



Hacking, tracking, stealing & sinking ships

Who am I?

An ethical hacker / security researcher

Team of 60 who test ship security @pentestpartners

Several ex-ships crew on the team

Help improve cyber security for vehicles, ATMs, banks, government, military

 info@pentestpartners.com

 +44 (0)20 3095 0500

 @PenTestPartners

 PenTestPartnersLLP

The background of the slide is a blurred, high-contrast black and white photograph of electronic components, likely a circuit board or a dense array of sensors, creating a sense of motion and technological complexity.

IoT

The background of the slide is a grayscale, motion-blurred image of electronic components, likely a printed circuit board (PCB) with various chips and connectors. The blur creates a sense of dynamic movement and technological advancement.

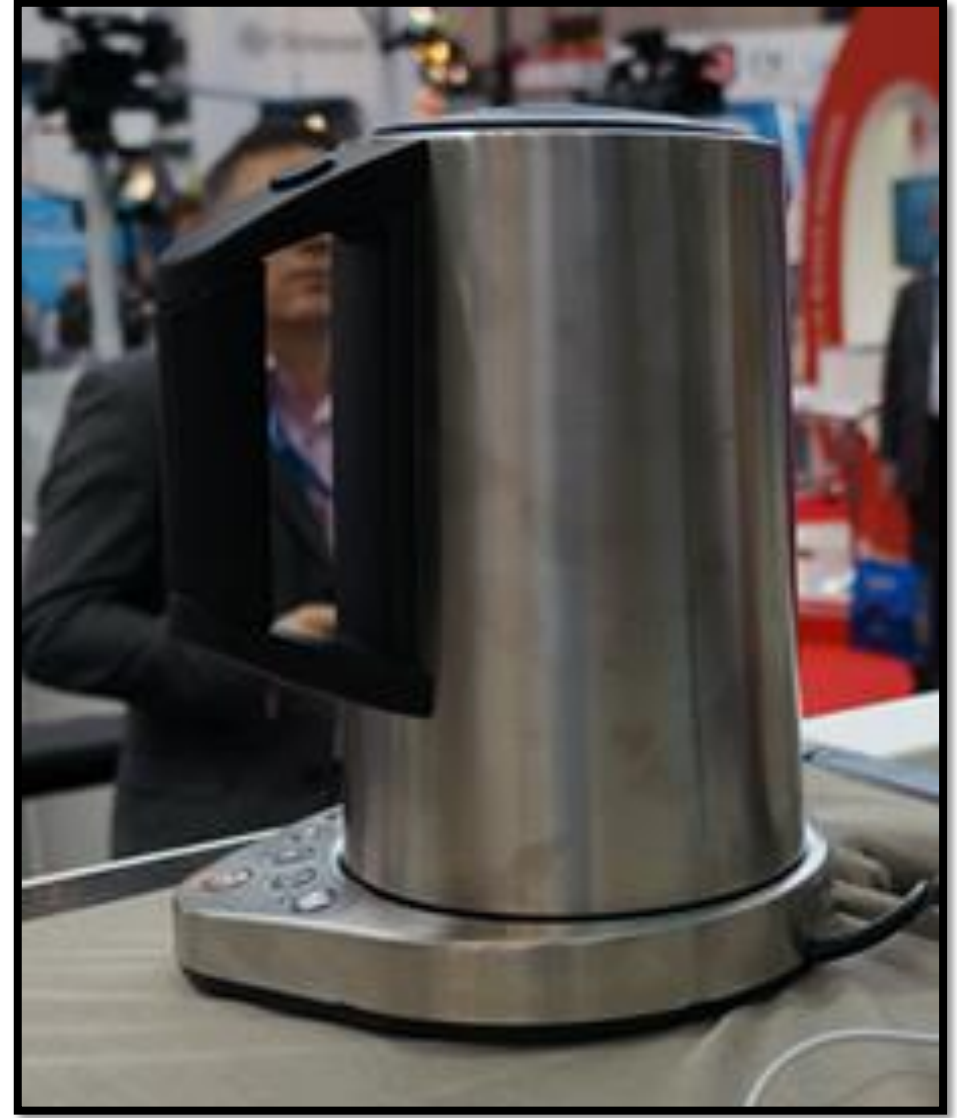
Internet of Tea

A Wi-Fi tea kettle

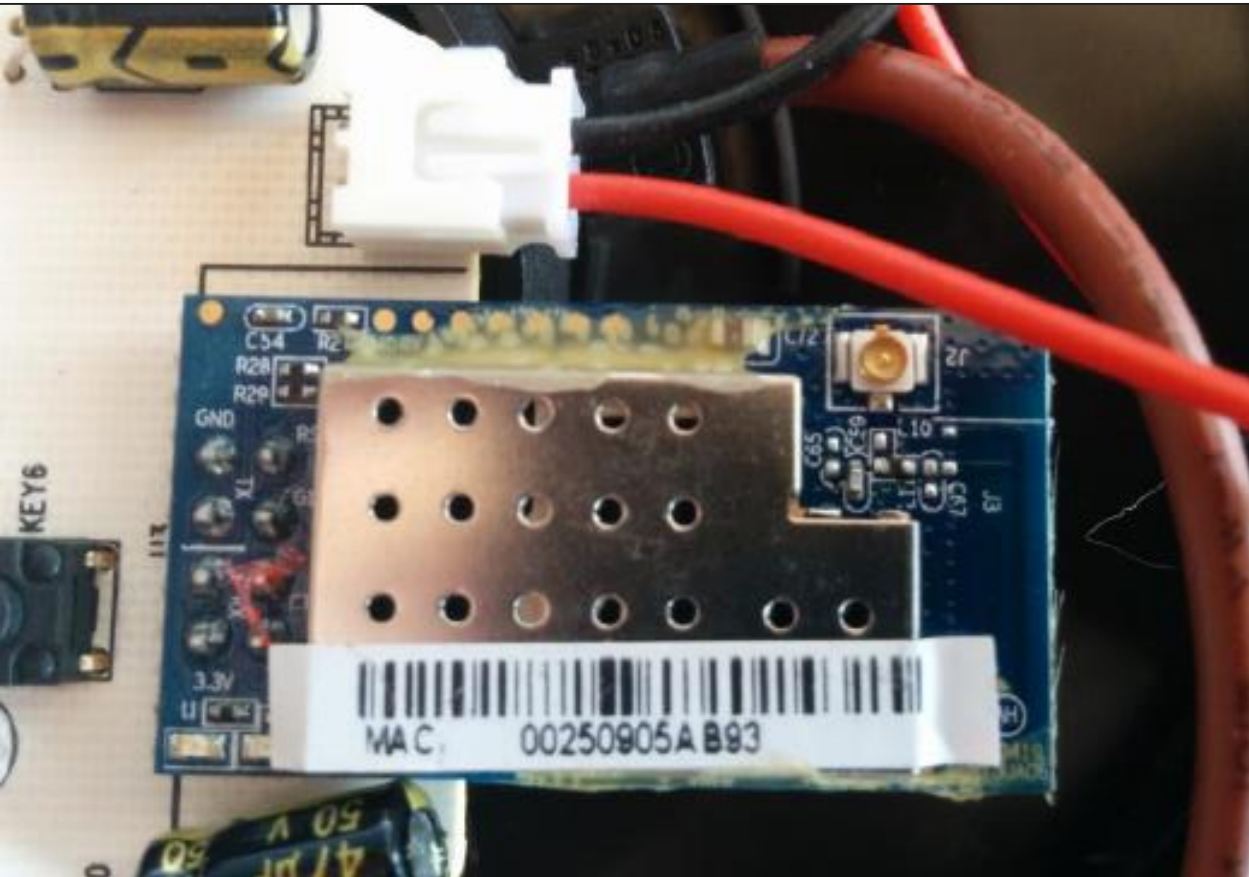
A Wi-Fi enabled kettle, essential for every British home

Comes with mobile app, from which kettle can be boiled

Offers stunning time saving, at a \$100 premium over a regular non-smart kettle



How to hack a kettle



#1 take it apart

#2 locate chipset manuals

#4 review mobile app source code

#5 find security flaws

#6 make tea!

UART WIFI TRANSPARENT MODULE



Copy Right Reserved By Elechouse

www.elechouse.com



4.3.7 System parameters

4.3.7.1 System password

Table 4-34 System password

Parameter name	Parameter	Correlative Command
System password	Login Password	AT+PASS
Description		
The login password for accessing the module through WEB server or wireless configuration.		
The default setting of system is "000000".		

4.3.7.2 WEB server

6.2.4.6 AT+KEY

Function:

Set or query network key. What should be noted is that, before using this command to set network key, user must set the encryption mode with the command AT+ENCRY.

Format:

AT+KEY=[!?][format],[index],[key]<CR>

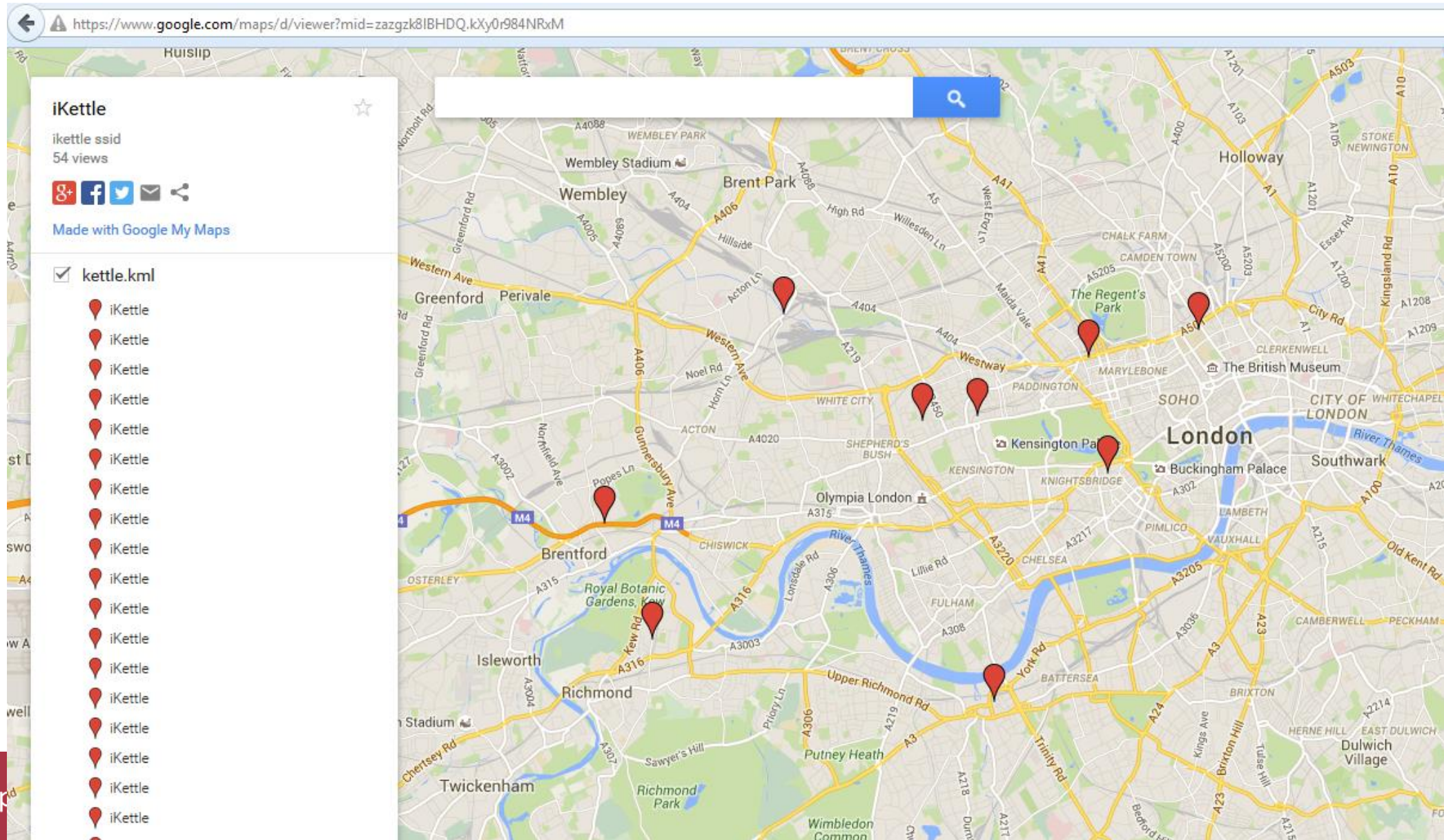
+OK[=format,index,key]<CR><LF><CR><LF>

Disclosure

“It’s OK” said the manufacturer

...the hack requires specialist knowledge and one would have to be very lucky to find a user with a wifi kettle

Wi-Fi is trackable. Find kettles to steal Wi-Fi security key from:



So what?

Do you have any control over the smart devices your crews bring on board?

How secure are the wireless networks on board your vessels?

Have you checked the separation of your on-board networks?



Another way: satcoms

Let's go find some ships that could be hacked

Many ships are now permanently connected to the internet

www.shodan.io is a search engine that can be used to find always-on devices e.g.:

‘sailor 900’

‘Inmarsat Solutions’

‘Telenor Satellite’

‘commbbox’

The screenshot shows the Shodan search engine interface. The search bar contains the query "html:sailor 900". The results are displayed in a grid format. On the left, there are summary statistics: "TOTAL RESULTS: 51", "TOP COUNTRIES" (United States: 33, Norway: 7, Singapore: 4, United Kingdom: 3, Albania: 2), "TOP SERVICES" (HTTP: 27, HTTPS: 17, Qconn: 4, HTTP (8080): 3), and "TOP ORGANIZATIONS" (IsoTropic Networks: 28, Telenor Satellite AS: 7, Intelsat Global Services Corporation: 4, Satellite Mediaport Services Ltd.: 3, Level 3 Communications: 3). The main results area shows three entries for "SAILOR 900 VSAT Ku". Each entry includes the IP address, organization name, location, technologies, and a detailed view of the SSL certificate and supported SSL versions. The first entry is for IP 100.42.7.14, issued by Cobham SATCOM, with an expiration date of Thu, 15 Feb 2018 05:15:32 GMT. The second entry is for IP 62.145.79.96, issued by Cobham SATCOM, with an expiration date of Thu, 15 Feb 2018 00:01:46 GMT. The third entry is for IP 83.137.63.162, issued by Cobham SATCOM, with an expiration date of Wed, 14 Feb 2018 21:15:20 GMT.

Another example satcom issue. KVH are not at fault here

Comms not provided by KVH - vessel owner took a 3rd party service

Vessel owner didn't update the software

The screenshot shows the KVH Industries CommBox web interface. The main page has a blue header with the KVH logo and the text "KVH INDUSTRIES" and "CommBox - Connecting ship and office networks". Below the header is a login form with the text "Welcome to CommBox™ - Powered by KVH Industries Norway AS". The login form asks for "User Name" and "Password" and has a "Login" button. Below the login form, there is a red box containing the text "Active Crew Internet Users 2 / 20" and a link "Show Users". At the bottom of the page, there is a footer with the text "© KVH Industries Norway AS - Version: 1.12.5 - System name: Dawn Horizon" and "KVH Industries Norway AS recommends web browsers Firefox and Opera for safer web browsing.".

Overlaid on the main page is a window titled "[#] QuickCrew - Show Active Users - Google Chrom...". This window displays a table with the following data:

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

It's so easy!

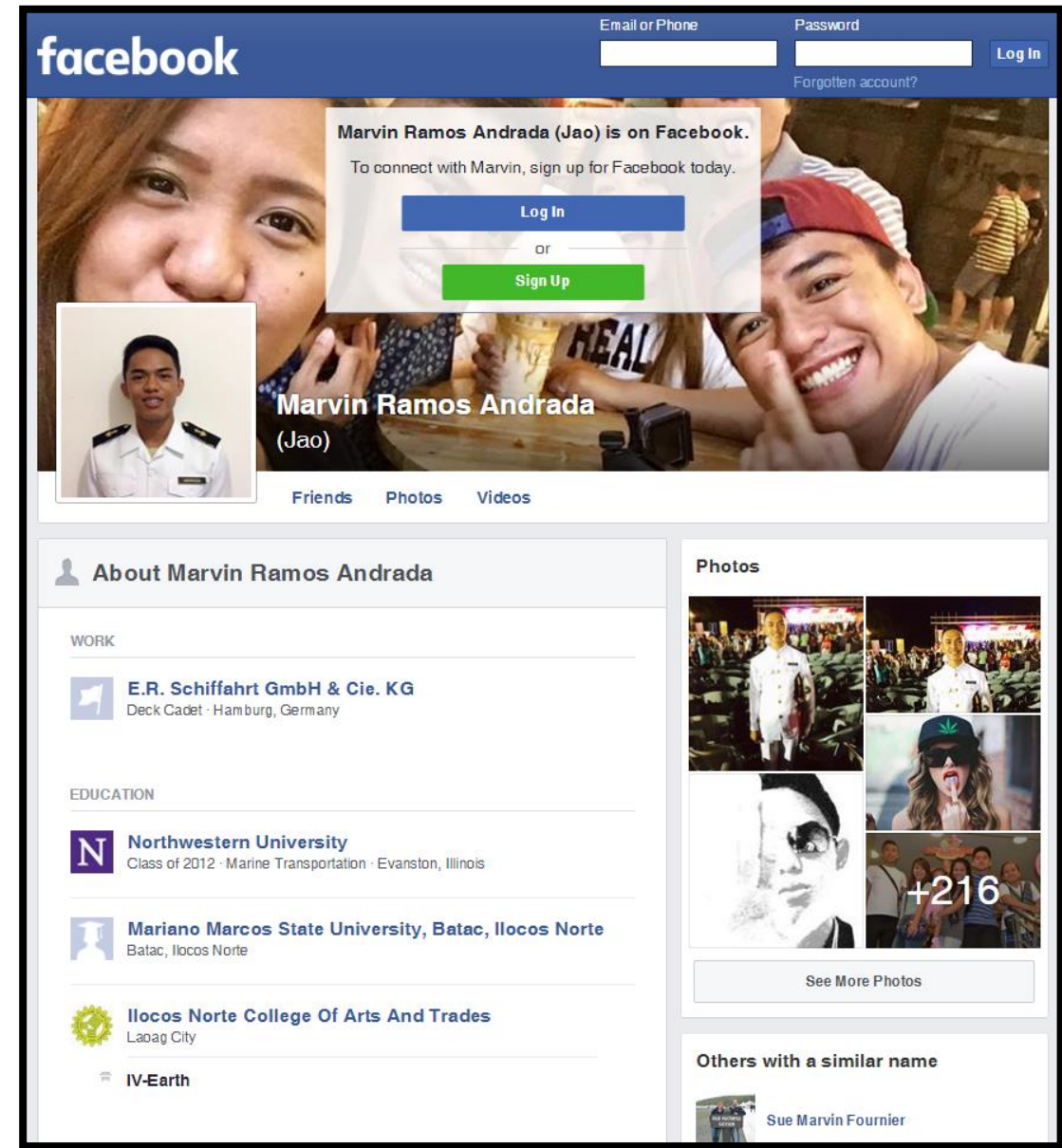
We know the vessel name, line and location from AIS

We know the names of the crew from the satcom box

We know their interests from Facebook

TIME FOR A PHISHING ATTACK!

With a phish, one can compromise the vessel network



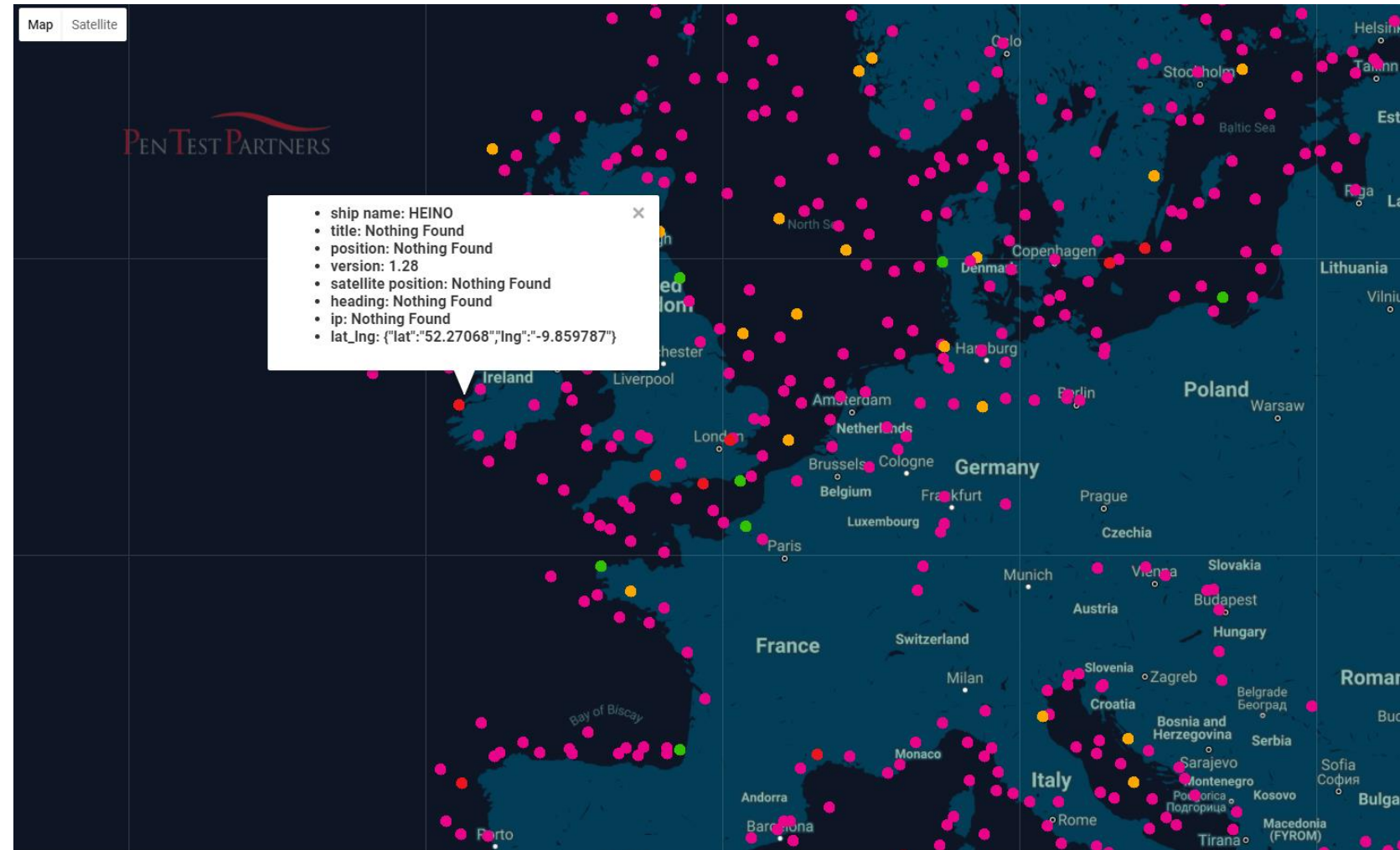
Let's go one better: a real time vulnerable ship satcom tracker

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



Software updates fix security problems

Satcom vendors rarely say:

‘we made a mistake, there’s a security problem in our vessel satellite terminal.

Here’s a really important software update that you need to apply urgently to prevent your vessel being hacked’

We more often see security bugs hidden in generic changelogs, e.g.:

“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.”

Nasty security flaw!

What if we could tell you immediately if an update is published for your satcom software?

How valuable would that be!

If you saw that, you would take immediate action!


Next research project

The hardware inside a satcom terminal

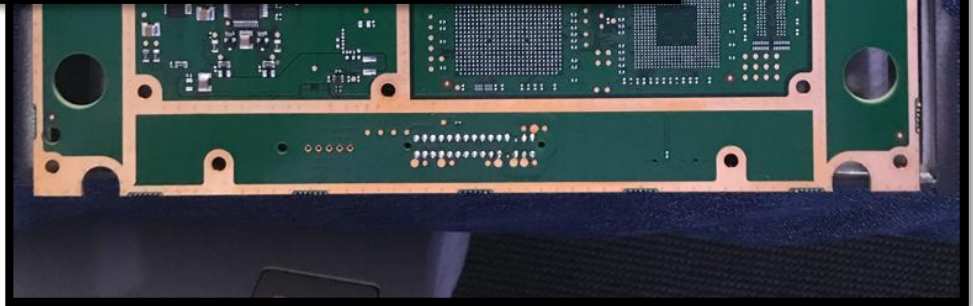
What sec
the firmw

Could a h
to the
vulnerable

What if
firmware yourself to increase
bandwidth ;-)



```
74 | SpaceCom Protect |
73 | ion!Chuck Norris |
00 | Kills U,..... |
78 | ^H@y. (...pG... \HAX |
```





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



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'

EDIFACT

Interfering with shipping



Potential to modify BAPLIE during transfer to or on board ship & affect metacentric height

Probably easier to modify data that it is constructed from: EDIFACT

Containerised transport is vulnerable to loading message interception and modification

Switching EDI message codes can cause misloading and out-of-trim situations

MEA+AAE+VGM+KGM:9580.7

HAN+PRI:HANDLING:306'

HAN+LTT:HANDLING:306'

Causing explosions through EDIFACT manipulation?

Further manipulation of dangerous goods codes can lead to explosions:

ATT+26+AGR:DGATT:306+**XS**:DGAGR:306 '

ATT+26+HAZ:DGATT:306+**FLVAP**:DGHAZ:306'

DGS+IMD+2.1::35-10+1954+055:**CEL**+1+F-ES-E



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 or narcotics

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?

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

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
- transshipment place
- place of delivery
- country of origin/destination

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



Hacking OT through RS232/485

Serial hacking



OT systems are controlled using serial protocols, typically RS232 or 485.

Think ballast/trim control, propulsion, steering, thrusters etc

Routing of traffic is often over ethernet networks

Numerous devices offer I/O for serial and ethernet, creating 'bridges' that the hacker can exploit

Serial-IP converters have had serious security flaws

OT hacking



HSMS in bulk carriers & tankers

Hull Stress Monitoring Systems are present to prevent misloading

They typically report to a rugged PC on the bridge

Connected to the voyage data recorder through a serial or IP network

Tamper with the data in real time, overstress the ship

OT hacking

Similar loading issues can occur with LNG carriers

Also concerns around cooling, management of tank pressure and fuel slosh / cofferdams

Heavy reliance on ballast pumps for trim. Communicate IP->CAN->RS485





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?



Hacking the VDR, BNWAS & GPS

VDR, BNWAS & GPS hacking

Voyage Data Recorder takes data from GPS, rudder, bridge audio etc etc, stored on a rugged Remote Storage Module

Bought a used RSM from eBay & went down a rabbit hole

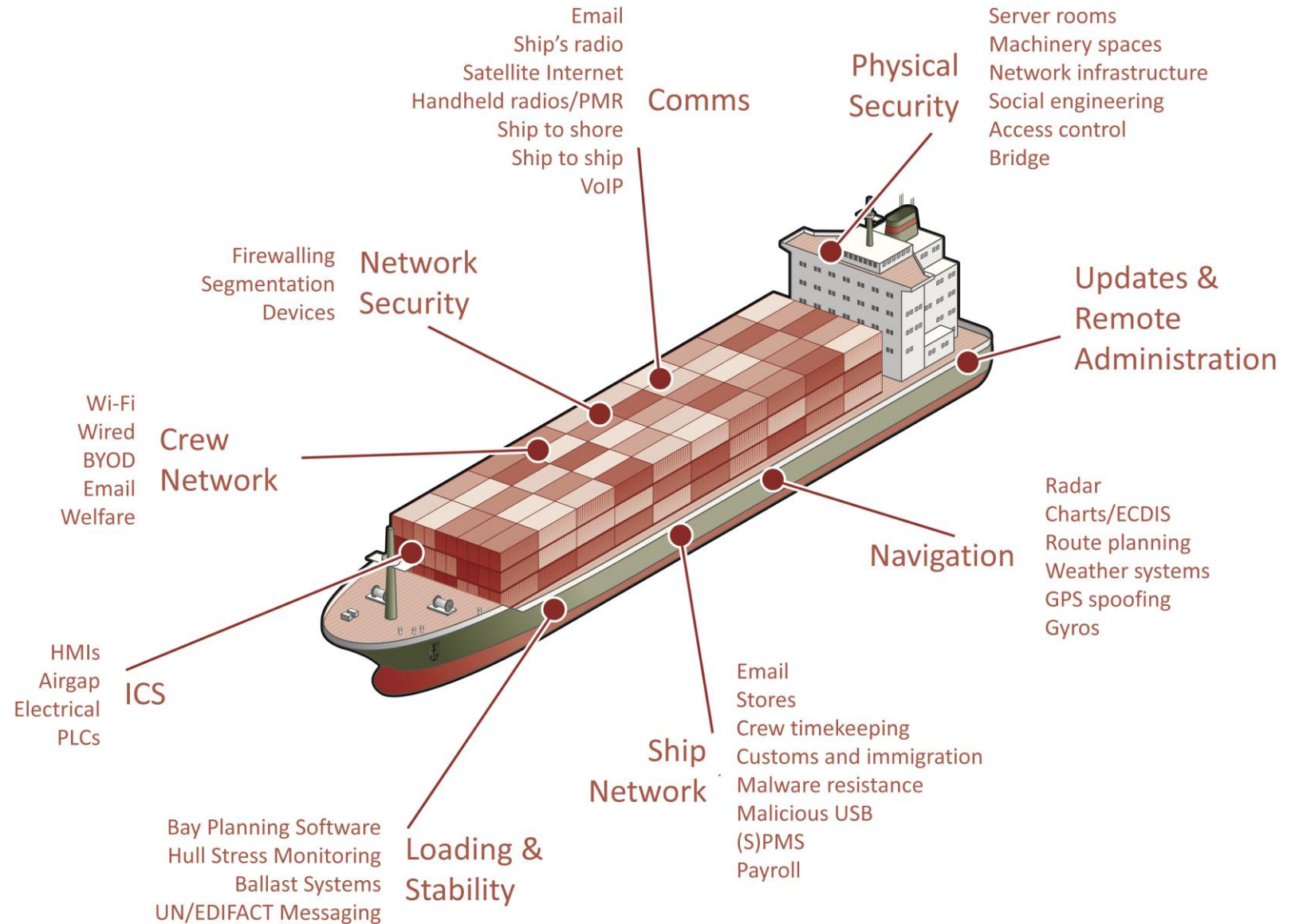
Data is based on NMEA 0183 messaging: unauthenticated serial messages. Crash ships?

```
ÝþR15$HEHDT,62.8,T*13
ÝþR11!AIVDV,46,16,0,A,1234567890XX1234567890XXX1234567890,82,232100.06,08,12,2013*4A
ÝþR12$GPZDA,232100.01,08,12,2013,0,0*6E
ÝþR11!AIVDV,47,16,0,A,1234567890XX1234567890XXX1234567890,83,232100.06,08,12,2013*4A
ÝþR16$BNALR,,000,A,V,C1=OFF;C2=12;C3=00*5A
ÝþR11!AIVDV,48,16,0,A,1234567890XX1234567890XXX1234567890,86,232100.10,08,12,2013*47
îþR14$GPGLL,1522.5150,N,2806.4014,E,232100.01,A,A*52
```

Hijacking the autopilot?

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

Where the heck do you start?





Tactical Advice

Tactical advice

Start with your **remote data comms**

Check that your satellite comms box isn't on the PUBLIC internet

Check that the admin passwords have been changed from the vendor default and are now **STRONG**

Check that your fleet has the latest version of satcom software and is updated each time an update is published

Check that Wi-Fi networks on board have strong passwords and config and are isolated from other systems

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: Ken Munro + cyber

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

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