Hacking Ships

Team of >60 who test ship security @pentestpartners

Several ex-ships crew on the team

Known for red teaming (CBEST), car testing, IoT, ATMs and full-spectrum pen testing

info@pentestpartners.com
+44 (0)20 3095 0500
@PenTestPartners
PenTestPartnersLLP


Hacking
Ship
Satcoms

Finding vulnerable ships

Most ships now permanently connected to the internet

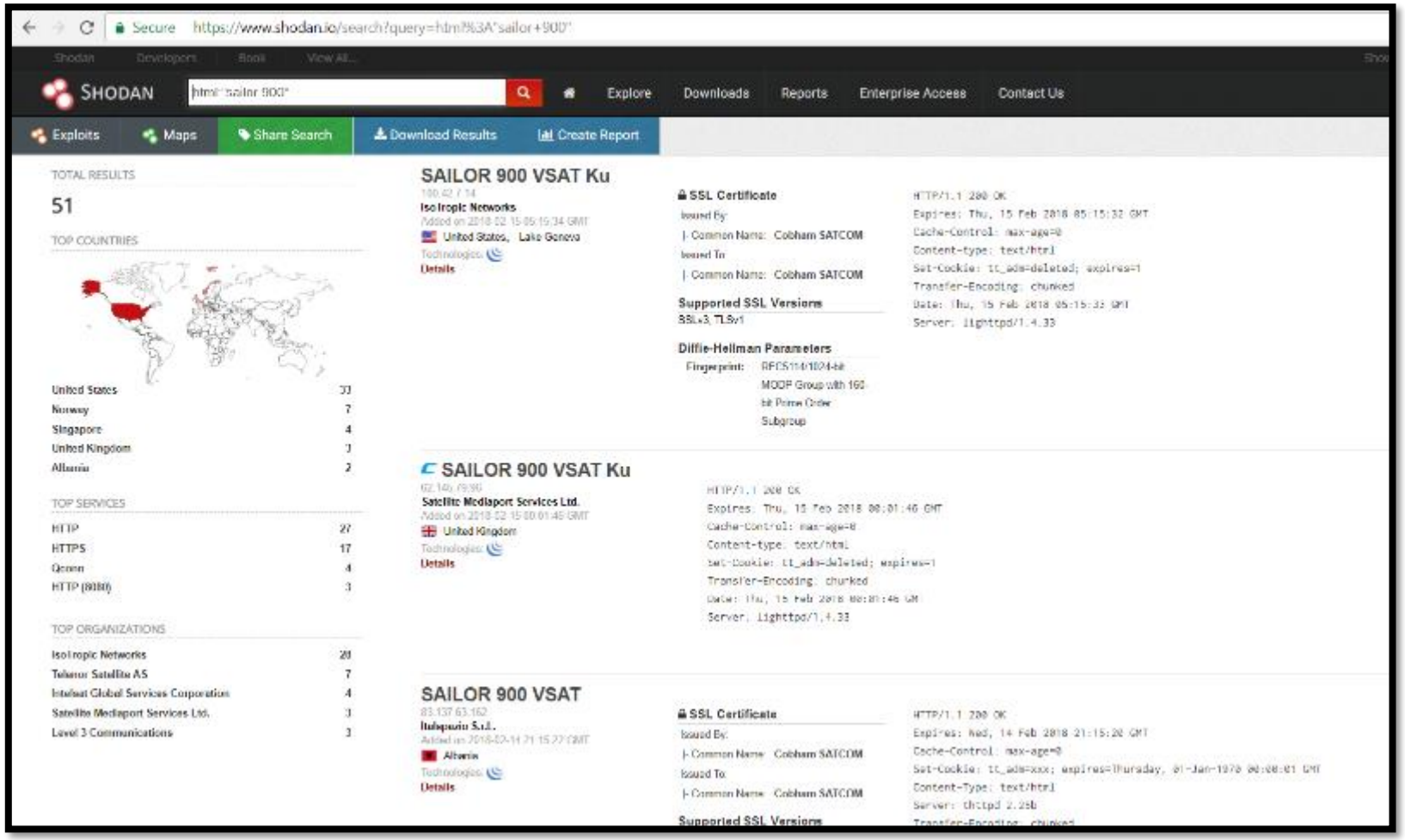
Shodan does it for you:

‘title:sailor 900’

‘Inmarsat Solutions’

‘Telenor Satellite’

‘ssl:commbox.com’



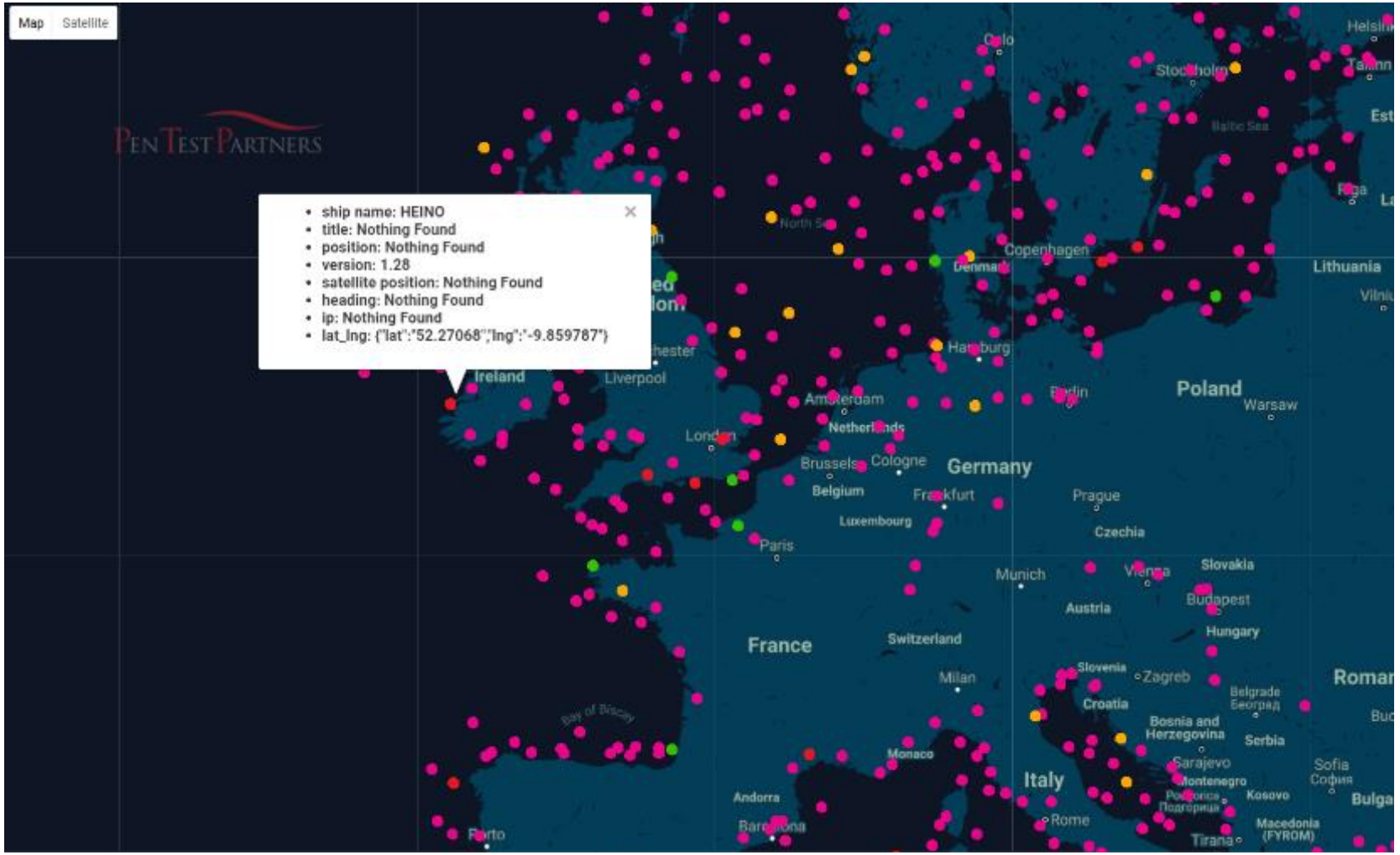
Let’s go one better: a real time vulnerable ship satcom tracker

By collating vulnerable satcom unit data with live AIS data…

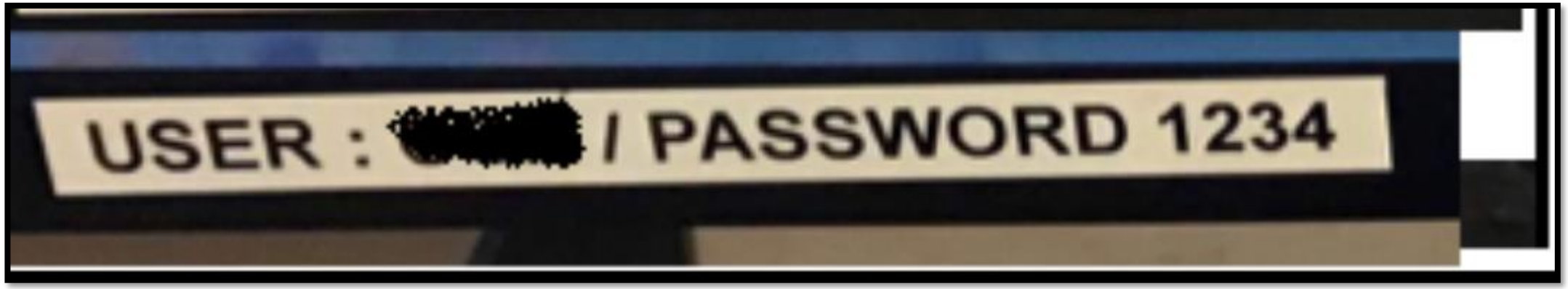
…we can geo-locate vulnerable ships in real time

Here we have a vessel with a very outdated satcom unit that is likely to be highly vulnerable to attack

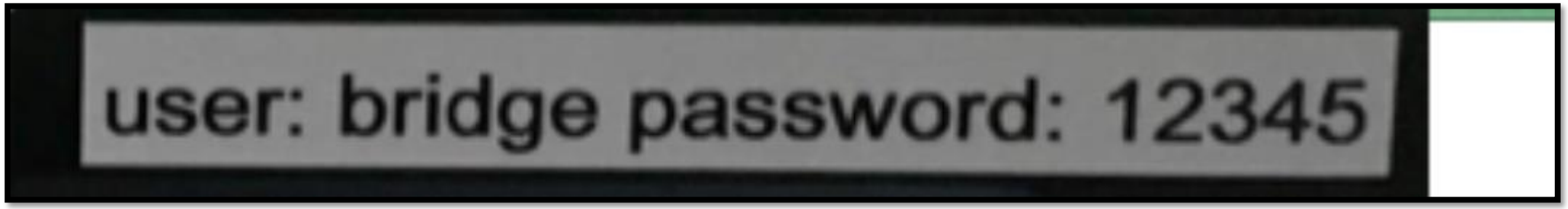
This is all open source data, all we have done is link it up

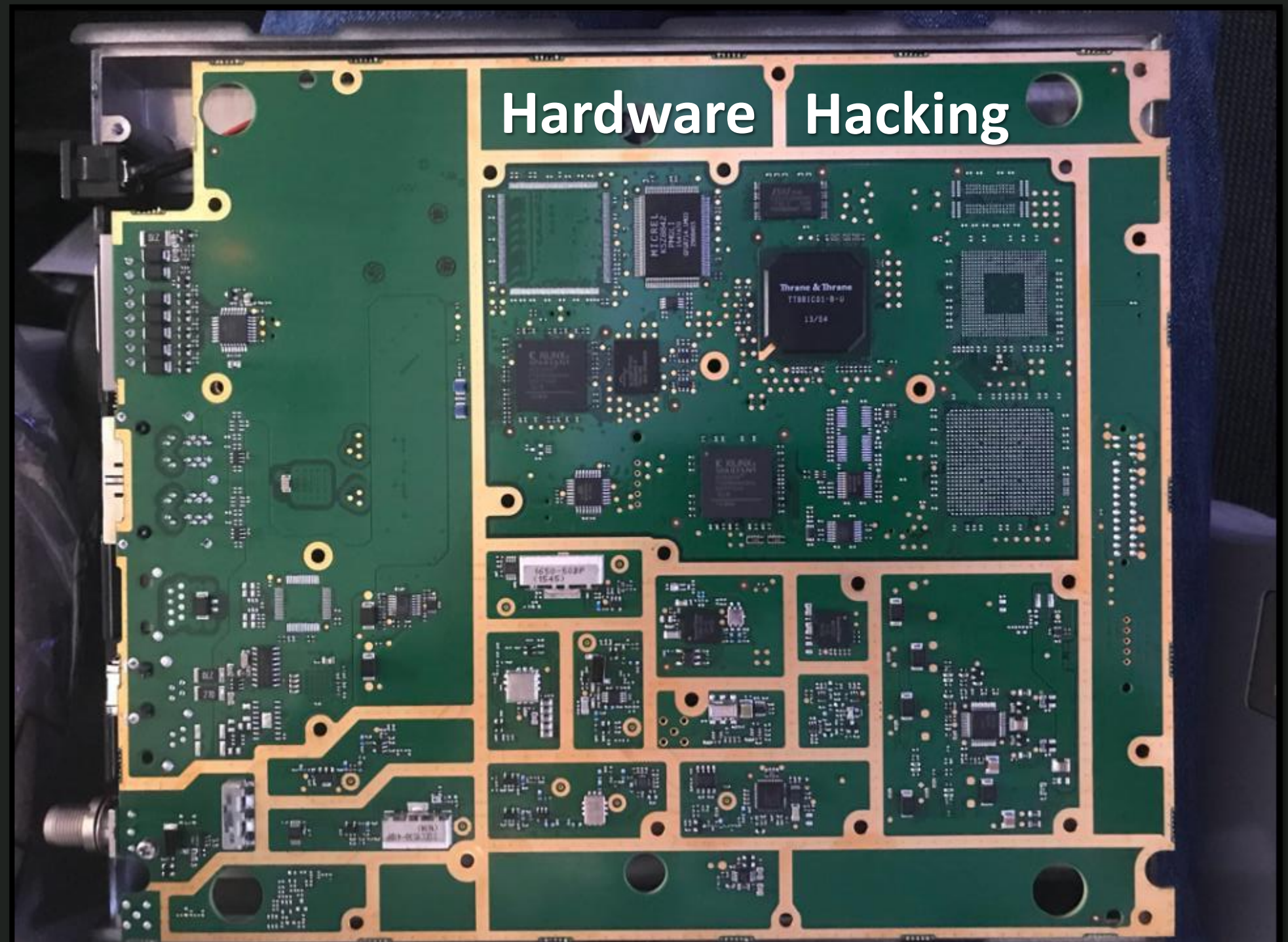


The most common satcom password



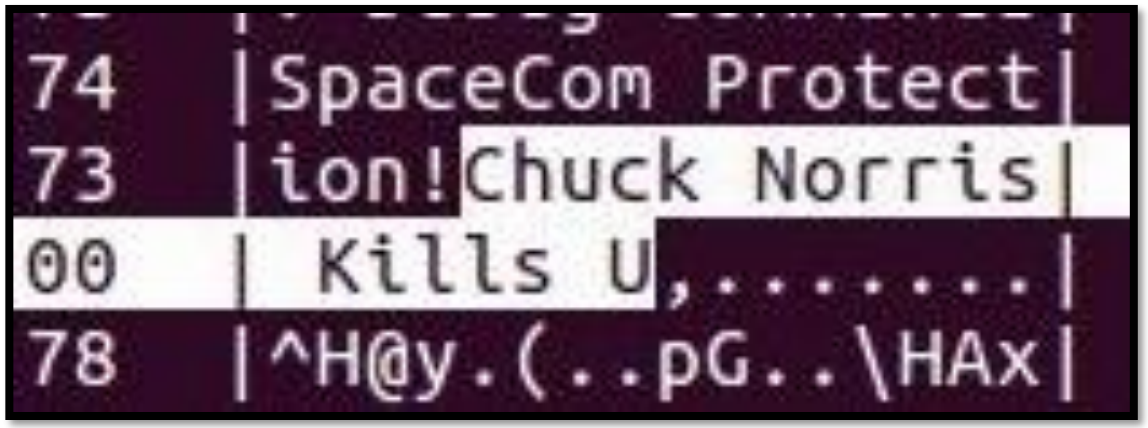
Recent improvement




Hardware Hacking

Satcom terminal hardware

Unsigned firmware, so hacker can roll back the code and introduce vulnerabilities



Telnet & HTTP logins

Privilege escalation, so any user can execute admin commands

All mitigated by changing the admin password!

Phishing Ships

Not secure | 49.128.227.56/commbox.php#

KVH INDUSTRIES

CommBox - Connecting ship and office networks

Important: KVH not at fault here – vessel operator has not updated terminal software in years!

[#] QuickCrew - Show Active Users - Google Chrom...

about:blank

First name	Last name	Session duration	Remaining
Marvin	Andrada	10 Min	40.23 MB
ALCAZAREN	JOHN	0 Min	33.33 MB

Welcome to

CommBox™

- Powered by KVH Industries Norway AS

Please enter your user name and password:

User Name:

Password:

Login

Active Crew Internet Users 2 / 20

Show Users

FBB WAN 2 | FBB WAN 1 | 3G | Open in new window

© KVH Industries Norway AS - Version: 1.12.5 - System name: Dawn Horizon

KVH Industries Norway AS recommends web browsers Firefox and Opera for safer web browsing

Why don’t operators update terminal software?

“New functions in the Cable calibration. Appendix II
Reset of event list in Diagnostic report.
Event log reset without deleting config. Appendix. III
Bearings/friction test for all axis
General improvements of security for "admin" account.
New ‘Local Admin’ activation.”

Login bypass!

Important security updates are often ‘hidden’ in changelogs, so the operator doesn’t realise

It won’t happen to me…

Why would a hacker attack my ships?

Surely it's easier to steal from a bank or other business?

The worst public security incidents aren't from hackers… yet

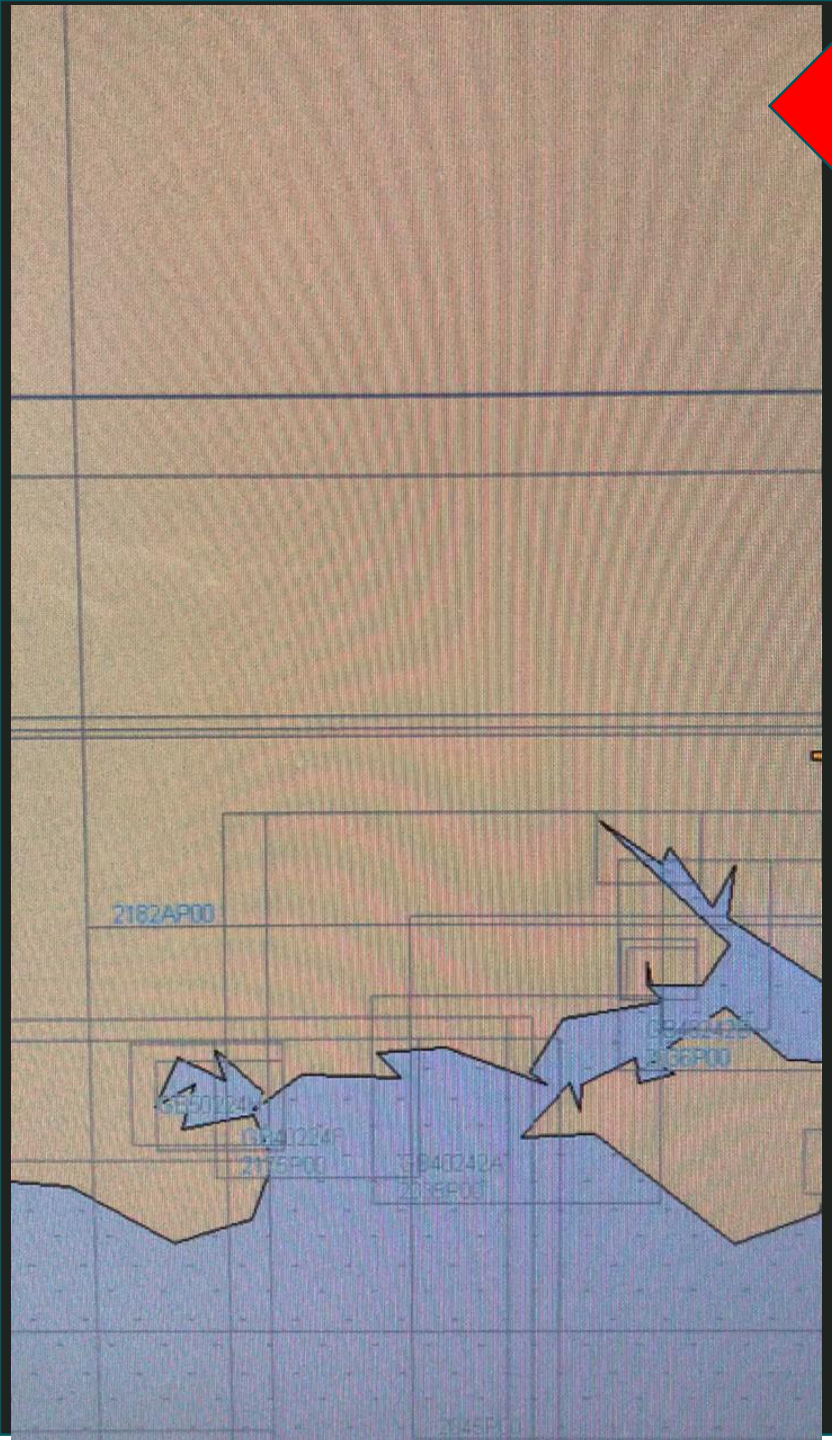
Maersk wasn't hacked

Collateral damage, kids & ransomware

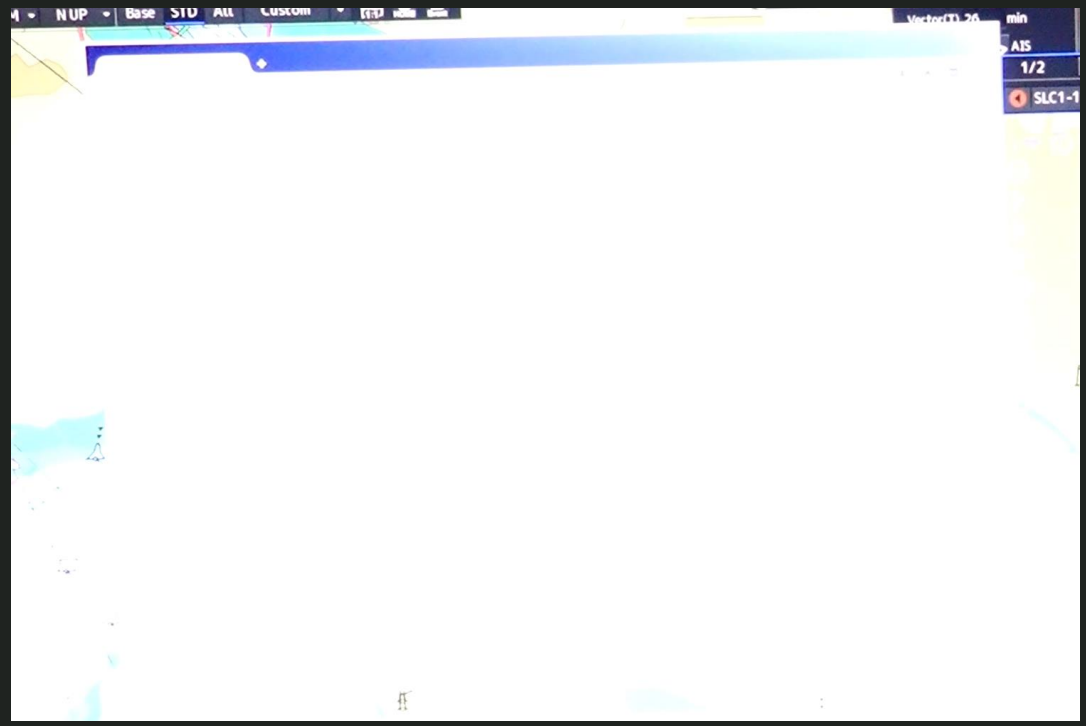
Crashing ships. Blocking the English Channel

ECDIS

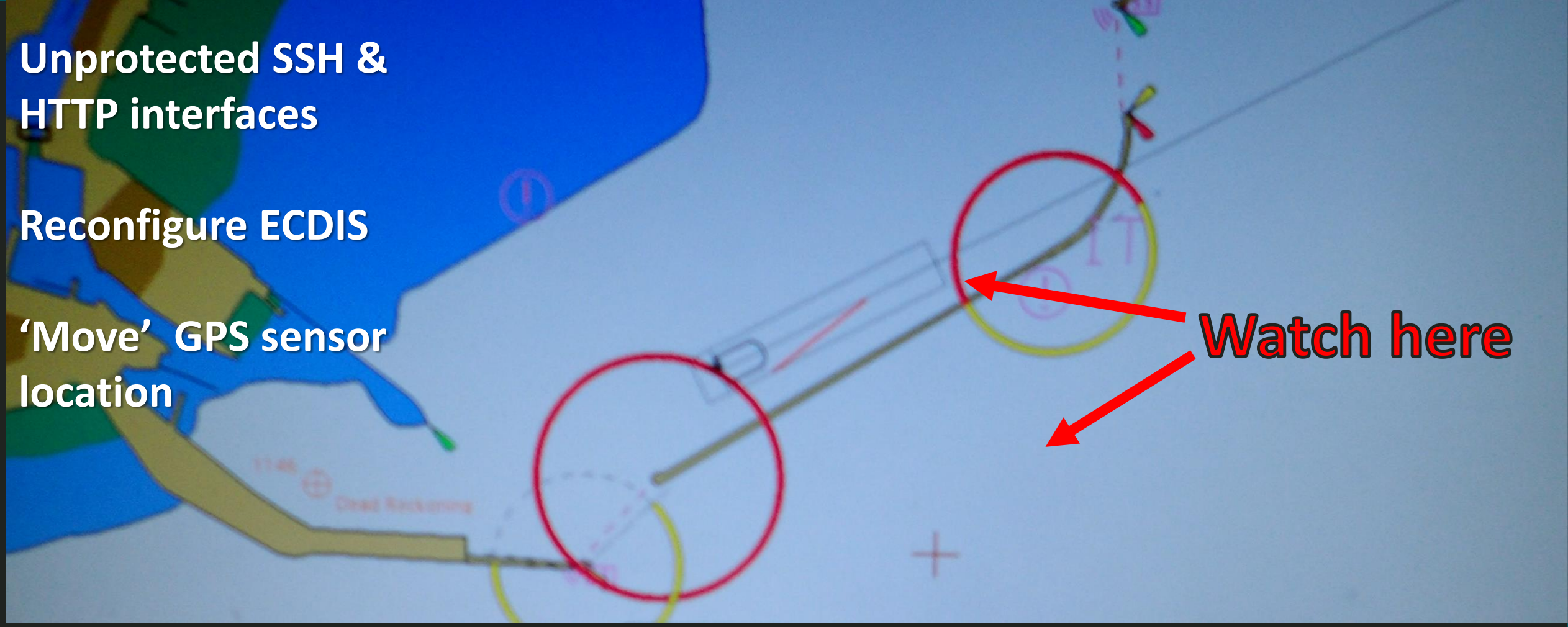
Found: remote code execution, Window NT & XP, dir traversal, offset injection…



A popular WECDIS, used by many navies:



A popular commercial ECDIS


Unprotected SSH &
HTTP interfaces
Reconfigure ECDIS
‘Move’ GPS sensor
location
Watch here

ECDIS can be used to populate AIS broadcast

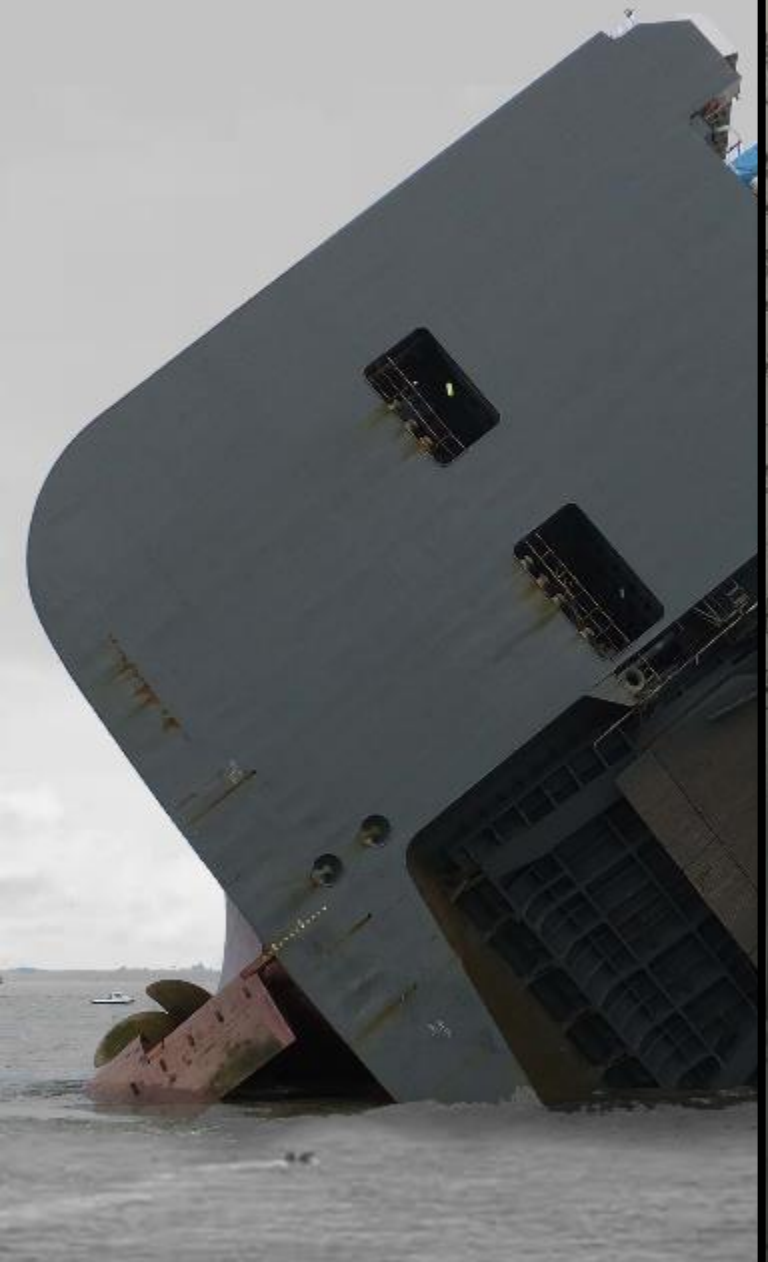
Or just hack the AIS transponder

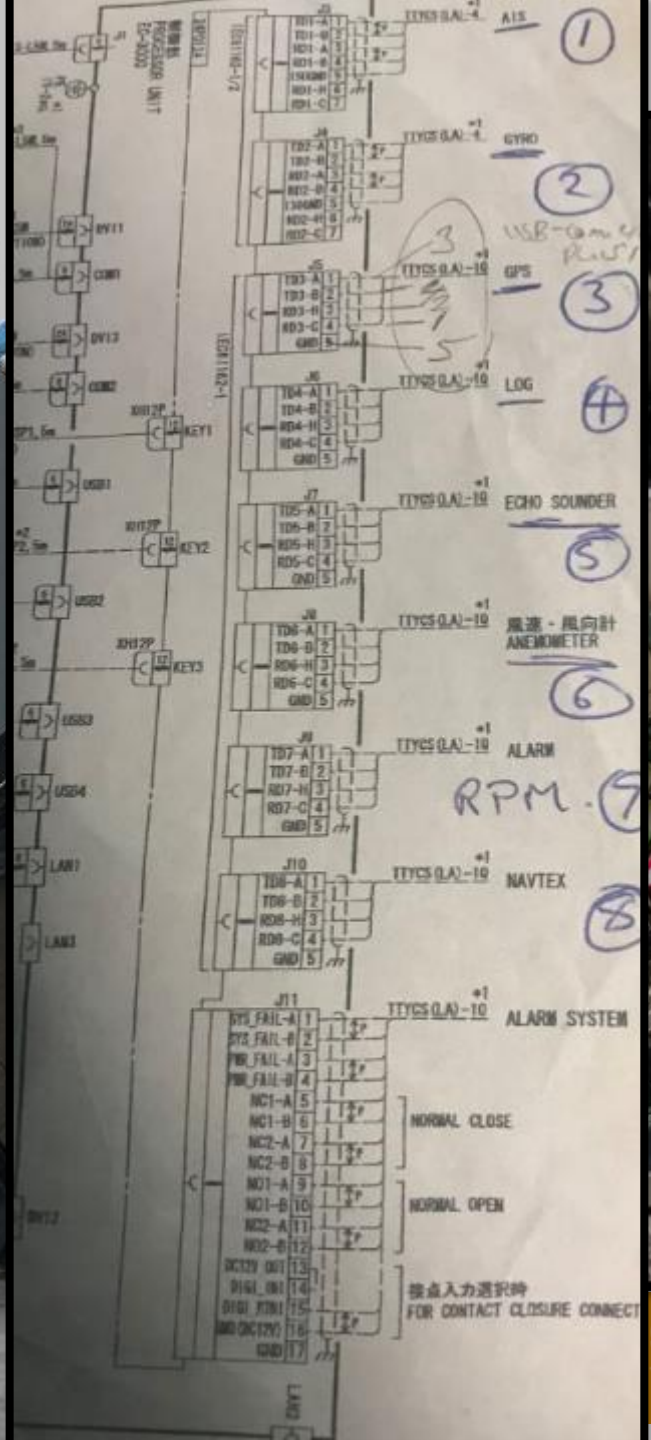
Reconfigure the ECDIS and ‘grow’ the ship to 1km square

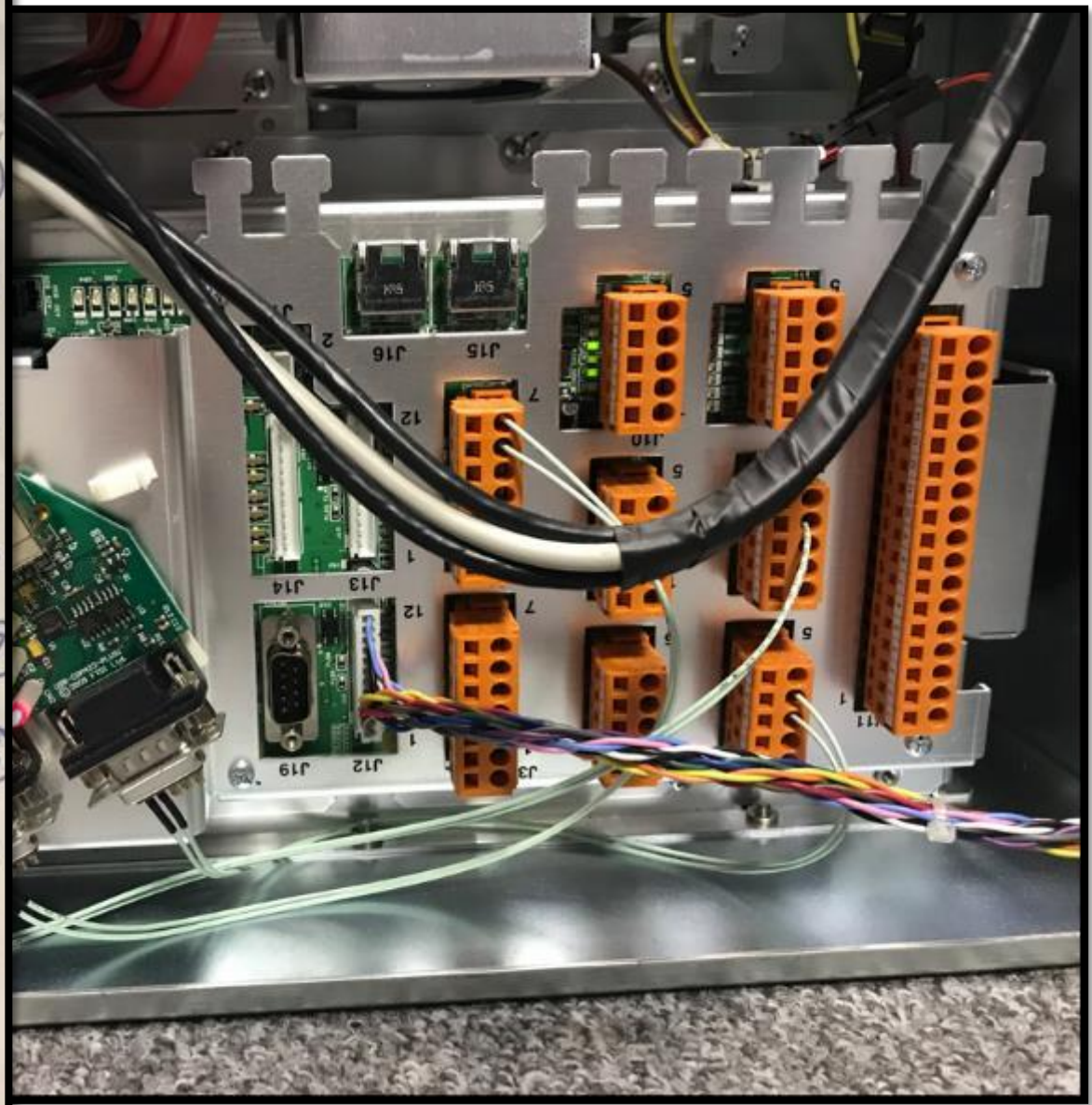
Now block the English Channel?


Crashing ships
Method 2

Serial hacking







@PenTestPartners

PenTestPartnersLLP

Intercept and modify GPS data on the ship network

‘Man in the Middle’ attack: undetectable, unlike GPS jamming or spoofing

Ethernet

Serial

ECDIS/synth radar

Serial

Ethernet

Hijacking the autopilot:

$GPAPA,A,A,0.10,R,N,V,V,011,M,DEST,011,M*82

Steering command for autopilot in ‘track control’ mode

Change R for L, amend 2 byte XOR checksum and rudder goes the wrong way!

Manual control…. Right…

```
UNB+UNOC:3+SENDER ID:ZZZ:
SENDER INT ID+RECEIVER ID:ZZZ:
RECEIVER INT ID+20151128:1037+1++++1++1'
UNH+1+ORDERS:D:01B:UN'
BGM+220+PO357893+9'

DTM+2:200808131430:102'
DTM+2:20151128:203'
FTX+DEL+1++INCLUDE TIME IN DELIVERY DATE'
RFF+AAN:APPTNO123445'
NAD+AA+Buyer_Id_12345::1'
LOC+1+Buyer Place Warehouse 678::1'
CTA+PD+BuyerEmployee1234:John Smith'
COM+Buyer_email@BuyerCompABC.com:EM'

NAD+AA+ShipTo_Id_87654::1'
LOC+1+ShipTo_Id_87654::1'
CTA+PD+BuyerEmployee1234:John Smith'
COM+ShipTo_Id_87654:EM'

LIN+1+1+1'
PIA+5+ENT-93474:BH'
IMD+F++:::Product Description'
MEA+AAA++EA:1'
QTY+21:3:A1B'
PRI+INV:3455.58'

UNS+S'
MOA+1:4406.57'
CNT+2:2'
UNT+30+1'
UNZ+1+1'
```

Manipulating load messages

MEA+AAE+VGM+KGM:9580.7

HAN+PRI:HANDLING:306′

HAN+LTT:HANDLING:306′

An EDIFACT cookbook for reefers

A recipe for prawn espresso:

HAN+**ACC**:HANDLING:306′

HAN+**NOR**:HANDLING:306′

HAN+**OSC**:HANDLING:306′

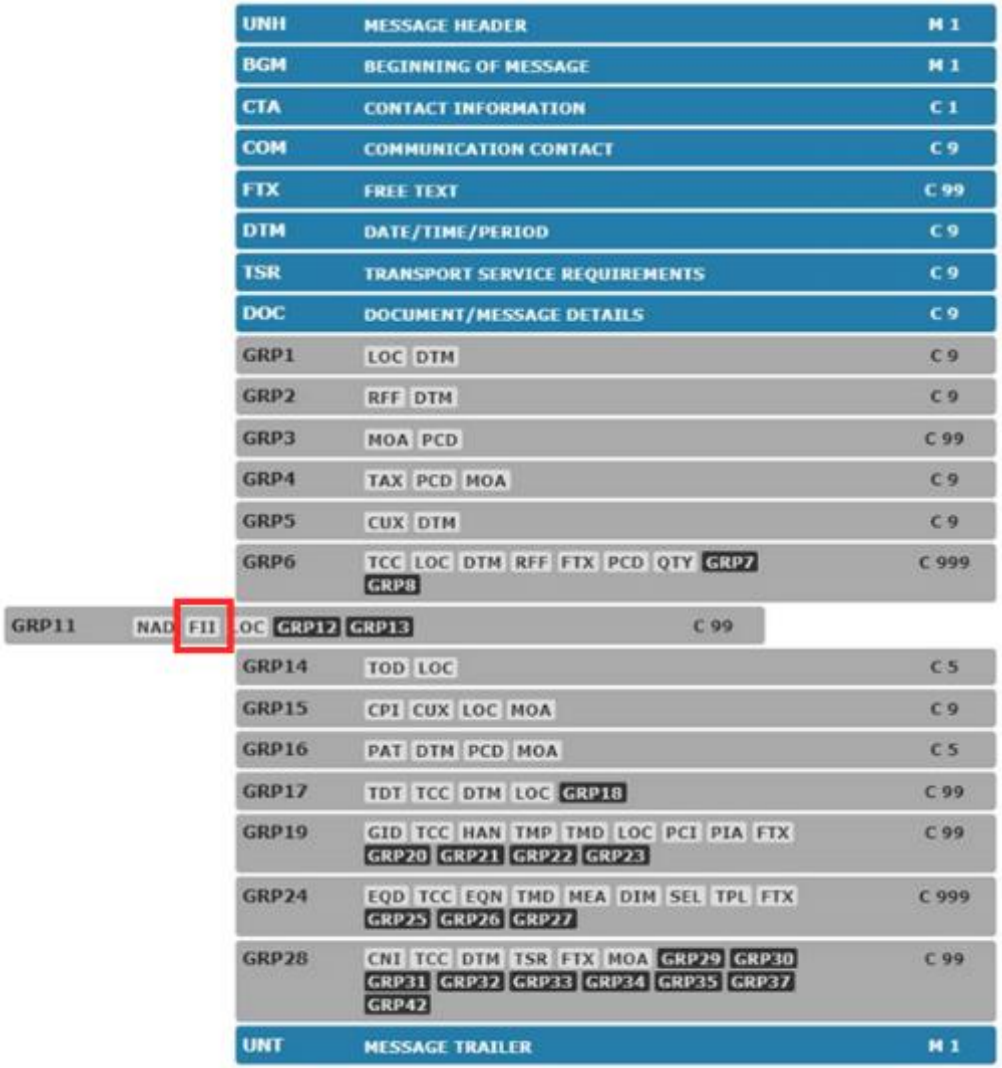
HAN+**OPD**:HANDLING:306′

HAN+**ODO**:HANDLING:306′

HAN+**KDR**:HANDLING:306′

Similar techniques could be used to disguise illegal shipments of arms & narcotics, or stealing containers

Stealing money using EDIFACT



UNH	MESSAGE HEADER	M 1
BGM	BEGINNING OF MESSAGE	M 1
CTA	CONTACT INFORMATION	C 1
COM	COMMUNICATION CONTACT	C 9
FTX	FREE TEXT	C 99
DTM	DATE/TIME/PERIOD	C 9
TSR	TRANSPORT SERVICE REQUIREMENTS	C 9
DOC	DOCUMENT/MESSAGE DETAILS	C 9
GRP1	LOC DTM	C 9
GRP2	RFF DTM	C 9
GRP3	MOA PCD	C 99
GRP4	TAX PCD MOA	C 9
GRP5	CUX DTM	C 9
GRP6	TCC LOC DTM RFF FTX PCD QTY GRP7 GRP8	C 999
GRP11	NAD FII LOC GRP12 GRP13	C 99
GRP14	TOD LOC	C 5
GRP15	CPI CUX LOC MOA	C 9
GRP16	PAT DTM PCD MOA	C 5
GRP17	TDT TCC DTM LOC GRP18	C 99
GRP19	GID TCC HAN TMP TMD LOC PCI PIA FTX GRP20 GRP21 GRP22 GRP23	C 99
GRP24	EQD TCC EQN TMD MEA DIM SEL TPL FTX GRP25 GRP26 GRP27	C 999
GRP28	CNI TCC DTM TSR FTX MOA GRP29 GRP30 GRP31 GRP32 GRP33 GRP34 GRP35 GRP37 GRP42	C 99
UNT	MESSAGE TRAILER	M 1

IFTFCC also contains interesting information for the hacker

Segment 0470:

FII: Financial Institution Information

‘Bank and account numbers’

This should be cross checked with the Bill of Lading before payment, but are you certain this is done?

Stealing containers?

LOC PLACE/LOCATION IDENTIFICATION

Function: To identify a place or a location and/or related locations.

010	3227	LOCATION FUNCTION CODE QUALIFIER	M	1	an..3
020	C517	LOCATION IDENTIFICATION	C	1	
	3225	Location name code	C		an..25
	1131	Code list identification code	C		an..3
	3055	Code list responsible agency code	C		an..3
	3224	Location name	C		an..256

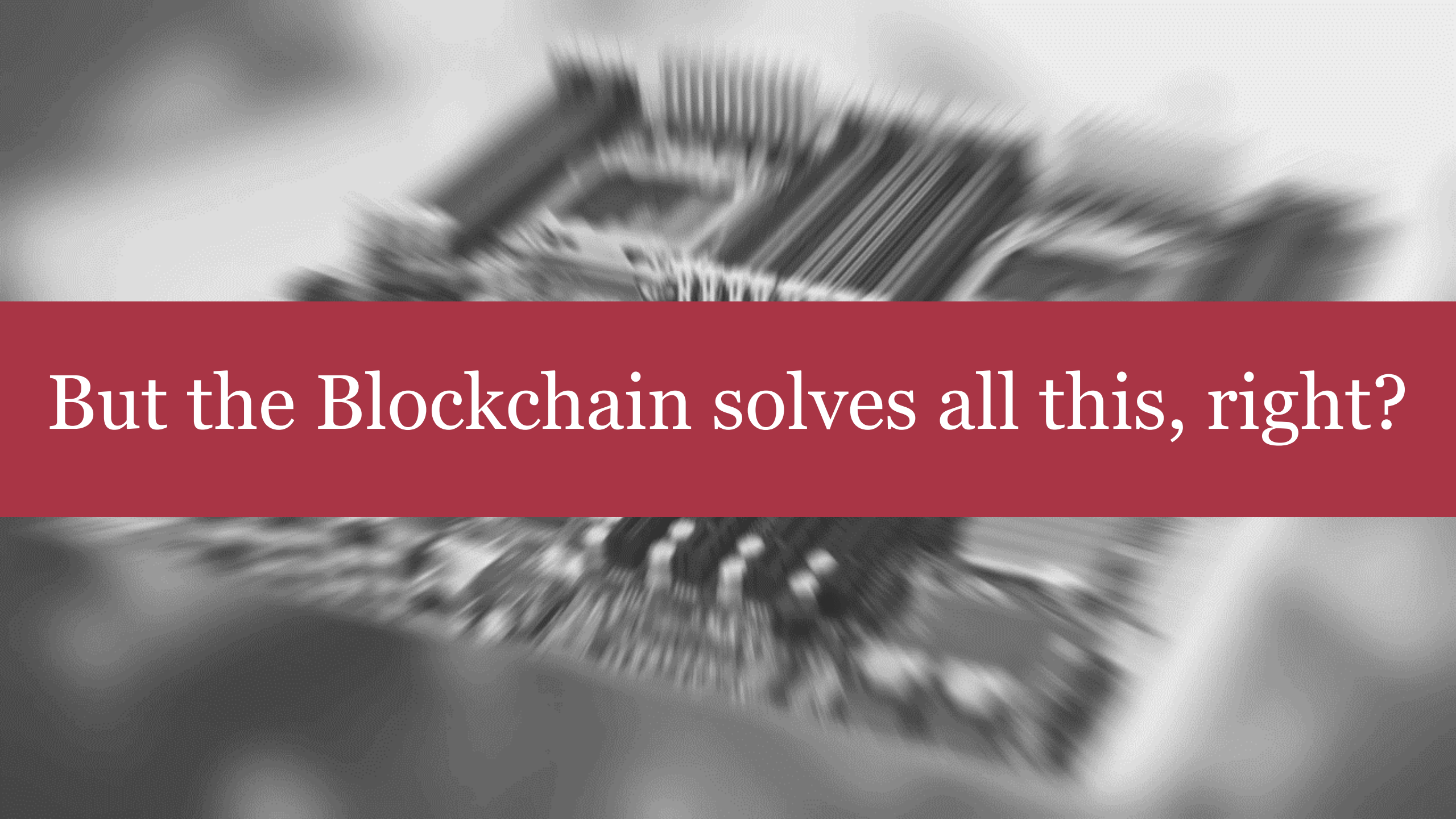
0270 LOC, Place/location identification
A segment to identify a location or country related to the equipment, such as:
- stowage cell
- (final) place/port of discharge
- transhipment place
- place of delivery
- country of origin/destination

Read the legal case involving Glencore and MSC from 2017: ~$1M of Cobalt stolen; two containers disappeared from a terminal

Case revolved around PIN codes given to truck driver. An inside job?

What if you could misroute containers by manipulating EDIFACT? LOC messaging is one way

Manipulate LOC segments of MOVINS, COPARN, COARRI, CODECO messages etc


But the Blockchain solves all this, right?

Blockchain is the solution?

Maybe…

…or maybe it just creates new security problems to solve

Private Key = Wallet

…protected by a password

Miner issues:

51% problem

Ledger disc storage problem

Bandwidth problem on ship

Numerous crypto algorithms have been broken over the years: RC4, MD5, SHA-1

What happens if processing power in future allows Blockchain collisions to be found?

Other insecure maritime communication protocols

AIS

Navtex

Echo sounder

Log data

BNWAS

Synthetic radar

GPS

DP

Tactical Advice

Tactical advice

REALLY BASIC PROBLEMS WITH SATCOMS

Check that satellite comms box isn’t on the PUBLIC internet

Check that the admin passwords are STRONG

Satcom terminal software updates

Check that Wi-Fi networks on board are segregated

Tactical advice

Check your on board networks are segregated:

Bridge, engine room, crew, Wi-Fi and business networks must be logically isolated

Secure USB ports on ship systems. If you have to update charts etc over USB, keep dedicated USB keys for this purpose only

Demand evidence from your maritime technology suppliers that their equipment is secure

And teach your crew about security

@thekenmunroshow

@pentestpartners

LinkedIn: Pen Test Partners

Blog: www.pentestpartners.com – full of useful advice for maritime systems security hardening

Start with a simple security audit of your vessel / terminal / systems from security experts who understand shipping

info@pentestpartners.com
+44 (0)20 3095 0500
@PenTestPartners
PenTestPartnersLLP