How applications like signal can undermine national security

Description:

The Department of Defense (DOD) uses encrypted applications in order to do their work for securing communications across DOD infrastructure and to support military operations.

For this article, we exammon and ask the question, is signal secure for government communications? Why, or why not?

# Information about the article and author

Adison Verlice. [averlicetech@proton.me](mailto:averlicetech@proton.me)

Cybersecurity enthusiast

Publication date is N/A.

# Notice

This article is written and made by Adison Verlice.

You have permission to distribute the copy free of charge or permission.

You may also build upon this work without permission, given you have given adison verlice credit

You do not have permission to claim ownership of this article.

All sources used within this document, along with being linked to the relevant part of the article, will be listed after the article.

# Introduction

Before we can talk about this, we need to discuss what signal <https://signal.org> is.

From [wikipedia](https://en.wikipedia.org/wiki/Signal_(software))

Wikipedia

“Signal is an American open-source, encrypted messaging service for instant messaging, voice calls, and video calls. The instant messaging function includes sending text, voice notes, images, videos, and other files. Communication may be one-to-one between users or may involve group messaging.”

To summarize the signal for you, it’s an end to end encrypted messenger that secures messages, and calls.

# Signalgate

On March 24th, 2025, Jeffrey Goldberg reported on the Atlantic that Trump's national security adviser Mike Waltz had sent war plans by accident to him.

<https://www.theatlantic.com/politics/archive/2025/03/trump-administration-accidentally-texted-me-its-war-plans/682151/>

March 24th, 2025

Jeffrey Goldbirg

Published by the atlantic

From jeffrey: “U.S. national-security leaders included me in a group chat about upcoming military strikes in Yemen. I didn’t think it could be real. Then the bombs started falling.”

He was added to a signal chat that had JD Vance, Pete Hegseth, Michael Waltz, and even the director of national intelligence Tulsi Gabbard, along with other top officials in Trump's cabin and administration.

# The problem with signals.

Signal is great for end to end encrypted messaging.

However, there are a few things it should not be used for.

1 of those things is for sending war plans, or any top secret information for that matter.

Here are some underlying problems with signal.

# Potentially violates the federal records act.

# Federal records act (FRA)

<https://www.archives.gov/news/topics/federal-records-act>

“Records are the foundation of open government, supporting the principles of transparency, participation, and collaboration. Well-managed records can be used to assess the impact of programs, to improve business processes, and to share knowledge across the Government. Records protect the rights and interests of people, and hold officials accountable for their actions. Permanent records document our nation's history.”

To put that in dumb language, this basically means the government is required to maintain records.

Signals, disappearing messages, could potentially violate this act with disappearing messages feature.

<https://support.signal.org/hc/en-us/articles/360007320771-Set-and-manage-disappearing-messages>

The reason this could potentially violate the FRA is because, well, the government can’t store those messages, meaning that they can’t manage those records, and can’t see if the administration, say, violated a law using signals.

In fact, the DDS (defense digital service) issued a memorandum basically saying, do not use signal, because of this.

<https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Personnel_Related/22-F-0350_DDS_Comms_Policy-Signal.pdf>

“The practical impact of this restriction shows up in the use of the communication application, Signal. The developers envisioned strong encryption paired with automatic deletion of content in order to provide secure messaging – and they succeeded. The consequence of this success with the addition of voice calls in 2017, has made Signal a preferred method for hosting secure communications. Of course, the downside is that Signal does not require messages to be stored, and allows the user to set up auto-deletion for specified periods ranging from 5 seconds to 7 days. As a result, DDS cannot track this activity – or comply with FREEDOM OF INFORMATION ACT (FOIA) requests for files. 5 USC § 552, et seq. Yet, unless someone officially records them, voice communications – ordinary calls over ordinary providers using ordinary encryption – are too ephemeral to capture and too impractical to store. So, at present FOIA does not require agencies to record phone calls. “

# Personally identifiable information (PII).

As you know, if you’ve ever signed up for signal, you will know it requires a phone number to use.

If government employees are using their personal phone number, that means they are exposing themselves to danger. Even if there is a hash rather than the phone number being in plaintext, that is still a threat as those phone numbers can be dehashed.

# Public infrastructure

Signal is public infrastructure.

And cellcrypt hosts a great article on why this is bad.

<https://www.cellcrypt.com/post/consumer-secure-messaging-apps-are-not-the-solution>

To give you an idea, here’s a summary.

Signal messages, yes, are end-to-end encrypted, but again, they store PII about you, and that is not good for the military.

Also, public infrastructure, if it gets hacked, metadata, at least forms of it, is available.

Additionally, it doesn’t have any government related features, so it’s not like the DOD could manage users

Plus, if signal servers get hacked, they could potentially push an update which pushes malicious software (this can be said for any company).

I have taken some text from the post, this ones a bit long but you should read it.

“Encrypted messaging apps like WhatsApp and Signal implement end-to-end encryption, but their server infrastructure is still exposed to the public Internet. A compromise of their servers or takeover of message routing channels could allow highly capable adversaries to disrupt communications or selectively degrade service.

WhatsApp has also experienced security flaws that allowed remote code execution on its servers in the past. Even Signal, while open-source and security-audited, still relies on centralized services, which remain prime targets for well-resourced attackers aiming to undermine the platform's integrity.

Metadata Leakage Despite Encryption

**Salt Typhoon Tactic: Infiltrating lawful interception systems to gain access to sensitive communication records and metadata.**

Both WhatsApp and Signal generate metadata like IP addresses, phone numbers, and message timestamps that can reveal highly sensitive information about contacts and communication patterns even without access to message contents.

WhatsApp's metadata leakage is even more concerning because the app integrates closely with the mobile device's contact list and relies heavily on phone numbers as user identifiers. Similarly, Google Messages generates metadata that can be exploited despite its encryption features. The danger multiplies further when the metadata from these apps gets vacuumed up by global telecom infrastructure and routing systems outside the control of enterprises.

Susceptibility to Manipulated Routing and Connectivity

**Salt Typhoon Tactic: Leveraging trust relationships between different networks to expand attacker reach via manipulated routing (i.e. BGP hijacking).**

WhatsApp and Signal rely fundamentally on the public internet backbone, global DNS infrastructure, and third-party content delivery networks (CDNs) to transmit messages between different devices and regions. Highly sophisticated adversaries can potentially exploit blind spots in these trust relationships through tactics like rerouting data flows or launching man-in-the-middle interception attacks. Even with encryption in place, attackers faking or manipulating connectivity paths can effectively block, slow down, or selectively allow communications to disrupt operations and gain a situational advantage.

Consumer apps offer little to no enterprise control or custom routing options to counter these advanced network-level attacks, and their security features may not be sufficient to address these vulnerabilities.

Providing a False Sense of Security

**Salt Typhoon Tactic: Covering up evidence of infiltration and data exfiltration within the "noise" of legitimate user communications.**

One of the most pernicious aspects of these messaging apps in sensitive environments is that they can instill a false sense of security among high-value targets. Users may feel protected because their messages are "end-to-end encrypted", not realizing that resourceful adversaries have numerous other ways to access their communications.

The apps provide a side channel that sophisticated attackers can then silently monitor or infiltrate with advanced malware, confident that users will discuss sensitive topics. This creates an extremely attractive "honeypot" for hostile intelligence gathering and data exfiltration that's psychologically masked by the apps' encryption promises.

The Historical Trail of Compromises

Far from hypothetical, several high-profile security incidents have already proven how vulnerable telephone networks, as well as enterprise and consumer messaging apps, can be against determined attackers, underscoring the need for enterprise-grade secure communication tools to protect sensitive information:

* **Operation Socialist (2010-2013):** Leaked documents revealed how Britain's GCHQ successfully infiltrated the networks of Belgacom (now Proximus), a major Belgian telecom company. The agency gained access to Belgacom's employees' computers and private communications, likely including popular consumer messaging apps. This showed that even strong encryption is moot if the underlying network gets compromised.
* **Android FakeSMS Malware (2021)**: Researchers discovered new Android malware called FakeSMS that targets messaging and social media apps like WhatsApp, WeChat, and Twitter. The malware spread via trojanized Android app stores and used fake sign-in overlays to steal credentials and session keys. This highlighted the risk of malicious apps abusing the accessibility features of mobile operating systems.
* **SolarWinds Supply Chain Breach (2020)**: Russian intelligence hackers pulled off a massive supply chain attack by compromising the update infrastructure of SolarWinds' Orion IT management software. The tainted updates provided a foothold to breach hundreds of organizations and government agencies. The same supply chain risk could easily apply to the auto-update mechanisms of any consumer messaging app.
* **WhatsApp's CEO-impersonation Hack (2019)**: Security researchers demonstrated a clever social engineering attack against WhatsApp's verification system. They used a rogue phone number and other tricks to impersonate another user's account and access their contact list and messages. This proved that encryption alone does not stop some very low-tech threats.“

# What do the DOD usually use?

Offen, you’ll find the DOD using something like cellcrypt.

For example, for the DMCC-TS classified phone, one of the applications listed is cellcrypt.

<https://www.disa.mil/-/media/Files/DISA/Fact-Sheets/DMCC-TS-FactSheet_051220.ashx>

Also, there is a special internet the DISA created, known as secret internet protocol router (siprnet).

<https://apps.dtic.mil/sti/citations/ADA512554>

“SIPRNET, the Secret Internet Protocol Routing Network, is DoDs wide area network for encrypted hosts handling classified traffic. It is managed by the Defense Information Systems Agency. In 1997 the U.S. Naval Observatory established network time synchronization service on SIPRNET, with dedicated servers providing Network Time Protocol NTP. These servers are synchronized to the USNO Master Clocks. An overview of time server design is presented, with details on expected accuracy and accessibility.”

The national security agency also has a list of products on classified commercial solutions.

See <https://nsa.gov/csfc> for more information

# Some other (possible) attack vectors

# The possibility of compromise

Because they were using signals, it’s likely that the devices used were not DOD approved.

This means that SS7, or other attack vectors like someone falling for a phishing attack could’ve fallen at the hands of a nation state actor like China or their enemies.

They may have also not followed the DODs best practices for mobile device security, such as location services being turned on, and possibly taking devices to sensitive areas.

<https://www.arcyber.army.mil/Portals/78/Documents/FactSheets/NSA%20Mobile%20Devices%20Best%20Practices/NSA%20FACT%20SHEET%20MOBILE_DEVICE_BEST_PRACTICES%20(OCT%202020).PDF?ver=uVTyj5wWZya_EGQvulnz-g%3D%3D>

There is also a possibility that they were using home networks that were not at a classified state, and therefore, if that is the case, that would have resulted in networks being compromised.

# Conclusion

The conclusion is that you should not use signals for top secret information, as it undermines national security.

**References**

cellcrypt. (2024, 12 6). *From the Frying Pan to the Fire: Why Consumer 'Secure' Messaging Apps Are NOT the Solution in a Post-Salt Typhoon World*. Why Consumer 'Secure' Messaging Apps Are NOT the Solution in a Post-Salt Typhoon World. Retrieved 30 3, 2025, from https://www.cellcrypt.com/post/consumer-secure-messaging-apps-are-not-the-solution

defense information systems agency. (2015, 9 15). *DMCC-TS Classified Phone*. DMCC-TS Classified Phone. Retrieved 3 30, 2025, from https://www.disa.mil/-/media/Files/DISA/Fact-Sheets/DMCC-TS-FactSheet\_051220.ashx

executive services directorate & defense digital service (DDS). (2020, 10 27). *Policy On Use Of Communication Applications - signal*. BAH 20201027 DDS Coms Policy - Signal. Retrieved 3 30, 2025, from https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Personnel\_Related/22-F-0350\_DDS\_Comms\_Policy-Signal.pdf

Goldberg, J. (2025, March 24). The Trump Administration Accidentally Texted Me Its War Plans. *The Trump Administration Accidentally Texted Me Its War Plans*. https://www.theatlantic.com/politics/archive/2025/03/trump-administration-accidentally-texted-me-its-war-plans/682151/

National Archives. (2023, March 28). *The Federal Records Act*. National Archives. Retrieved April 5, 2025, from https://www.archives.gov/news/topics/federal-records-act

national security agency. (n.d.). *National Security Agency | Mobile Device Best Practices*. Department of Defense. Retrieved April 5, 2025, from https://www.arcyber.army.mil/Portals/78/Documents/FactSheets/NSA%20Mobile%20Devices%20Best%20Practices/NSA%20FACT%20SHEET%20MOBILE\_DEVICE\_BEST\_PRACTICES%20(OCT%202020).PDF?ver=uVTyj5wWZya\_EGQvulnz-g%3D%3D

Schmidt, R. E., & NAVAL OBSERVATORY WASHINGTON DC. (1997, november 01). *Defense Technical Information Center*. DTIC. Retrieved April 5, 2025, from https://apps.dtic.mil/sti/citations/ADA512554

signal foundation. (n.d.). *Set and manage disappearing messages – Signal Support*. Signal Support. Retrieved April 5, 2025, from https://support.signal.org/hc/en-us/articles/360007320771-Set-and-manage-disappearing-messages

*Signal (software)*. (n/a, n/a n/a). Wikipedia. Retrieved March 31, 2025, from https://en.wikipedia.org/wiki/Signal\_(software)