Hacked at sea: Researchers find ships' data recorders vulnerable to attack

Voice, data records on ship "blackboxes" easily destroyed or altered by attackers—or crew.

by **Sean Gallagher** - Dec 11, 2015 1:45am CST

Share Tweet 14

A voyage data recorder recovery capsule aboard a container ship. Some VDRs may be an easy target for hackers--or crew members who don't want what they've done to be recorded.

Hervé Cozanet

When the freighter *El Faro* was lost in a hurricane on October 1, one of the goals of the salvage operation was to recover its voyage data recorder (VDR)—the maritime equivalent of the "black box" carried aboard airliners. The VDR, required aboard all large commercial ships (and any passenger ships over 150 gross tons), collects a wealth of data about the ship's systems as well as audio from the bridge of the ship, radio communications, radar, and navigation data. Writing its data to storage within a protective capsule with an acoustic beacon, the VDR is an essential part of investigating any incident at sea, acting as an automated version of a ship's logbook.

Sometimes, that data can be awfully inconvenient. While the data in the VDR is the property of the ship owner, it can be taken by an investigator in the event of an accident or other incident—and that may not always be in the ship owner's (or crew's) interest. The VDRs aboard the cruise ship *Costa Concordia* were used as evidence in the manslaughter trial of the ship's captain and other crewmembers. Likewise, that data could be valuable to others—especially if it can be tapped into live.

It turns out that some VDRs may not be very good witnesses. As a report recently published by the security firm IOActive points out, VDRs can be hacked, and their data can be stolen or destroyed.

The US Coast Guard is developing policies to help defend against "transportation security incidents" caused by cyber-attacks against shipping, including issuing guidance to vessel operators on how to secure their systems and reviewing the design of required marine systems—including VDRs. That's promising to be a tall order, especially taking the breadth of systems installed on the over 80,000 cargo and passenger vessels in the world. And given the types of criminal activity recently highlighted by the *New York Times*' "Outlaw Ocean" reports, there's plenty of reason for some ship operators to not want VDRs to be secure—including covering up environmental issues, incidents at sea with other vessels, and sometimes even murder.

LATEST FEATURE STORY

FEATURE STORY (3 PAGES)

The *Kick Off 2* World Cup: Competitive e-sports with a 25-year-old Amiga game

Since 2001, players have been gathering annually to play the (digital) beautiful game.

WATCH ARS VIDEO

Ars tours the Sims Municipal Recycling facility in Brooklyn, NY

John Timmer learns about the state of recycling in NYC.

STAY IN THE KNOW WITH

LATEST NEWS

Couple takes pics of Star Wars figure they bought, gets DMCA notice from Lucasfilm

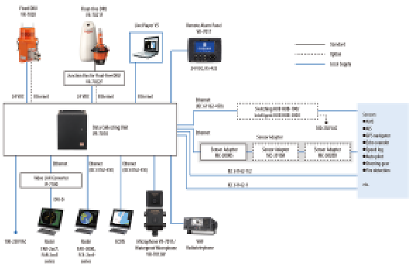
The Pixel C was probably never supposed to run Android

IOActive researchers looked specifically at the Furuno VR-3000, a VDR that was involved in a case in 2012 where data for a period during which Italian marines aboard a freighter fired upon an Indian fishing vessel "mysteriously" corrupted before investigators could access it. The marines, who were embarked aboard the freighter Enrica Lexie, claimed that they were in international waters and believed the fishermen to be pirates. The data that could have proven their location, along with communications data, was lost.

The VR-3000's Data Recording Unit is essentially a Linux-based personal computer with little in the way of security hardening. Other manufacturers use various industrial, real-time operating systems. But at least it's more secure than some of the other VDRs sold by Furuno. In another incident with a different, Windows XP-based VDR in 2012, data was corrupted when a crewmember on a Singapore-flagged ship inserted a USB drive into a port on the VDR—causing it to be infected with malware and

IOActive did a deep analysis on the VR-3000 and found a number of vulnerabilities, including:

- Weak encryption of voice data files using an embedded, shared password.
- Vulnerabilities in software services that allowed remote attackers to execute code on the data recording unit with root privileges, including the ability to "delete certain conversations from the bridge, delete radar images, or alter speed or position readings."
- The VDR could also be turned into a remote bug to spy on the crew of a ship through its attached microphones.



Enlarge / The network of devices connected to a voyage data recorder system.

Furuno

To execute remote attacks on the VDR, the attacker only needed access to the network. Since many VDR systems use Ethernet and sit on the same network as satellite communications systems (some of which are known to be vulnerable to attacks), there are a number of potential ways attackers could breach the security of the VDR while not being aboard. Terrorists, pirates, hostile state actors and others could pinpoint the location of ships of interest and then listen to the conversations of crewmembers as well as their radio calls.

IOActive revealed these vulnerabilities to the Department of Homeland Security's Industrial Control Systems Computer Emergency Response Team (ICS-CERT) and Japan's CERT Coordination Center (JPCERT/CC) over a year ago. Furuno was notified as well, but it promised only to patch the problem "sometime in 2015," according to the IOActive report. There's no word on whether the patches have been distributed to ship operators.

READER COMMENTS 14

Share 147 Tweet - Google 9 Reddit 11

Sean Gallagher / Sean is Ars Technica's IT Editor. A former Navy officer, systems administrator, and network systems integrator with 20 years of IT journalism experience, he lives and works in Baltimore, Maryland.

@thepacketrat on Twitter

← OLDER STORY NEWER STORY →

Defunct social network asks court to reverse Facebook's $3M award in spam case

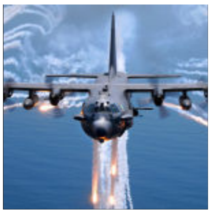
Senate committee talks Turing—"My biggest challenge is to not lose my temper"

SHA1 sunset will block millions from encrypted net,

YOU MAY ALSO LIKE

Ars talks with David Braben on the challenges of making games for real VR

Turkish F-16 shoots down Russian jet for disputed airspace violation



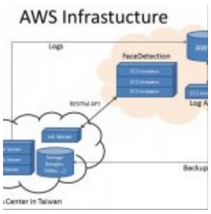
How tech fails led to Air Force strike on MSF’s Kunduz hospital

Laser strike said to give ferry pilot 3rd degree burns on his eyelid

Hands-on: Eve: Valkyrie is more than just a tech demo

Commercial space station resupply launch success—Cygnus blasts off

Getting a Linux box corralled into a DDoS botnet is easier than many think



Researchers poke hole in custom crypto protecting Amazon Web Services

SITE LINKS

About Us
Advertise with us
Contact Us
Reprints

SUBSCRIPTIONS

Subscribe to Ars

MORE READING

RSS Feeds
Newsletters

Visit Ars Technica UK

CONDE NAST SITES

Reddit
Wired
Vanity Fair
Style
Details

Visit our sister sites
Subscribe to a magazine

VIEW MOBILE SITE

CONDÉ NAST

Ad Choices