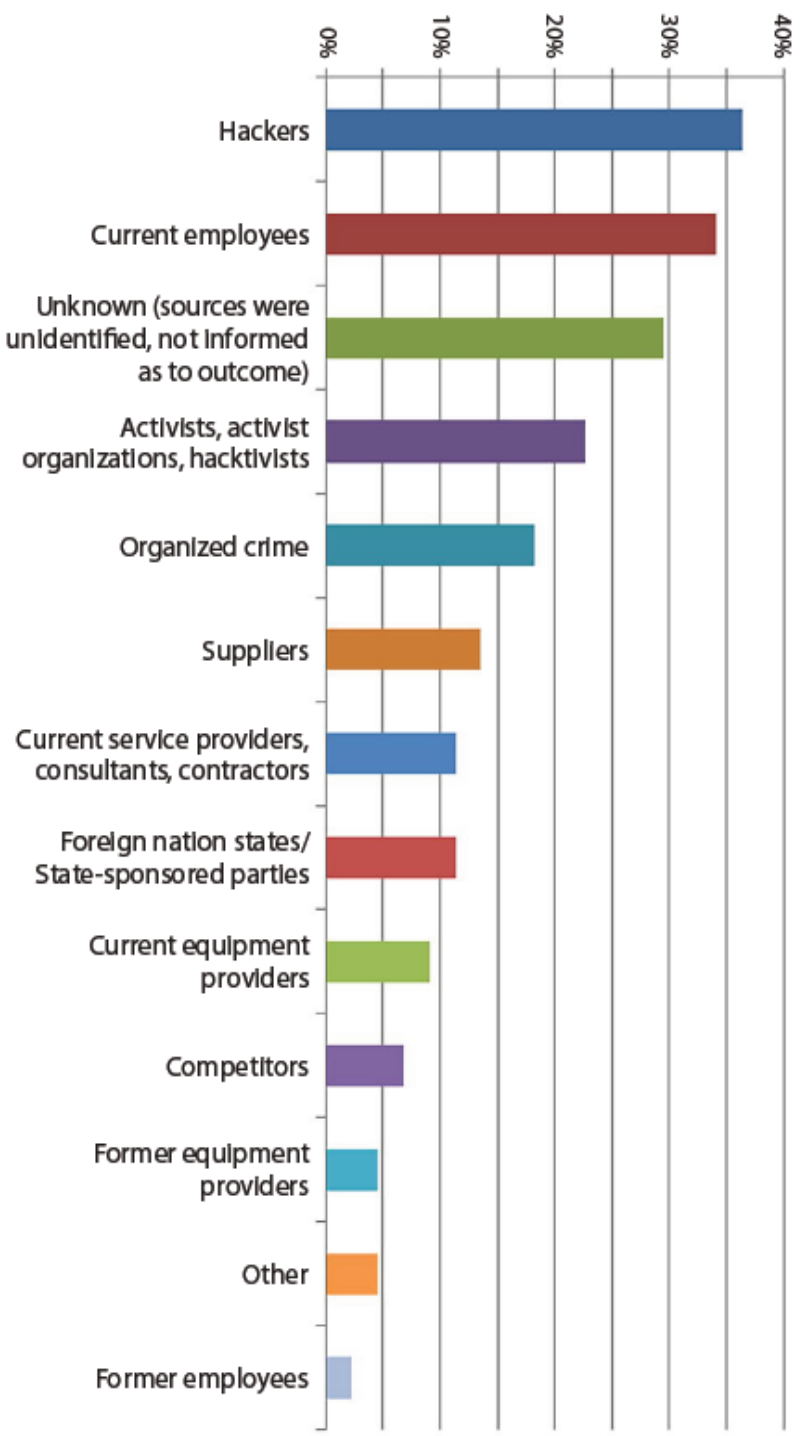
Thank you

GRAD Driving Innovation for Safer Maritime Navigation

G. Wimpenny, J. Šafář, A. Grant & M. Bransby
General Lighthouse Authorities of the UK and Ireland
Research and Development Directorate

Martin.bransby@gla-rad.org
T: 01255 245042
M: 07770 265652

Backup Slides



GRAD Driving Innovation for Safer Maritime Navigation

Understanding the problem

- Many attacks are untargeted (automated scripts)
  - You are at risk, even if you think you are not!
- More sophisticated targeted attacks may be conducted for many reasons

Graph: SANS State of ICS Security Survey 2016