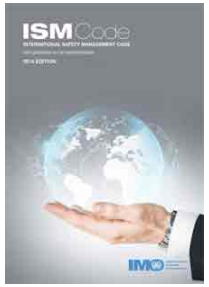
Cybersecurity from a corporate perspective

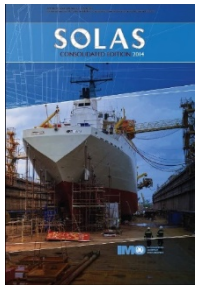
Noel Koutlis
Research & Development Department Danaos Shipping

Topics in this presentation

- Maritime industry view
- insiders and outsiders in a corporate environment
- internet of things - hundreds of sensors in vessels – IMO FAL 38/7
- telecommunications systems - the weak wireless part & encryption – MitM
- passwords - interesting facts - biometric passwords, pictures etc
- injections, sessions that stay open, misconfigurations, penetration tests
- digital forensics
- backup and disaster recovery systems

Current situation





- **International Safety Management Code (ISM)**
- **International Ship and Port Facility Security Code (ISPS)**
  (part of SOLAS Chapter XI-2 – Special measures to enhance maritime security)
- The Industry Guidelines on Cyber Security (ICS, BIMCO, INTERTANKO, INTERCARGO, CLIA) on board Ships to be considered by the Maritime Safety Committee 96 in May 2016. This guidance to ship owners and operators includes how to minimize the risk of a cyber-attack through **user access management**, **protect on board systems**, **develop contingency plans, awareness and education and also manage incidents if they do occur**.
- International Electrotechnical Commission prepares a standard which is an add-on to the existing interconnection standard, which specifies a method by which navigational and radiocommunication equipment can be safely interconnected using an Ethernet network on a ship.
- Regarding the draft proposal for a directive (NIS Directive - COM 2013 48 final/7.2.2013) to include maritime companies and vessels the view of European Community Shipowners Association and our union is the complete removal of vessels and maritime companies for the directive's implementation

Awareness and education

- Establishing awareness of why owners, seafarers and other stakeholders should spend time and attention on cyber security is essential.

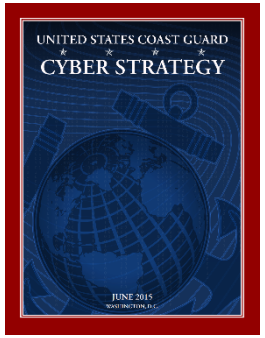
- Guidelines for the personal use of email, software, and social media to keep sensitive information in safe custody must be addressed. For example, information about cargo or a ship's movements may be of interest to criminals. So it is essential for cyber security that everyone concerned is educated on how to avoid such vital information being intercepted.

- Further, education and training should address software systems which are critical to the safety of the ship such as navigation, steering control, communication and cargo systems and how to protect them against introduction of malware. Safe use of such systems in manual mode must be trained.

- Education and training should be tailored to the appropriate levels for:

- Master, officers and crew : Organization including management ashore, Major stakeholders in the supply chain such as charterers, classification societies and service providers

US Coast Guard (USCG) new Cyber Strategy (June 2015)



- Prevention and Response strategy
- The strategy obligates the USCG **to collaborate with industry on cyber issues using area maritime security committees to provide recommendations** for area maritime security plans (AMSP) and the National Maritime Transportation Plan (MTSP)
- The USCG's position is that Maritime Transportation Security Act of 2002 (MTSA) provides it with the authority to develop and implement a Cyber Strategy – in effect directing the formulation of best practices or a new standard of care for an organisation in managing cyber risks.
- The USGC views cyber risk prevention and response as operational responsibilities of management, not the IT department.
- Leadership will be expected to establish a reasonably viable cyber risk management programme, one that includes continuous assessment, co-ordinated planning, investment, benchmarking, training and possibly risk transference, for example, cyber insurance.

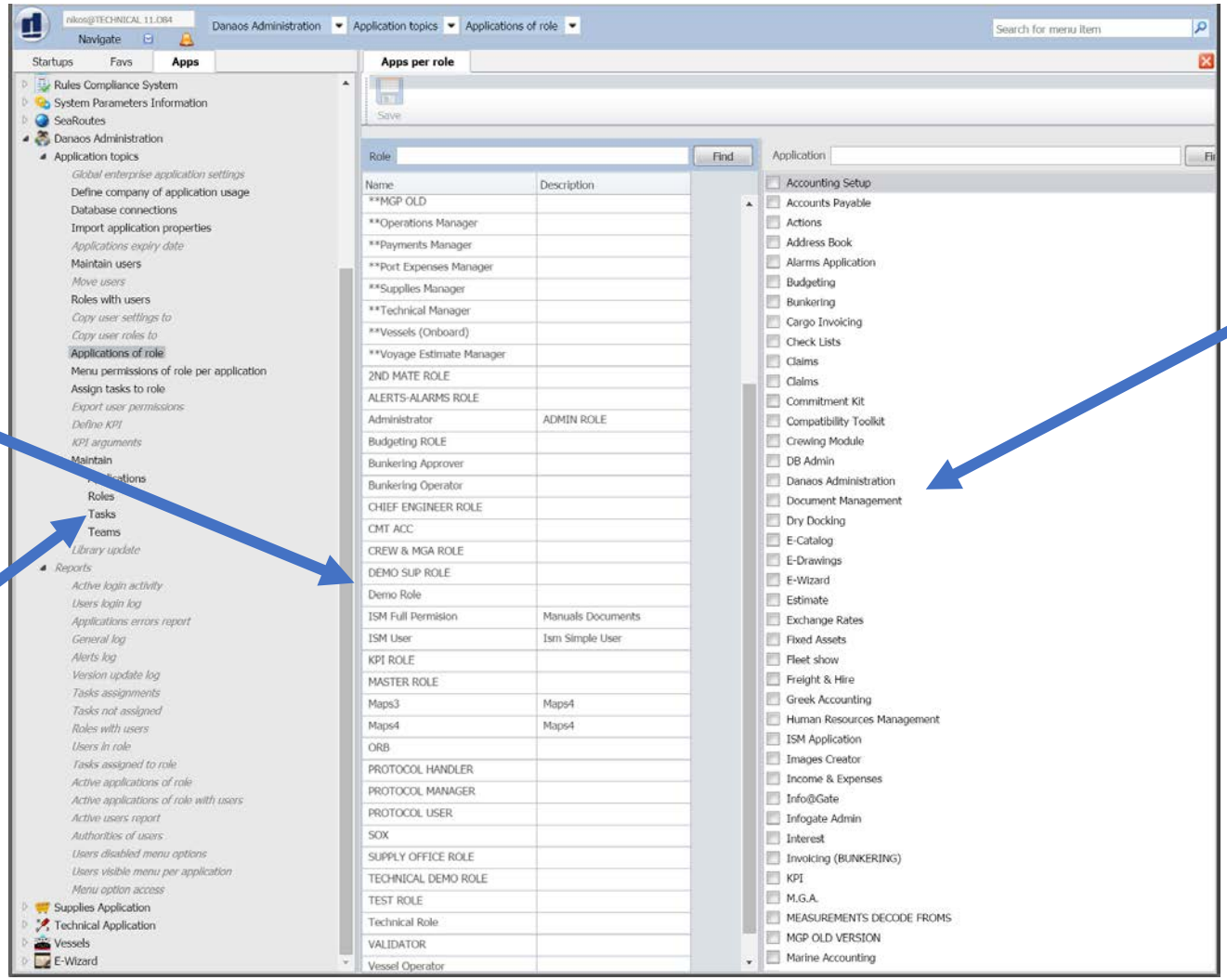
insiders and outsiders in a corporate environment

TRUST	OUTSOURCING	SUPPORT
• HR PSI-TEST • STRANGE BEHAVIOUR • EDUCATION	• PARTNERS • SUB-CONTRACTORS • AGENTS	• REMOTE DESKTOP • VNC / TV etc

Role Based Security and Access Control

Application Roles

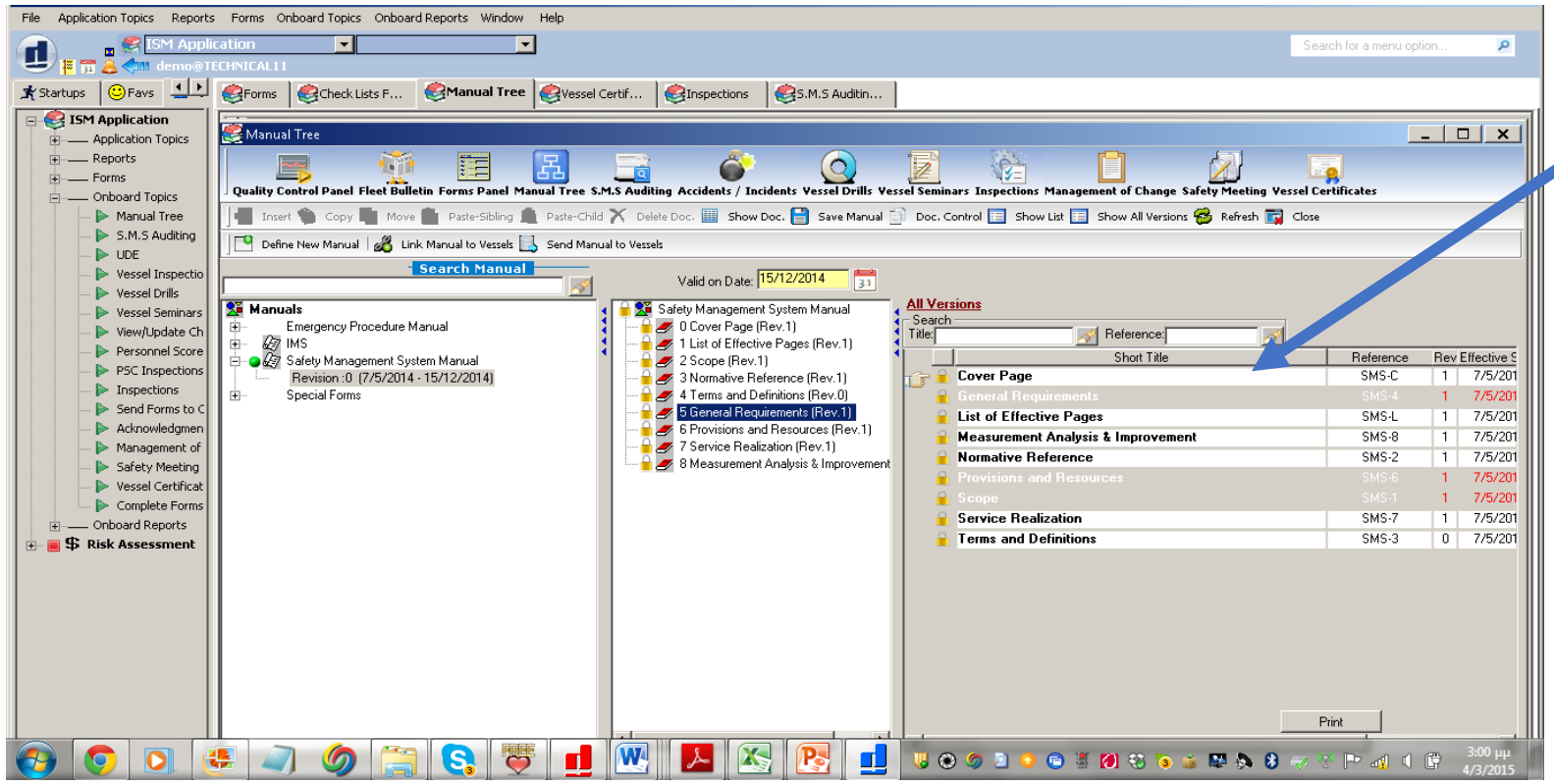
Tasks inside an Application



Applications the role can see

Safety Management Systems

- Quality Control Systems
- Compliance Toolkits



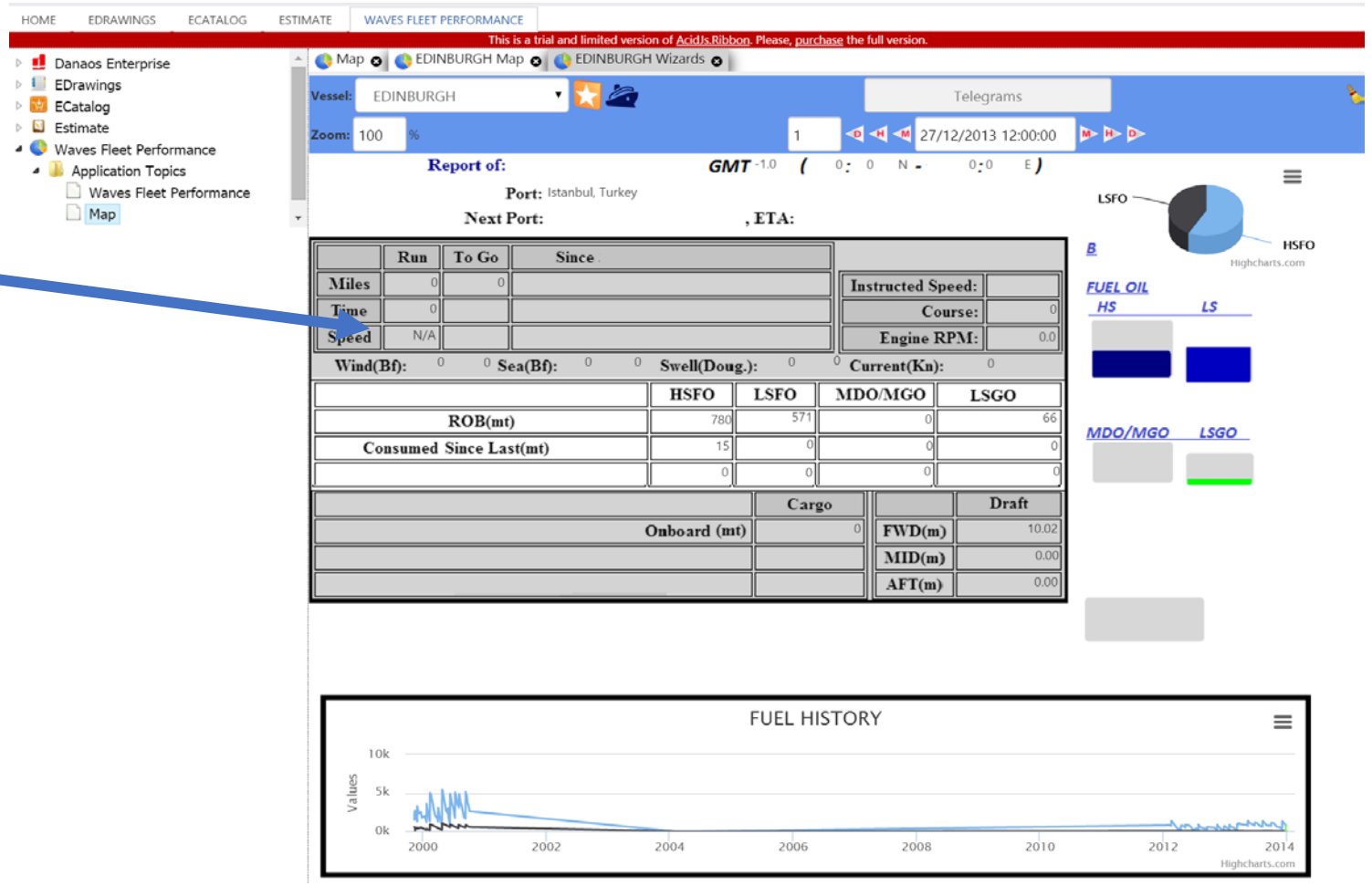
Electronic versions of onboard manuals

Internet Of Things
- hundreds of sensors in vessels

- As devices multiply, so do security risks
- Machine failure can be predicted *(case of propulsion analytics)*
- Sensor failure can also be predicted *(case of paper)*
- Example of a Performance Monitoring System

internet of things – waves dashboard

Sensor output
In a dashboard



lMO - FAL 39/7 examples of cybersecurity issues - 10 July 2014

- researchers from the University of Texas in the United States demonstrated in July 2013 that it is possible to change a vessel's direction by interfering with its GPS signal to cause the onboard navigation systems to falsely interpret a vessel's position and heading;
- a hacker caused a floating oil-platform located off the coast of Africa to tilt to one side, thus forcing it to temporarily shut down;
- hackers infiltrated cyber systems in a port to locate specific containers loaded with illegal drugs and remove them from the port undetected;
- Somali pirates employed hackers to infiltrate a shipping company's cyber systems to identify vessels passing through the Gulf of Aden with valuable cargoes and minimal on-board security which led to the hijacking of at least one vessel;
- denial of service attacks (initiating a very high number of requests to a system to overwhelm it and cause it to cease operating) against ports have been reported;
- efforts to gain unauthorized access to wireless Internet networks in ports have been reported;
- studies by the Brookings Institution and the European Union Agency for Network and Information Security both concluded that there is very little awareness of cybersecurity issues in the maritime transportation sector and few initiatives underway to enhance cybersecurity.

Paper: GPS Jamming and the Impact on Maritime Navigation (The General Lighthouse Authorities of the United Kingdom and Ireland)

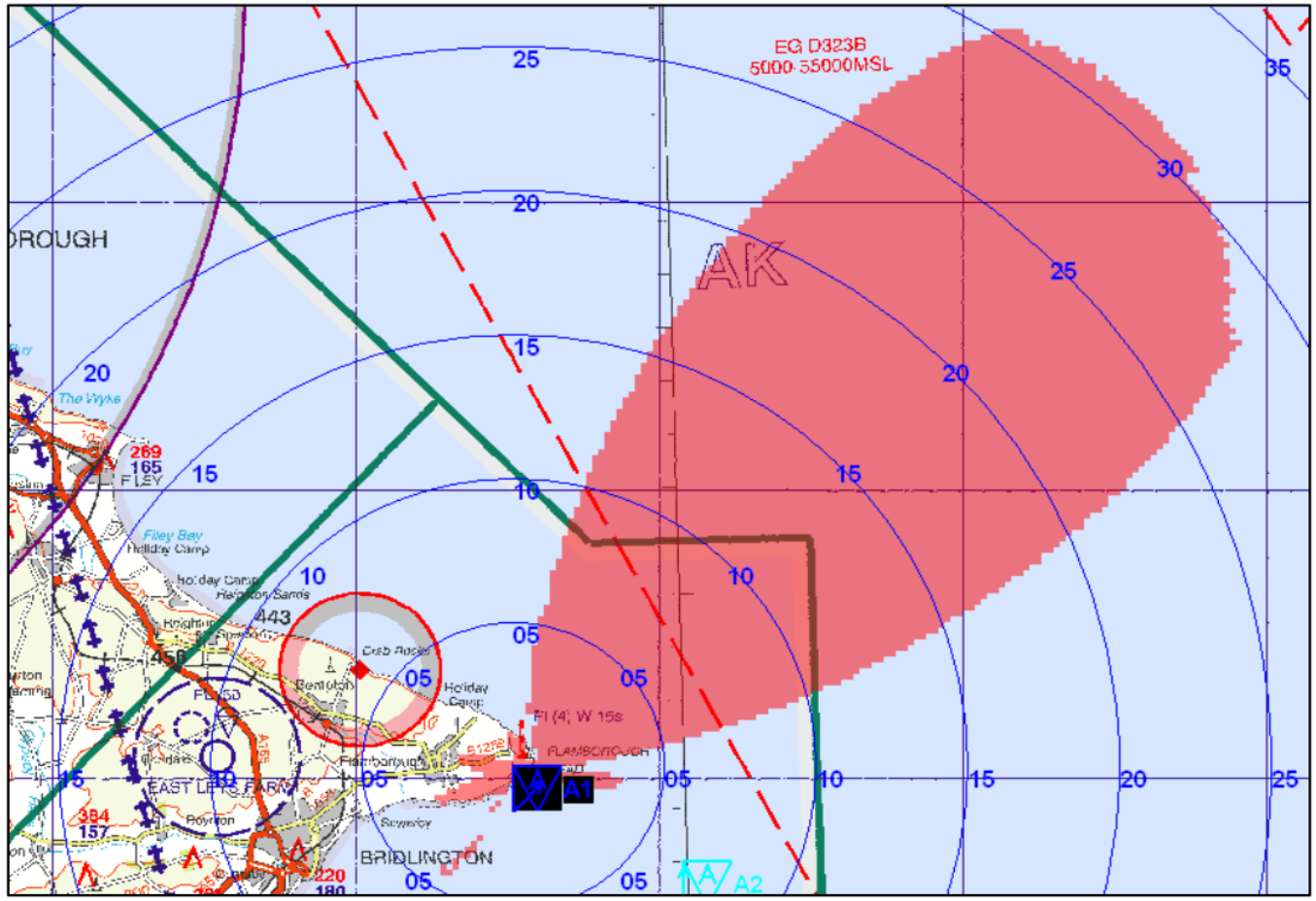


Figure 2 : Coverage area of the GPS jamming unit at 25m above ground level on maximum power of 1.58W ERP. (Image courtesy of DSTL)

Signal Blockers - Jammers

12 Antennas Newest Adjustable WiFi GPS VHF UHF LoJack 3G 4G All Bands Signal Blocker

Price: EUR €569.04
SKU: JFC-021-0102
Rating: ★★★★★ (5 product reviews)
Shipping: Calculated at checkout
Quantity: 1 ▼

Add to Cart

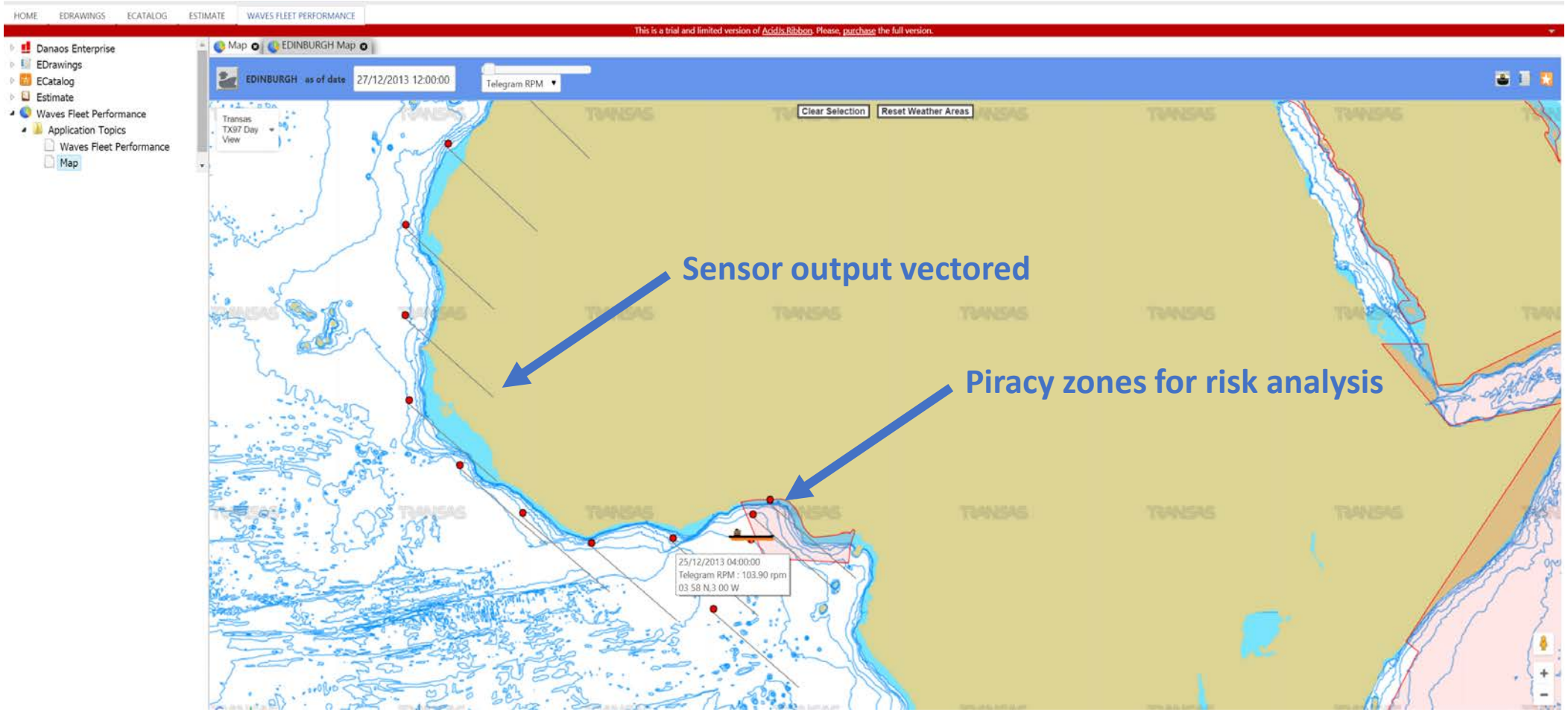
JammerFromChina Wholesales Discount

- Buy 2 - 4 and pay only EUR €557.66 each
- Buy 5 - 8 and pay only EUR €540.59 each

not just a Bob and Alice case anymore

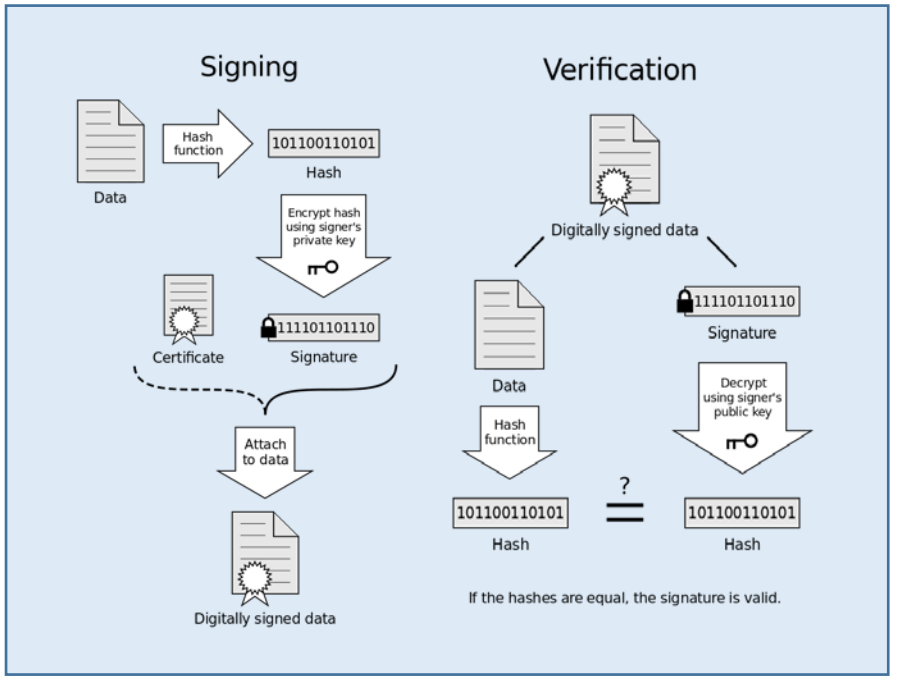
12 Antennas Newest Adjustable WiFi GPS VHF UHF LoJack 3G 4G All Bands Signal Blocker

Sensors, privacy zones, geospatial data, risk analysis



Wireless systems (WiFi in Ports)

- Digital ID’s to ensure the originator
- Authentication systems
- Cryptography to ensure the transmission
- MitM attack works by providing a stronger wireless signal that looks like the originator



passwords - interesting facts

- Most used passwords for **2014** (20 years the same…)
- People need to be educated on security risks

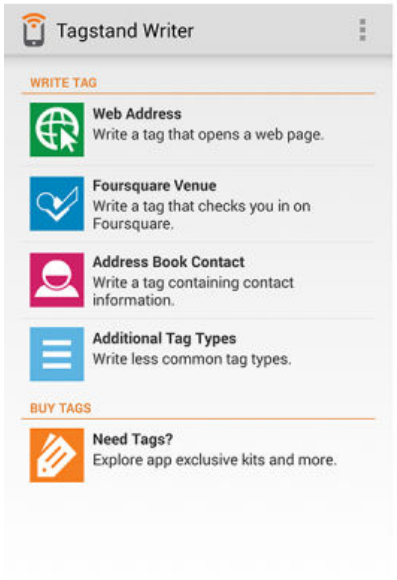
123456 (Unchanged)	**abc123** (Down 9)
password (Unchanged)	**111111** (Down 8)
12345 (Up 17)	16.mustang (New)
12345678 (Down 1)	access (New)
qwerty (Down 1)	shadow (Unchanged)
123456789 (Unchanged)	**master** (New)
1234 (Up 9)	michael (New)
baseball (New)	**superman** (New)
dragon (New)	696969 (New)
football (New)	**123123** (Down 12)
1234567 (Down 4)	batman (New)
monkey (Up 5)	trustno1 (Down 1)
letmein (Up 1)	

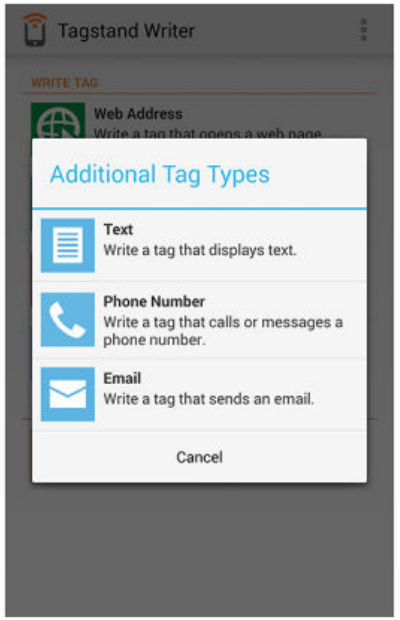
Fast Identity Online (FIDO) Alliance USB key

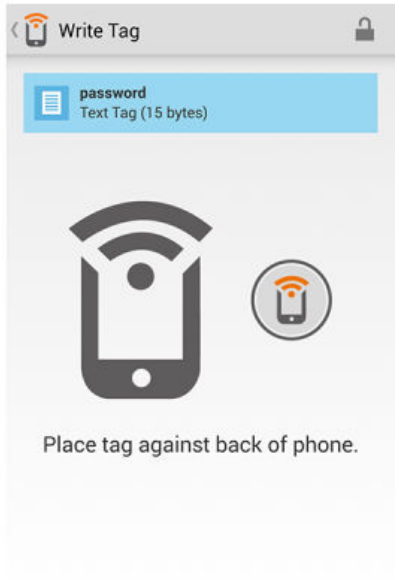
- Solution 1 (backed by Google)

NFC passwords

- Solution 2 (used now in payment systems)







OTP keys

- Solution 3 (used in banking)

QR codes in certificates

- Proposal for a solution for electronic certificates for seamen and vessels
- The Japanese immigration system uses encrypted QR codes when issuing visa in passports
- Bar code copy example

injections, sessions that stay open, misconfigurations, penetration tests

- Google expires a cookies after 2 years
- It was setup to last to 2038 before
- Spending thousands for security software/firewals can prove meaningless without **configuration from an expert**
- Keyloggers, Identity theft, Browser hijacking, Phishing, Typosquatting
- Penetration tests on software, websites, webservices, even physical, social and corporate procedures

Example of Professional Social Networks

- Store data in participant systems instead of the cloud
- Web services on the participant systems are used to create the user interface in the client
- Firewall at each side

Digital forensics

- How do you find the intruder? Evidence? Are traces left?
- Do you keep log files?
- Network monitoring tools, firewals
- Web filtering tools (Barracuda, IronPort etc)
- Fireshark packet analyser
- typical Internet providers keep track history of 1 year

backup and disaster recovery systems

- Do we have a plan B ?
- Our backups and disaster are in the same building?
- Have we ever tested the systems? (a simple restore sometimes is useful)
- Do you have only one communications provider?
- If it can fail, it will fail, eventually..