The Role of Commercial End-to-End Secure Mobile Voice in Cyberspace

Elad Yoran
Edward G. Amoroso

ABSTRACT

Commercially-available, end-to-end encryption software application solutions address cyber threats from advanced nation-state actors by securing mobile voice communications from eavesdropping. Existing mobile security frameworks, such as explained in a recent Department of Homeland Security (DHS) study, provide a good base for analysis, but are shown to have dealt insufficiently with the threat to mobile voice and corresponding encryption-based safeguards. A secure cyberspace thus requires increased attention to securing voice in addition to data when using mobile devices.

INTRODUCTION

During the Vietnam War, the National Security Agency (NSA) supported a tactical secure voice system called NESTOR,[1] which was used for communications between American warfighters. NESTOR equipment was bulky, often requiring a large man-pack. To make a secure call, the operator had to work through a series of complex keying options using a mechanical loader with a matrix of switches. Once connectivity was established, voice quality using this secure voice scheme was generally poor.

Fast forward to modern civilian, industrial, and military contexts, and one finds a variety of improved options for secure voice. The warfighter, for example, has access to customized Command, Control, Communications, Computers, and Intelligence (C4I) systems with rugged ergonomics and support for secure voice using special radios that offer location, texting, and related real-time data. These radios are typically tailored for military use and built to the specification of the warfighter (see[2], for example).

In addition, however, modern users of mobility in both military and non-military contexts now have access to secure end-to-end voice options using familiar, commercial off-the-shelf (COTS) solutions available on smartphones made by the likes of Samsung

Elad Yoran is Executive Chairman of KoolSpan and CEO of Security Growth Partners (SGP). He is a 20+ year cybersecurity veteran, among other things having founded and led many foundational cyber start-up companies. He was honored as "Entrepreneur of the Year" by E&Y. Elad's cybersecurity entrepreneurial experience includes Riptech, acquired by Symantec; MediaSentry, acquired by SafeNet; Sentrigo, acquired by McAfee; and Vaultive. Previously, Elad served as VP Global Business Development at Symantec. In addition, Elad was a strategic investor and advisor to Red Owl Analytics, acquired by Forcepoint; NetWitness, acquired by RSA; ThreatGrid, acquired by Cisco; and Insightix, acquired by McAfee.

He serves as director at Infinidat. Elad also serves on several government and industry boards. He is an advisor at the Army Cyber Institute, director of the Cloud Security Alliance, and previously, the FBI IT Advisory Council. Elad is the author of many cyber articles going back to the original Internet Security Threat Report research papers. Previously, Elad served as a US Army officer and is a graduate of the Wharton School and West Point.

and Apple. While one would not expect pure COTS to supplant tailored military voice applications, cybersecurity practitioners have come to recognize that cyber threats from nation-states and others extend far beyond traditional military and government organizations, and target commercial businesses for valuable IP, trade secrets, business strategies, negotiating positions, and more. Corporate espionage executed via interception of mobile communications is a growing global phenomenon.

As one might expect, mobility is a direct target in such contexts–and this includes the plethora of ecosystem components used to support mobility services. To this end, the DHS recently issued a technical report in conjunction with the National Institute of Standards and Technology (NIST). With the simple title: *Study on Mobile Device Security*[3], the report offers a thorough overview of issues in protecting mobile devices and systems from cyber threats across a range of individual, corporate, and government scenarios.

While the DHS study offers a thorough description of general mobile security, we believe that its emphasis on secure mobile voice is insufficient. Such oversight is indicative of a larger trend where protection of voice communication is often ignored by security engineers designing modern cyber defenses. With growing cyber threats to communications using mobile devices and infrastructure, increased focus in this area will help safeguard the use of mobility across all aspects of cyberspace.

General Model of Secure Mobility

A significant contribution of the *Study on Mobile Security* is that it offers a clean model of the commercially-available mobile ecosystem–one that we recommend as the canonical default for anyone trying to make a claim or technical point concerning any aspect of mobile security, including outside

Dr. Edward G. Amoroso is Chief Executive Officer of TAG Cyber LLC, a global cyber security advisory, training, consulting, and media services company supporting hundreds of major organizations across the world. Ed recently retired from AT&T after thirty-one years of service, beginning in Unix security R&D at Bell Labs and culminating as Senior Vice President and Chief Security Officer of AT&T from 2004 to 2016. He was elected an AT&T Fellow in 2010.

Ed has been Adjunct Professor of Computer Science at the Stevens Institute of Technology for the past twenty-nine years, where he has introduced over three thousand graduate students to the topic of information security. He is also a Research Professor in the Computer Science Department at the NYU Tandon School of Engineering, and a Senior Advisor at the Applied Physics Laboratory at Johns Hopkins University. He is author of six books on cyber security, and dozens of major research and technical papers in peer-reviewed journals and conference proceedings.

the United States. Below, we redraw the model with more generic icons and connections; readers are encouraged to use this simple base to instantiate a more tailored local enterprise view.

The components of the DHS mobile ecosystem model include the five main commercial components of government, enterprise, and consumer mobility: *Mobile devices, mobile apps, mobile operating systems, enterprise mobility management (EMM),* and *mobility networks.* These components form the base on which further cybersecurity investigation to minimize mobile risk can be performed. The DHS study does an admirable job in this regard for general threats to mobility for mobile data, mobile Internet, and mobile app usage.

Mobile devices and operating systems, for example, are shown to require considerable security regarding their design and operation. The device technology stack is shown to create opportunities to harden devices from advanced cyberattacks. Mobile apps made available from mobile app stores are also shown in the DHS study to offer opportunities for improved security, as are EMM systems, common in modern businesses.

The study also explains the challenges of mobile network infrastructure in dealing with attacks. It introduces a threat taxonomy that operators and users of modern WiFi, 2G, 3G, 4G, LTE, and emerging 5G networks must contend with, as they use commercially obtained mobile devices to accomplish their mission–whether business or entertainment-related. The report does not, however, adequately cover the threats or corresponding solutions for supporting secure mobile voice. The remainder of this paper is designed to fill in that gap.

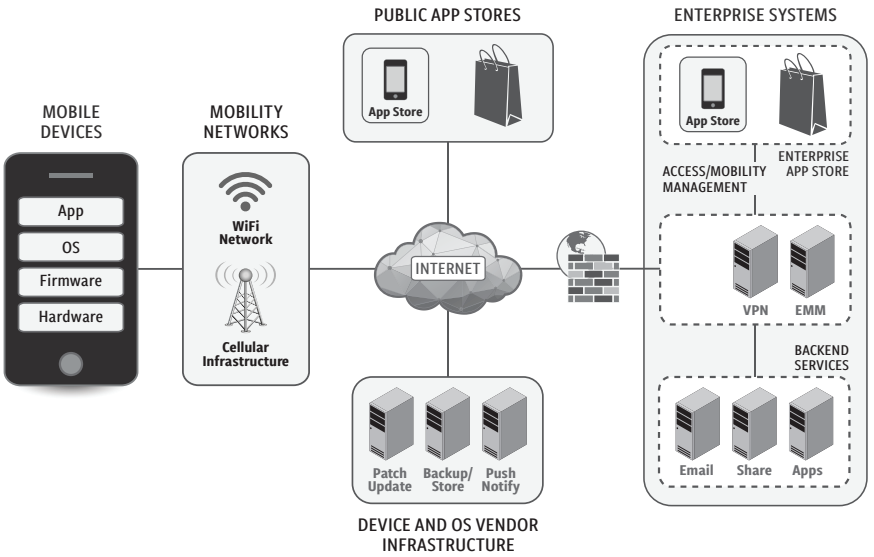

Figure 1. Generic DHS Mobile Ecosystem Model

Threats to Mobile Voice

The obvious threat to mobile voice is an eavesdropper listening to conversations for purposes that can range from military tactics to corporate espionage. For many years, security engineers have drawn the proverbial diagram showing Alice and Bob communicating end-to-end, with Eve positioned as an active man-in-the-middle adversary, collecting targeted communications from network media, and then analyzing and interpreting the content. In the early days of voice, this was done using simple wiretaps on circuit-switched lines.

One might have expected that with the advent of packet-switched voice communications such as Long Term Evolution (LTE), that mobile voice wiretapping would be no longer feasible. Internet packets, after all, are scattered across networks, which would seem to imply that adversaries with wiretap equipment would no longer have an easy time clamping onto a circuit to listen. The reality, however, is that many reasonable options still exist for modern mobile voice communications to be eavesdropped by third-parties.

The most commonly cited example of mobile voice interception by an adversary is the so-called *IMSI catcher method* [4]. Each mobile network operator (MNO) supports a non-secret individual mobile subscriber identifier (IMSI) that allows for differentiation between mobile end-users. The idea of an IMSI catcher attack is that a fake base station is placed proximate to the intended surveillance target. Since earlier generation mobile technologies including 2G services do not include tower authentication by the base unit, any device using such technology–and this includes popular fallback services for coverage–will be tricked to connect to the fake station.

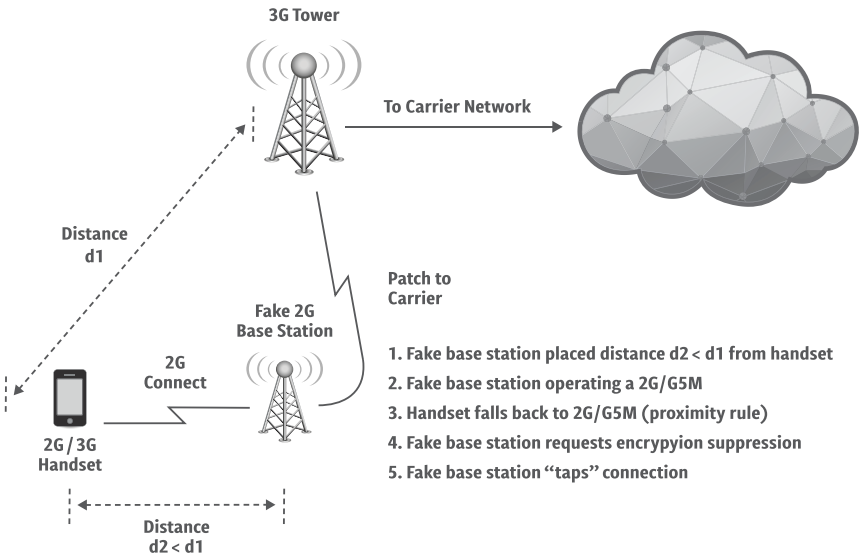

Figure 2. IMSI Catcher Concept

The result of this tactic is that the interceptor can collect all transmitted communications, such as a voice conversation, and through directed, suppressed encryption, can perform a wiretap. IMSI-based surveillance is prevalent today, including use by law enforcement organizations at Federal, state, and local levels. While they generate a fair amount of media attention and legal debate regarding the constitutionality of how IMSI catchers are used, over time, with most MNOs retiring older technologies in lieu of more secure mutually authenticated and encrypted protocols, this surveillance technique should be less of an issue. But it illustrates effectively the types of security problems that emerge in any complex mobile infrastructure setting, and it underscores the importance of security vigilance by the mobile carrier.

An additional and far more widespread and long-term threat to secure mobile voice involves the mobile network infrastructure. Core mobile network operation in the DHS report, for example, is recognized as having "virtually unlimited options and attack vectors." This has traditionally involved denial of service and other attacks on infrastructure, but more recently has involved weaknesses in the legacy Signaling System 7 (SS7) protocol, used for the past three decades as the global signaling standard for public switched telephony, which continues to support a large portion of mobile traffic.

SS7's designated successor, the Diameter protocol, supports similar functions. While Diameter is designed to be more resistant to attack, the Federal Communications Commission (FCC) claims that it could introduce new vulnerabilities that need to be considered. From an FCC report, the claim is made that "the two protocols work very differently as do their network substrates and systemic effects, and this should be taken into consideration when assessing Diameter. That said, the research community has given demonstrations

using the Diameter protocol to execute similar exploits seen on the SS7 network. Also, researchers have identified other potential, theoretical exploits on Diameter." [5]

From the perspective of secure voice services, the primary concern regarding SS7/Diameter is the purported possibility of a man-in-the-middle eavesdropping threat, which can include direct wiretaps of conversations by untrustworthy mobile network operators. As described in the DHS study, these threats have been demonstrated in numerous cases including by German researcher Tobias Engel [3]. According to the DHS report, "Gaining unauthorized access to the core SS7 or Diameter network is a risk since there are tens of thousands of entry points worldwide, many of which are controlled by countries or organizations that support terrorism or espionage." While direct access to SS7 has been assumed to be a pre-requisite, several scenarios have emerged with indirect access via femtocell or other equipment. [6]

Another consideration regarding this threat is the national economic threat posed by corporate espionage, especially in places where traveling business executives find themselves where the mobile network operator might be largely unconstrained regarding the SS7-based operation. This results in the unusual situation where the modern traveler experiences the type of threat pressure previously experienced by warfighters in foreign battlefields. Corporate IT Security teams deal with this problem through policies that prevent executive travel into certain regions with their mobile devices [7].

Commercial End-to-End Encrypted Calling

Users of mobility who are concerned with the mobile voice threats posed by IMSI catchers or signaling vulnerabilities–especially in cases where the mobile services are being offered in a geographic region with less robust security–should immediately consider the use of an over-the-top encrypted voice solution. This end-to-end risk mitigation makes perfect sense for the modern, traveling business executive. It also makes sense for anyone–including military personnel–who are concerned with secure voice protection.

The primary functional requirement for secure, end-to-end encrypted voice capability is that it operates independently of underlying mobile network operations. That is, over-the-top (OTT) security is a critical need if existing (or future) vulnerabilities in the network infrastructure could undermine confidentiality demands. This requirement also implies that the encryption support is enabled in proximity to the actual human voice, which suggests that end-to-end encryption becomes a client-enabled function embedded in the mobile device.

Due to this mobile endpoint emphasis, second-order functional requirements emerge to support secure end-to-end mobile voice. First, the end-user should not have to engage in complex administration such as manual keying. Instead, the secure mobile solution should make it simple for end-users to engage in encrypted calls without any specialized training. Second, the end-to-end solution must integrate with modern devices and services. In the

military, for example, as in the commercial world, it is impossible to separate the warfighter, corporate executive, or traveling business person from their iPhone and Android devices. They have become ubiquitous, and the convenience of voice calling, mobile app use, and Internet access have overshadowed threats targeting governments, business people, and citizens.

The overall functional schema for end-to-end secure mobile voice using commercially available devices and network services are shown in Figure 3 below. The administration and set-up of this capability are not shown on the diagram, but would likely follow procedures consistent with the procurement and use of any commercial capability such as buying and enabling an iPhone from an Apple store. This is an essential point because different products will have different administrative procedures for distribution, maintenance, and support (see [8] as an example of one provider's approach).

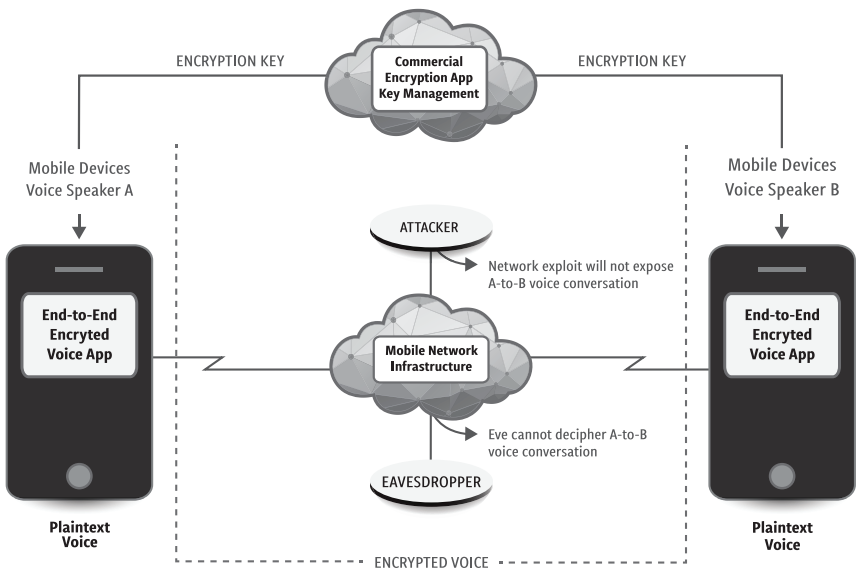

Figure 3. End-to-End Secure Encrypted Mobile Voice

This simple encrypted mobile voice set-up is surprisingly resilient against most modern cyber threats. Certainly, modern mobile communications would not be protected from massive destructive or denial-of-service attacks against the underlying network infrastructure; the provision of end-to-end encryption for voice deals with the disclosure issue primarily. In addition, this end-to-end solution using commercially available encryption would likely not be a robust option in cases where the adversary is likely to employ the most advanced forms of nation-state sponsored cryptanalysis. Tailored military encryption with the proper certifications would be best in these cases.

To the degree, however, that the modern virtual battlefield in cyberspace includes citizens, consumers, businesses of all sizes, civilian agencies, and military organizations–and this extends to all nations, the use of commercially available, end-to-end encryption solutions for mobile voice is both effective and recommended. As the DHS study called for end-to-end encryption for all communication paths, one would hope that national initiatives would be championed at the senior-most levels of government to drive this point. Everyone should be encouraged to make use of secure mobile voice, perhaps even as a casual matter of normal voice communications. With such senior emphasis, one might expect that future DHS studies would focus more on this issue.

CONCLUDING REMARKS

In closing, it is helpful to remember that mobile devices and the supporting ecosystem were originally developed to support voice applications and that this remains a foundational application of mobility. During the past decade, however, most marketing emphasis in mobility has been directed at messaging and mobile application use, rather than voice. We believe, however, as argued in this paper, that the pendulum has swung too far from voice and that mobile security will be better served with more balance between data and voice security.

To help demonstrate the reality of the threat to mobile voice, one might consider that the typical consumer or business person has repeatedly been warned to avoid typing anything into an email or social post that would reflect poorly if posted to the cover of a newspaper. We all know this common aphorism: *If you wouldn't want something printed in the New York Times, then don't put it into an email.* This is sensible advice, and most individuals have tried to adjust accordingly.

An irony, however, is that many sensitive business and personal communications have been shifted from written email to spoken voice, simply to avoid the prying eyes of some man-in-the-middle hacker. This is a good decision in the presence of proper voice security but can be cataclysmic in its absence. Perhaps a new warning should emerge: *If you wouldn't want the transcript of your voice conversation posted to WikiLeaks, then don't say it into your mobile.*

The good news is that with advanced secure end-to-end encryption solutions for mobile voice, the reality is that private citizens, business people, and government officials can make use of their commercially available mobile devices to hold private conversations beyond the reach of an adversary. With the front lines of cybersecurity now extending far beyond the traditional military battlefield, this advance is imperative. By employing such capability, we can all help make cyberspace a more secure environment in which to maintain a safe society.

NOTES

1. http://www.governmentattic.org/18docs/Hist_US_COMSEC_Boak_NSA_1973u.pdf.
2. https://defensesystems.com/articles/2017/11/cw/navy-darpa-voice-text.aspx.
3. https://www/dhs.gov/publication/csd-mobile-device-security-study.
4. https://techcrunch.com/2017/06/02/who-catches-the-imsi-catchers-researchers-demonstrate-stingray-detection-kit/.
5. Federal Communications Commission, *The Communications Security, Reliability and Interoperability Council V Working Group 10 Final Report March 2017,* https://www.fcc.gov/files/csric5-wg7-finalreport031517pdf.
6. https://www.cbsnews.com/news/60-minutes-hacking-your-phone/.
7. http://searchsecurity.techtarget.com/answer/How-to-protect-sensitive-data-when-executives-travel-abroad.
8. https://koolspan.com/solutions/.