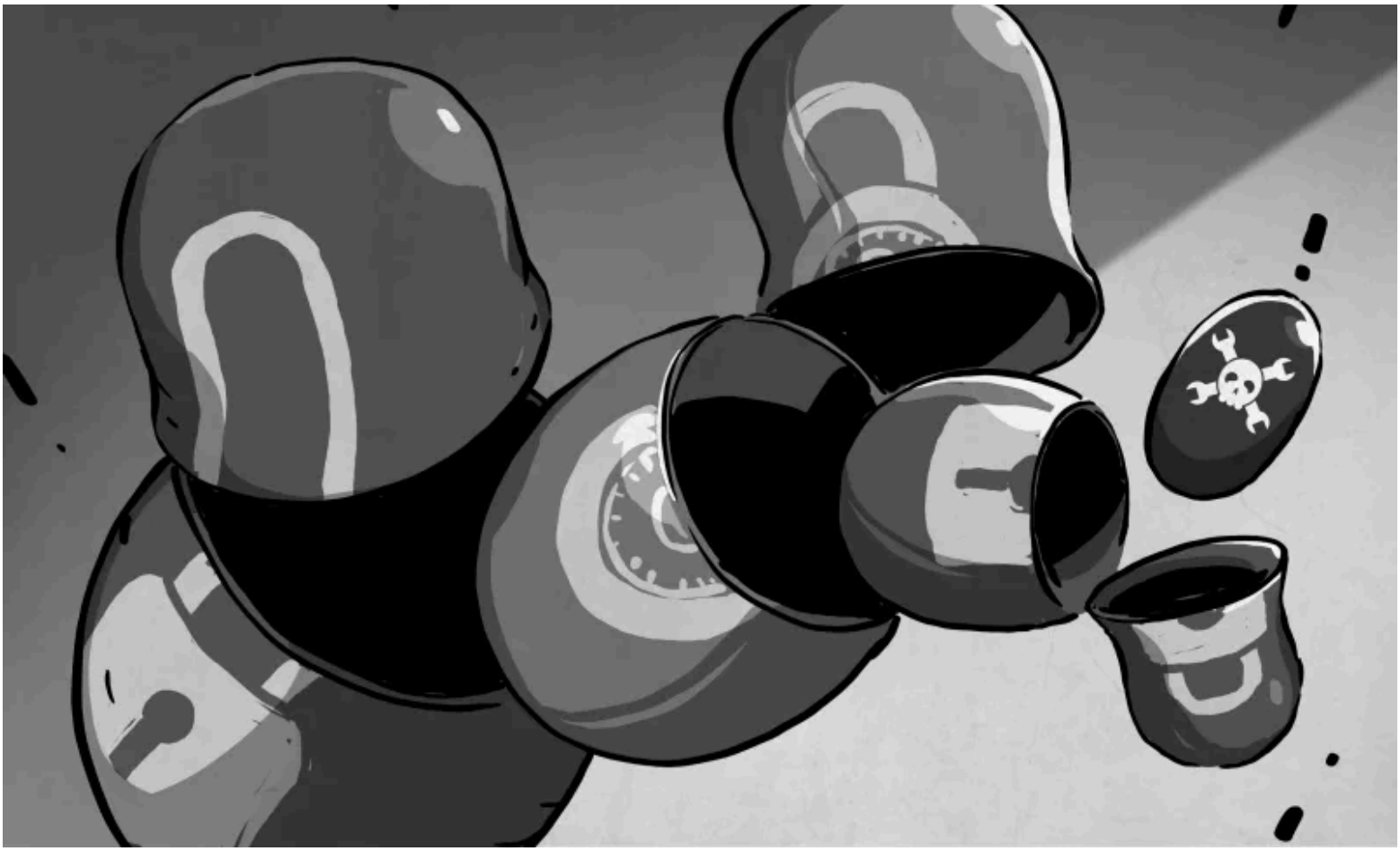
HACKADAY

SECURE COMMUNICATION, BURIED IN A NEWS APP

by: Lewin Day

25 Comments

March 9, 2026



Cryptography is a funny thing. Supposedly, if you do the right kind of maths to a message, you can send it off to somebody else, and as long as they're the only one that knows a secret little thing, nobody else will be able to read it. We have all sorts of apps for this, too, that are specifically built for privately messaging other people.

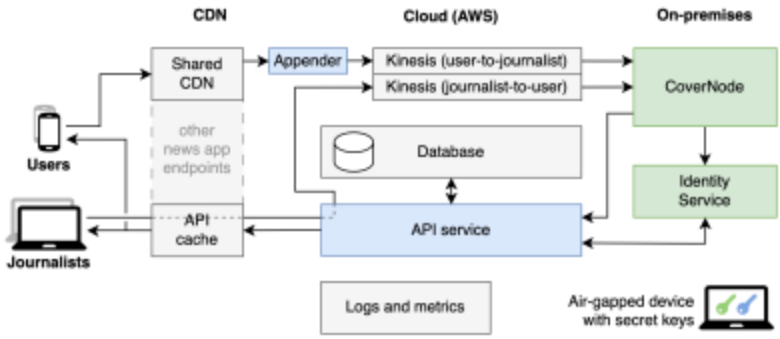
Only... sometimes just *having* such an app is enough to get you in trouble. Even just the garbled message itself could be proof against you, even if your adversary can't read it. Enter *The Guardian.* The UK-based media outlet has deployed a rather creative and secure

way of accepting private tips and information, one which seeks to provide heavy cover for those writing in with the hottest scoops.

HIDING IN PLAIN SIGHT

There are plenty of encrypted messaging apps out there, of greater or lesser value. Ultimately, though, they all have a similar flaw. If you have one of these ultra-secure apps on your phone, or malicious authorities capture you sending lots of messages to such a server, it can be somewhat obvious that you're doing something worth hiding. You might not be—you might just have a penchant for keeping your fantasy football submissions under wraps. Regardless, using heavily-encrypted messaging systems can put a bit of a beacon on you, at a time when you might be hoping to stay as unobtrusive as possible.

It's this precise problem that *The Guardian* and developers at the University of Cambridge hoped to solve with the CoverDrop messaging system. It's designed specifically for users of news apps to be able to make confidential submissions to journalists without leaving a telltale trail of evidence that could reveal their actions. It's intended to be suitable for implementation by a wide range of news agencies if so desired, as laid out in the project white paper.



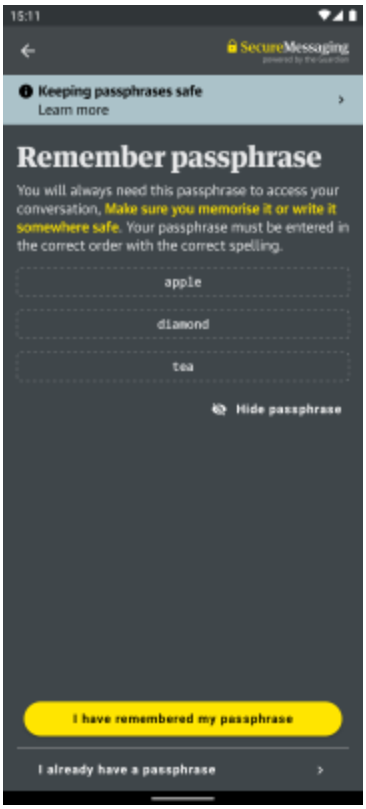
The CoverDrop system is built to maintain message security while also providing deniability for those using the system. Credit: The Guardian via Github

The CoverDrop system uses multiple techniques to not just encrypt messages, but hide whether or not any messaging is happening in the first place. The key is that CoverDrop is integrated into every copy of the *Guardian's* news app out there, and each app sends small amounts of encrypted information to the system at regular intervals. Most of the time, this is just meaningless text with no information content whatsoever.

That is, unless somebody has a message to send to a journalist. In that case, the message and the source's public key is encrypted with the journalist's public key, packaged up, and sent in such a way that it appears fundamentally no different to any other garbage message that is being sent to the CoverDrop servers. Both real and cover messages are encrypted the same way and have the same length, and are sent at the same times, so anyone monitoring network traffic won't be able to tell the difference.

At the receiving end, CoverDrop's secure servers remove an initial layer of encryption to filter out real messages from the cover messages. These are then provided to journalists via a dead drop delivery system, which pads the still-encrypted real messages with some cover

messages to ensure the drops are always the same size. In the event a dead drop contains a message for a given journalist, they can decrypt it since it was encrypted with their public key in the first place. Since the messages also include the source's public key, replies can be sent in the reverse fashion in a similarly secure way.



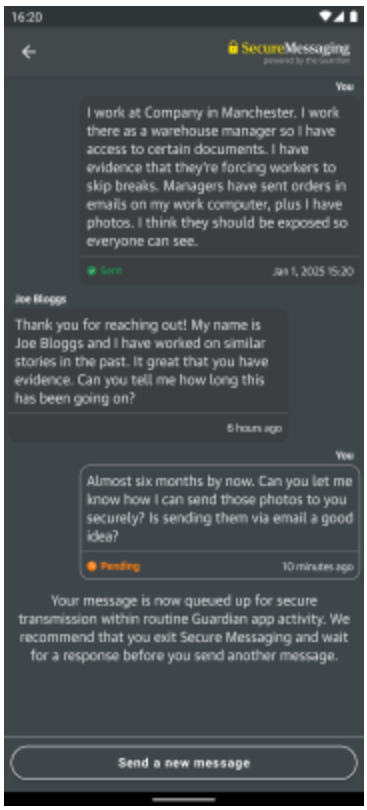
Messages sent via the app are encrypted, and are only retrievable with the use of the correct passphrase. Otherwise, the app will appear as if no messages were sent at all. Still, this doesn't stop malicious interrogators from beating you if they think you're holding out on coughing up a passphrase, regardless of if you have one or not. Credit: The Guardian via Github

As for on-device security, the system is designed to be as unrevealing as possible as to whether it has been used for secure messaging or not. Message storage vaults used by the app are encrypted, maintained at a regular size, and are routinely modified at regular periods whether covert messages are being sent or not. Unless the decryption passphrase is known, there is no obvious evidence that the app has been used to send any messages at all.

For those eager to implement the system, or merely audit its functionality, the CoverDrop codebase is available on Github. Providing a secure *and* deniable method of submitting sensitive tips is desirable to many newsrooms, which could lead to wider adoption or similar systems popping up elsewhere. Of course, no system is absolutely secure, but having a messaging system that focuses on more than just simple encryption will be a boon to those looking to communicate with less fear of surveillance or retribution.

Posted in Current Events, Featured, Interest, Security Hacks

Tagged encryption, news, news app, secure communication, security, the guardian



The system is designed for secure two-way communication between journalists and sources. This means if you want to chat securely with your friends, one of you has to get a job at The Guardian. Whether that's a price worth paying is for you to decide. Credit: The Guardian via Github

← THE MOON IS SAFE, FOR NOW: NO COLLISION IN 2032 AFTER ALL

TAKE A RIDE ON WRONGBAUD'S HARDWARE HACKING HIGHWAY →

25 THOUGHTS ON “SECURE COMMUNICATION, BURIED IN A NEWS APP”

UnderSampled says:

March 9, 2026 at 7:57 am

Does this count as steganography? It certainly an interesting technique, to introduce a new medium that’s easy to hide in. On the other hand, isn’t encrypted messaging *already* a good percentage of network traffic, now that HTTPS is commonplace? The app should already be making all of it’s requests to the Guardian through encryption. I’d be curious to understand where that isn’t sufficient.

Reply

Report comment

Defdefred says:

March 9, 2026 at 1:01 pm

Is https secure?
In China, only tls 1.3 is forbiden…

Reply

Report comment

JNA says:

March 11, 2026 at 2:08 pm

B/C of government mandated MITM though (probably).

Report comment

Reply

Truth says:

March 10, 2026 at 3:34 pm

https relies on 100% valid certificates, which, through deliberate design, can be generated and issued by ANY certificate authority globally for any DNS domain.

However since 2017, it is mandatory for every certificate authority to check DNS records of the domain name for a list “Certification Authority Authorization” before issuing a valid certificate. If they are not on the list they should not issue a valid certificate. But if you are a state actor and have enough control to fake DNS entries, these safeguards can be bypassed by orwellian regimes.

It always boils down to who you are trying to prevent from read your messages.

Reply Report comment

JayTee says:

March 9, 2026 at 8:23 am

Easy “fix” if you’re an oppressive regime: just make having news apps evidence of guilt. Problem == solved.

Reply Report comment

Mark Topham says:

March 9, 2026 at 8:50 am

Bingo.

Reply Report comment

A says:

March 9, 2026 at 8:55 am

I was thinking the same, it’s a clever idea but unfortunatley not much better than regular encryption apps if you have to have the app of a banned media outlet. Might be some use in the US where there’s still a pretence that the government believes in free speech.

Reply

Report comment

dremu says:

March 9, 2026 at 9:10 am

> *Might be some use in the US where there's still a pretence that the government believes in free speech.*

I assure you that has gone out the window, now that we have a circus peanut as president.

Reply

Report comment

a_do_z says:

March 9, 2026 at 9:18 am

It's interesting that you feel free to make such a comment.

Reply

Report comment

Chris Daniels says:

March 9, 2026 at 10:11 pm

I think there's quite a difference between whether the government, or the representatives thereof, believe in Free Speech and whether free speech is actively being curtailed. In the US, it's really under the courts purview, in cases including Murthy v. Missouri (2024) National Rifle Association v. Vullo (2024) Molina v. Book (Ongoing) Students for Justice in Palestine at the University of Florida v. Raymond Rodrigues (Ongoing). Certainly Obama was not a free speech champion either, none of the Presidents have been for a while, although lately Republicans and even conservative media seem determined to misrepresent when and what freedoms are being violated, and how; that's become more partisan. So, no, it's not just the current administration, but saying so here isn't really indicative of anything.

Report comment

David says:

March 9, 2026 at 9:23 am

When I hear people comparing *SOME_PERSON* to *SOME_OBJECT* the cynic in me wants to ask “what do you have against *SOME_OBJECT*?”

Reply

Report comment

Wilko says:

March 9, 2026 at 9:45 am

“what do you have against SOME_OBJECT?”

nothing, but I think it pretty insulting for SOME_OBJECT

Report comment

echodelta says:

March 9, 2026 at 11:39 am

It’s been a long time since I ate one of those orange puffed squishy candies that I originally thought were imitation orange sections. They were always associated with the cheapest of any candy. If you know what that particular candy represents, it’s the best polite metaphor I’ve heard yet. People in China and Russia have to use such meta words to conceal meanings when referring to their own great leader.

Report comment

Jeff Wright says:

March 10, 2026 at 11:06 am

This is why you hack the computer in another cubicle, and have that news app only visible via this tech–“negative light:”

https://techxplore.com/news/2026-03-negative-technology-plain-sight.html

This way you not only have plausible deniability, but you get to cosplay THEY LIVE, but for reals…in that only you see the feed with proper optics as your dull-witted cubicle mate lusts after the red Swingline.

“I always knew he was bad, commissar!”

Reply

Report comment

yngndrw says:

March 9, 2026 at 2:24 pm

Or in the UK, they will just require all apps with encryption to require ID and age verification.

Reply

Report comment

Foldi-One says:

March 10, 2026 at 4:36 am

And that verification must be provided by approved suppliers, that probably all have ties to Blair in some way…

Reply

Report comment

SteveT says:

March 9, 2026 at 9:35 am

Reminds me of the shortwave radio number stations. Send a lot of random info so you can hide small bits of important info.

Reply

Report comment

Piotrsko says:

March 9, 2026 at 11:09 am

Even better yet, don't send anything but do force the interceptors to waste time and resources to verify that

Reply

Report comment

Andrew says:

March 9, 2026 at 1:17 pm

Don't send anything, but force the interceptors to waste time beating people up while insisting something was sent.

Report comment

Reply

ialonepossessthetruth says:

March 9, 2026 at 12:07 pm

“Message storage vaults used by the app are encrypted, maintained at a regular size, and are *routinely modified at regular periods* whether covert messages are being sent or not.” That strikes me as a possible problem.

I know what a “dead drop” is in meatspace, is the author talking about a dropbox?

Reply Report comment

Richard says:

March 9, 2026 at 12:12 pm

The cynic in me thinks that this is a great way for the news apps to spy on all their users. The random nonsense sent back periodically might not stay so random

Reply Report comment

D says:

March 9, 2026 at 8:29 pm

…what? The system described here is for sending messages that must be hidden. App monitoring doesn’t even fall into that category.

The only defense to an app spying on you is an OS that denies permissions by default. The apps already can (and do) phone home about anything you do within the app. I work at a not-very-large company and every tap you make in our app is logged to our server. No need for any of the stuff above.

Reply Report comment

 says:

March 9, 2026 at 3:28 pm

Tyrannical Government: “So it is just random data eh, OK then we will block those packets and it will have no impact on users.” …

Reply

Report comment

Jim Horn says:

March 9, 2026 at 9:48 pm

Good old Autodin's EFTO comes to mind...

Reply

Report comment

Hugo Oran says:

March 10, 2026 at 12:50 am

Recommended reading to multilayered cryptography: Memoirs Found in a Bathtub, Stanislaw Lem, 1961

Reply

Report comment

Leave a Reply

Please be kind and respectful to help make the comments section excellent. (Comment Policy)

This site uses Akismet to reduce spam. Learn how your comment data is processed.

SEARCH

Search ...

SEARCH

NEVER MISS A HACK

SUBSCRIBE

Enter Email Address SUBSCRIBE

IF YOU MISSED IT

POKEMON GO HAD PLAYERS CAPTURING MORE THAN THEY REALIZED

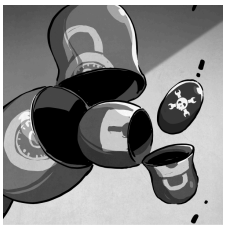
No comments

GERMAN FIREBALL'S 15 MINUTES OF FAME

7 Comments

THE "TIN BLIMP" WAS A NEITHER TIN NOR A BLIMP: THE DETROIT ZMC-2 STORY

21 Comments



SECURE COMMUNICATION, BURIED IN A NEWS APP

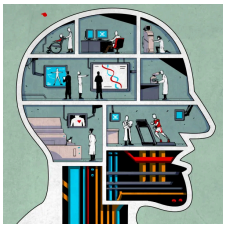
25 Comments

NEW ARTEMIS PLAN RETURNS TO APOLLO PLAYBOOK

54 Comments

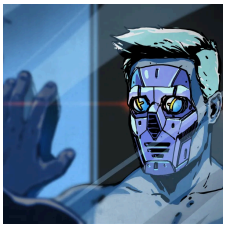
More from this category

OUR COLUMNS



BLOOD TESTS COULD PROVIDE EARLY WARNING OF ALZHEIMERS DISEASE

2 Comments

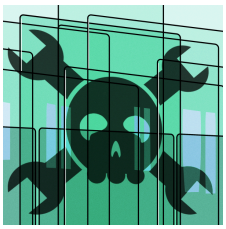


ASK HACKADAY: WHAT WILL AN LLM BE GOOD FOR IN THE PLATEAU OF PRODUCTIVITY?

67 Comments

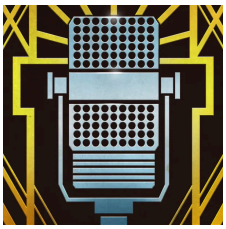
HACKADAY LINKS: MARCH 8, 2026

8 Comments



CHOICE, CONTROL, AND INTERRUPTION

47 Comments



HACKADAY PODCAST EPISODE 360: COOL RUBBER BANDS, SCIENCE-Y STUFF, AND THE WHYS OF OFFICE SUPPLIES

7 Comments

More from this category

NEVER MISS A HACK