The FBI Communications Breach of 2010: Applications and Perspectives

by

Marc J O'Connor

First appearing in the autumn issue of 2600: The Hackers Quarterly, December 2021

The FBI Communications Breach of 2010: Applications and Perspectives

Marc J O'Connor

Introduction

This paper explores the "FBI communications breach," first reported in 2019, as an application of publicly known and researched vulnerabilities of P25 communications systems and considers them in an operational and intelligence context with possible tactics employed and as exploration of open source technologies and literature.

This paper assumes the Russian Intelligence Service (RIS) targeted Federal Bureau Investigation (FBI) land mobile radio (APCO P25) and cellular telephony (4G LTE) employed by FBI counter-intelligence activities in order to develop intelligence on FBI counterintelligence operations directed against the RIS.

Overview

P25 Land Mobile Radio systems is the communication technology employed by law enforcement and emergency first responders by over 38 countries, including the US, Canada, Mexico and Russia. In the United States, it is the result of a decades long transition from analog single channel radio systems to networked digital radio systems beginning sometime in the 1990's and reaching some degree of completion in the mid-2000's.

APCO P25 Land Mobile Radio (LMR) systems are digital radio systems that provide narrowband data, voice encryption, addressable and trunked (like a subnet) communications. The P25 LMR can have 9,999,999 individually addressed subscriber units organized into Talk Groups. P25 can be trunked and transported over Internet Protocol networks.

The FBI maintains the largest P25 land mobile radio system in the world, providing nationwide coverage to federal law enforcement operations, and inferred in this paper, their counter-intelligence surveillance teams. The FBI maintains this system for the Department of Justice, and the customers are the DOJ appendixes: DEA, BATFE and U.S. Marshals Service and is not solely an FBI resource.

From public news services, it is found that the RIS employed an operation to develop intelligence from FBI telecommunications in 2010. These telecommunications is inferred to be the nationwide Land Mobile Radio (LMR) network developed by DOJ for federal law enforcement, and exploitation of the backup telecommunications system, provided in public sources as LTE, or Long Term Evolution, a cellular service more presently known as 4G, with an additional Push-To-Talk capability to act as a two-way radio.

Technical Background

An individual APCO P25 radio carried by a person or installed in automobiles is a "subscriber unit." Each subscriber unit must be programmed with a unique Unit Identification in order to participate in trunked or networked communication. Each unit must also be programmed with a group unique Talk Group Identification to participate in Talk Groups.

Cellular telephony selectors are better known: the IMSI or telephone number and the IMEI, which is the electronic serial number of many cellular devices. These two selectors, known as "the pair" are emitted constantly as the cellular device seeks an available base station to associate to the network. It is these selectors that are collected using IMEI catchers like the popular Stingray and Do-It-Yourself (DIY) systems.

P25 research has been performed using Software Defined Radio and Open Source software, notably, Ettus Research Universal Software Radio Peripheral (USRP) , GNU radio software and Wireshark.

It would appear axiomatic that an APCO P25 using country, like Russia, would have firsthand knowledge of vulnerabilities that would come to the attention of its intelligence services in addition to a large pool of talent and networks to develop technical exploits.

Operational-Technical Games

An actionable intelligence requirement for a clandestine intelligence officer is their surveillance status. Intelligence officers employ surveillance detection tactics, techniques and procedures to determine hostile surveillance status.

Based on known P25 and cellular handset vulnerabilities, it is possible to develop actionable intelligence to satisfy this requirement using only signal externals: the peculiar metadata accompanying each transmission that is necessary to implement the communications service, but does not include content, per se.

Here the presence of certain telecommunications metadata could aid in the surveillance determination. The "fact of " peculiar metadata in vicinity of the intelligence officer would strongly indicate hostile surveillance activity. That peculiar metadata may be envisioned as a "tag cloud" of selectors where each tag is a metadata element from some electronic device.

In this scenario, these metadata are the IMSI/IMEI from the PTT cellular devices, the Unit

Identification and Talk Group Identification from the inferred use of P25 radio's by the FBI and these metadata form part of the tag cloud surrounding the FBI counter-intelligence activity. These tag clouds are observable, unique and sufficiently unchanging.

RIS surveillance detection would take the FBI surveillance from the surveillance pick-up point, and maneuver on foot or vehicle to sift the collection of signal externals in order to isolate FBI peculiar selectors. That media reporting implicated California, New York and Washington D.C., RIS activities, then a better opportunity is presented for differentiation of selectors. In this, FBI tag clouds were observable at these locations, but the extraneous tag clouds unique to these locations would be eliminated, being peculiar to these geographic areas.

Over time, repetition of this sifting would refine the tag cloud collection---the same tag clouds in vicinity of an intelligence officer despite distance, observed and integrated over a long baseline. If one can envision that surveillance detection is a type of maneuver warfare, then the use of surveillance detection is limited by creativity and here it is likely used to provide a sifting/filtering mechanism.

The use of surveillance detection augmented with signals monitoring provided by COTS hardware and software would provide supporting data to confirm/deny the presence of FBI personnel in the area based upon presence of selectors and traffic analysis of Unit ID and Talk Group ID emitted from the APCO P25 handsets and IMSI/IMEI radiating from the PTT cellular handsets.

Once a RIS intelligence officer was certain they were under surveillance, this information may be correlated to observed selectors (the tag cloud) also at that point. Similarly, the absence of that metadata would inform perspectives as to a RIS officers surveillance status.

The use of traffic analysis and pattern observation from physical and technical surveillance is the crux of the exploit. Operational sophistication stems from this and it's fusion with tradecraft to produce military effects.

History

The use of SIGINT enhanced surveillance detection has precedents. In 1977, the CIA employed a specialized radio receiver to detect KGB surveillance of CIA officers stationed in Moscow. Such a receiver was discovered with CIA officer Martha Peterson after her capture by the Soviet KGB while she was engaged in a high-risk operation in Moscow.

KGB and East Bloc officers employed similar technologies with the *Kopchik* surveillance receiver. This communications breach is part of that historical and technical continuum.

Timeline of the Reported Breach in relation to P25 Security Research and News

2019 Yahoo breaks story. This is the first public reporting

2016 Russian diplomats expelled

2012 FBI "Full gravity" of breach realized

2011 P25 papers at Ruxcon and Securecomm

2010 FBI "First breach" detected; DES Research, first public P25 vulnerabilities made public

2009 Development of Open Source P25 research platform

Between 2010-2012, there was an investigation of the breach given the publicly reported outcome was "full gravity of hack realized." Such an investigation likely supported the expulsion of Russian diplomats and was a component of a larger counter-intelligence effort.

Application in Open Source Warfare

In this scenario, military effects--deny/degrade--were induced by one state actor upon another, but noteworthy that the technologies involved and the tactics needed to employ them are available as open source information and are developable and deployable by non-state actors.

Such application further distorts the symmetrical relationships and capabilities between state and non-state actors and develops a cognitive and perceptual terrain within that distorted space. Here, the non-state actor may develop counter-intelligence that can compete with the state actor security services and use this (formerly) advanced SIGINT capability in competition with other groups, as in a 4GW environment.

A perspective may be taken that this exploit was successfully tested between two technically and operationally sophisticated adversaries. Probably the most rigorous laboratory available for such an application.

Postface

This paper focuses on a plausible scenario of communications exploitation that would produce actionable intelligence using open source technologies. The thesis was developed from well-known security research that was operationalized in these exploits. It does not include specious and sensational narratives of vague "backdoors," and "broken encryption."

Bibliography

1. Zach Dorfman, Jenna McLaughlin and Sean D. Naylor. “Russia carried out a 'stunning' breach of FBI communications system, escalating the spy game on U.S. soil.” Yahoo! News, 16Sep2019. https://www.yahoo.com/now/exclusive-russia-carried-out-a-stunning-breach-of-fbi-communications-system-escalating-the-spy-game-on-us-soil-090024212.html

2. William Jackson. “Project 25: The Long And Winding Road To Radio Interoperability.” GCN,09Apr2013.https://gcn.com/articles/2013/04/09/project-25-road-to-radio interoperability.aspx

3. Stephen Glass, Vallipuram Muthukkumarasamy, Marius Portmann, Matthew Robert. “Insecurity in Public Safety Communications: APCO P25. Security and Privacy in Communication Networks.” 7th International ICST Conference,” SecureComm 2011, 7-9Sep2011. https://eudl.eu/pdf/10.1007/978-3-642-31909-9_7

4. Sandy Clark, Travis Goodpseed, Perry Metzger, Zachary Wasserman, Kevin Xu, Matthew A. Blaze. “Why (Special Agent) Johnny (Still) Can’t Encrypt: A Security Analysis of the APCO Project 25 Two-Way Radio System.” https://www.mattblaze.org/papers/p25sec.pdf, 10Aug2011.

5. Matt Robert. “APCO P25 Security Revisited.” RUXCON 2011. https://paper.seebug.org/papers/old_sebug_paper/Meeting-Documents/Ruxcon2011/RUXCON_2011_slides.pdf. 19Nov2011.

6. Sandy Clark, Perry Metzger, Zachary Wasserman, Kevin Xu, Matthew A. Blaze. “Weaknesses in the APCO Project 25 Two-Way Radio System.” https://repository.upenn.edu/cgi/viewcontent.cgi?article=1990&context=cis_reports. 18Nov2010.

7. Chris Paget. Practical Cellphone Spying. DEFCON 18. https://www.defcon.org/html/links/dc-archives/dc-18-archive.html 30Jul2010.

8. Steve Glass, Portmann Marius, Vallipuram Muthukkumarasamy. “A software-defined radio receiver for APCO Project 25 signals.” https://publications.csiro.au/publications/publication/PInicta:1710. 2009

9. https://www.cryptomuseum.com/people/peterson/index.htm

10. https://www.cryptomuseum.com/covert/radio/srr100/index.htm

11. https://www.cryptomuseum.com/covert/radio/kopchik/index.htm

12. Davey Winder. "Russian Spies Breached FBI Encrypted Communications" Forbes. https://www.forbes.com/sites/daveywinder/2019/09/18/russian-spies-breach-fbi-encrypted-communications-no-backdoor-needed/?sh=41366592128d. 18Sep2019.

13. Mike Masnick. "You'd Think The FBI Would Be More Sensitive To Protecting Encrypted Communications Now That We Know The Russians Cracked The FBI's Comms." Techdirt. 17Sep2019.

Contact

The author and publisher disclaim any responsibility from the use or misuse of this information.

Website: forestfrontpress.net | forestfrontpress.org

Contact: https://linktr.ee/forestfrontpress

LoFi Contact: https://pastebin.com/nnxdkQAA

Donations: https://www.buymeacoffee.com/5339529

Marc J O'Connor is the author of "Electronic Warfare for the Fourth Generation Practitioner."

Take care (and control)!