Survey of security features in Ultraprivate Smartphone technology

Achyut Parajuli
Department of Computer Science and Technology
University of Bedfordshire,
UKachyut.parajuli@study.beds.ac.uk

Md Mehedi Masud
Department of Computer Science and Technology
University of Bedfordshire, UK
mdmehedi.masud@study.beds.ac.uk

Abstract— **Smartphones commonly available on the market are less secured and the networks we have been using for data transmission are vulnerable. This paper presents survey on Ultraprivate Smartphones and Silent circle Network (SCN) both meant to more secured means and medium of communication. Considering the importance of security features in mobile phone technologies this paper will focus on different secured features of Ultraprivate Smartphones and their platforms. It will also illustrate network and protocol architecture and give brief comparison with existing mobile platforms. Security issues and vulnerabilities are also discussed followed by proposed solutions to eliminate those threats.**

***Keywords* — Ultraprivate Smartphone, ZRTP, SCIMP, SRTP, silentcircle, blackphone, PrivatOS**

I. INTRODUCTION

Cybersecurity and data protection has become a prime concern for most of the governments and companies from advance to developing economies. Cyber criminals, advertisement agencies and amateur hackers are keeping eyes on our daily activities tracking our mobile phones and others electronic means like emails and Apps. Situation is even worsening. Smartphone manufactures cares more about better cameras, higher resolution and slim looks rather than strengthening security features. This paper discusses about currently available Ultraprivate Smartphones, their types and differences, Silent Circle Networks and its network protocols.

II. ULTRAPRIVATE SMARTPHONE

Ultra Private Phones are built keeping privacy and security in mind. Post Snowden Era general public are more concerned about their data security hence investing time and money on the development of these technologies makes scene. Once Blackberry phones were considered to be the most secured phones but things has changed now so secure phone manufacturers are trying to get a grip on this market. Not only devices network infrastructures and servers are very vulnerable and can act as open door for hackers/attackers to sniff private data. Black Phone and Boeing Black are currently the main manufacturers of Ultra Private smart phones [1]. These secured Smartphones can be used for business purposes and even to save our secure data For example card numbers if it is proved to be secured. Obviously to keep it safer from future challenges phone manufactures must invest on research mechanisms so it can be improved in regular basis.

A. Boeing Black

Boeing is a Chicago based aerospace and defense contractor which has more than 100 years of IT innovation experience. Boeing Black is built keeping security and modularity on mind. Its security is maintained by Boeing Pure-Secure architecture build upon layers of trust. It comes with self-destructive features which mean any attempt to open the casing of Boeing black phone it will delete all data it was holding. The main foundation of this architecture is chain of trust from embedded hardware devices, policy control mechanism of operating system and its compatibility with others devices operated in the market. Flexibility of this phone is enabled by a modular expansion port which can be used for integrating additional technology enhancements and other customizations. Boeing black comes with disc encryption feature so even sensitive information can be stored securely. It runs with Android operating system with added security features which restrict it from data compromise and leakages. It comes with dual SIM feature which lets users to switch from commercial networks to government networks or vice versa. Boeing Black has excellent compatibility features which let it to operate seamlessly with VPN and customers mobile device management system [2].

B. Silent Circle Blackphone

Encryption firm Silent Circle which was developed by Phil Zimmerman and a mobile phone company Geeksphone teamed up to produce the Blackphone which runs on modified Android Operating System called PrivatOS. It is also called 1st level security of Black phone. PrivatOS was fortified by Blackphone experts addressing current privacy concerns as there is no leaky data, no bloatware and no hooks to carrier by default [1][4].

C. PrivatOS vs Android (Default)

In contrast Android phones by default are traceable, it comes with bundles of Apps which are privacy disabled by default, it’s Wi-Fi remains on for geo-location and user tracking and it is vulnerable to spoofed cell networks and Wi-Fi.

Balckphone are safer and secured then others as Balckphone uses its own Silent Circle Network which is built specially for secured communication of encrypted data using ZRTP and SCIMP protocols for transmission of voice and emails/texts.

There is another ultra-private phone available in the market called 'Snowden Phone'. It uses 128 bit encryption which is same to that of banks and government agencies. Enhanced security features are shown in table below [17].

Feature	PrivatOS Enhancement
Search	Anonymous
Bundled Apps	Few, all privacy enabled
Wi-Fi Usage	Smart disabling of all Wi-Fi expect trusted hotspots
App permissions	Fine-grained control in single interface
Communication Tools	Private calls, texting, video chat, file exchange up to 100mb, conference calls
Updates	Frequent secured updates from Blackphone directly
Remote Wipe and anti-theft	Delivering privacy as a premium, valued feature

Table 1: PrivatOS features

III. ARCHITECTURE OF ULTRAPRIVATE SMARTPHONES

A. Silent Circle Network overview

Silent circle Network is a network specially built for secure transmission of private data/information and is also called 2nd layer Security. They own, control and custom built their own equipment which reduces any kind of contractual risks. Silent Circle Network uses its own custom built servers, hardware, software and CODECs to ensure security is integrated through design. Every communication session will have to comply peer to peer key negotiation and encryption. Network servers with in the secure circle network do not hold any key and all the data are encrypted which reduces the risk of data interception while it is being transmitted or data disclosers as servers do not hold keys to unlock data. Keys are destroyed at the end of each communication session eliminating the risk of retroactive compromise.

Silent Circle Network do not use off the shelf infrastructure instead it has its own PBX, servers and hardware which helps it to increase its network performance since it will be using infrastructures specially built integrating security features through design.

Video and vocal verification technique applies Short Authentication string (SAS) to avoid man in the middle attacks. SCN uses peer reviewed encryption which is more trustworthy and has very little chances of bugs which will definitely help to increase the reliability and effectiveness of the whole network.

It also uses peer reviewed hashing algorithms which are specially written keeping security aspect and nature of network on mind. SCN firmly adopts minimum data retention policy so only adequate data is logged to keep daily service moving.

B. ZTRP overview

Internet based VOIP calls are growing fast as a replacement of PSTN based phone calls. Lack of security features and infrastructure makes VOIP sessions more vulnerable to intercept than PSTN based calls. ZRTP provides solutions to eliminate security risks for both voice and VOIP calls. This protocol provides stronger encryption to secure communication sessions between two parties.

During initial stage RTP is used as transport protocol and data is transferred through SRTP after session starts. ZRTP does not need support from signalling protocols but provides option for integration. Key agreement based protocol uses DH key exchange rather than PKI which makes it more secured. Encryption and authentication is performed over RTP sessions of peer-to-peer connection.

ZRTP enables two parties to agree on key parameters to start SRTP (secure real time transport protocol) session. ZRTP has three different working modes [3].

- Diffie-Hellman mode is based on DH key exchange that allows both parties to generated secret values to compute SRTP keys.
- Multi-stream mode is used when an active SRTP is in place between two parties. This allows parties to compute SRTP keys based on previous DH exchange information rather than computing new ones.
- Pre-shared mode use cached SRTP keys which were generated on earlier sessions. It does not rely on DH method but as long as the secret cache does not get compromised this mode maintains secrecy and each session termination also deletes key initiation materials.

Due to the nature of these modes, only DH mode is vulnerable to attacks as secret key is shared in this session. Following modes only rely on earlier key initiation so if this mode remains secured that ensures integrity throughout the whole session [3]. Initiation and authentication process for ZTRP is shown in figure: 1 below.

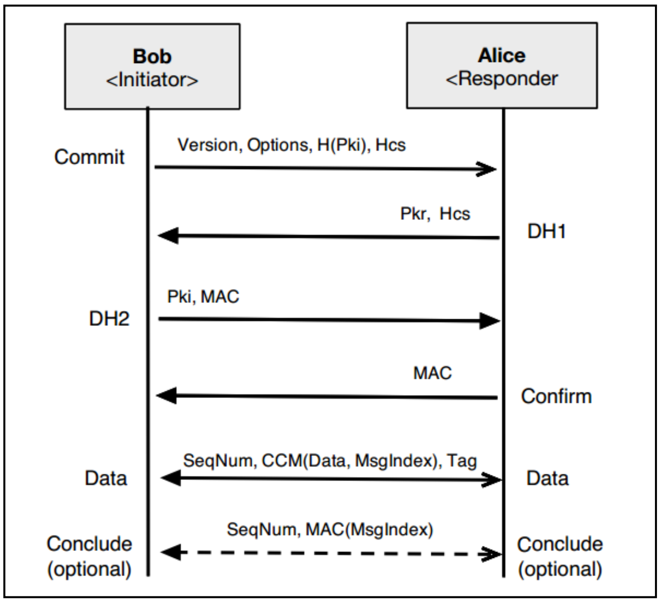


Figure 1: ZTRP authentication process [3]

To initiate the protocol initiator and responder exchange messages in 4 steps:

- Discovery – identity information and session parameters are exchanged between the agents in this stage;
- Hash commitment – procedure for key agreement is started by initiator;
- Diffie-Hellman key exchange – public keys are generated and exchanged;
- Confirmation – both the agents confirm key agreement.

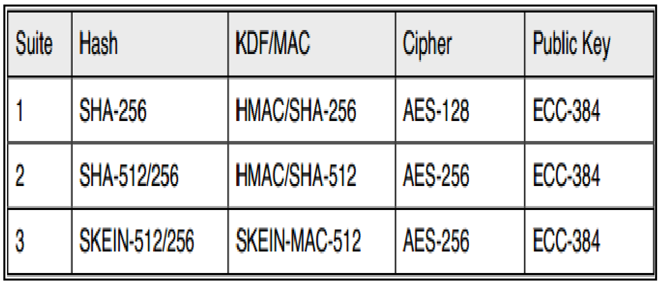
SIP initiates RTP session between two parties during ZRTP initiation at earlier stage of discovery phase. Hash commitment is made to negotiate key generation. Protocol role definition and session parameter is also negotiated same time. One of the commitments is that none of them can change their DH key pair during the process [4][5][6].

Initiator generates its key before sending hash commitment but does not reveal it which prevents responder to alter its key deliberately according to the initiator. Modular exponentiation method is used on initiator's public key to the power of responder's private key to compute DH keys. HMAC is also sent with the key to distinguish and discard non matching secrets. These keys are then concatenated with hashed messages which become new secret between both parties. Both SRTP session and SAS are derived using this secret keys and both parties exchange confirmation of key generation procedure. To continue session with same pair shared secret is cached by both clients which is used to derivate new DH keys to start new session [7].

C. SCIMP overview

SCIMP protocol is the core behind the messaging service used for ultra-private smart phones. SCIMP is drawn from ZRTP protocol and both of the latest encryption ECDH and AES have been integrated with this protocol for secured key derivation. Initiation of messaging service between two end points is performed through similar phases of ZRTP where Diffie-Hellman keys are generated through hash encryption. Secured encryption, forward secrecy and authentications are main features of SCIMP [7] [9] .

Ephemeral Elliptic Curve Diffie-Hellman (EC-DH) key arrangement is employed to derivate shared secret between initiator and responder. Shared secret based hash commitment ensures authenticity through key continuity. Being peer-to-peer, SCIMP does not need other third party to establish communication and prevents exposure of secret keys. List of keys used in SCIMP is shown in figure: 2 below.



Suite	Hash	KDF/MAC	Cipher	Public Key
1	SHA-256	HMAC/SHA-256	AES-128	ECC-384
2	SHA-512/256	HMAC/SHA-512	AES-256	ECC-384
3	SKEIN-512/256	SKEIN-MAC-512	AES-256	ECC-384

Figure 2 : SCIMP key mechanism [3]

To initiate communication, sender sends a hash commitment to the responder by generating ECDH public key and responder replies back with its public key. At this stage both parties are unaware of others public key. These messages also include cached secret hashes which are derived from previous SCIMP execution. Last phase of SCIMP initiation is that initiator sends an authentication code to responder based on a known value. Finally previous cached secret keys are refreshed by newly computed shared secret keys. After SCIMP initiation both users verify SAS (short authentication string) with each other to eliminate risks of MITM attack [9].

Algorithm suite to use for commit message is specified by the initiator in SCIMP protocol. Responder simply ignores and discards commit message if it does not support the requested algorithm. Responder replies back with own message to specify supported algorithm to initiate session if needed.

IV. EXISTING SMARTPHONE PLATFORMS

Different security measures have been adopted by major smart-phone providers: IOS, Android and Blackberry. Not being an open platform, IOS faces less security threats comparing android and blackberry. SBC (secure boot chain) components are verified and cryptographically signed by Apple [10]. Code signing verifies integrity and prevents unauthorized code execution. It also allows only authorized users to access the system. AES 256 crypto engine along with SHA-1 algorithm are integrated for encrypted IOS communications. File data is also protected between user pass code and data encryption which prevents to access data when phone is not being used. IOS core supports transport layer security (TLS) protocols along with IPSec and SSL security features [11].

Linux based android is highly relying on UNIX security mechanisms. Being an open source platform it attracts more threats and risks comparing apple and blackberry systems. Application container in android isolates system data from outside application or data pair to prevent any leakage. On device data encryption uses passphrase and HMAC along with one way hash value named salt. This process is simultaneously repeated to derive the final cryptographic key. This encryption mechanism also covers external SD cards. VPN and VOIP based calls are also supported through IPSec protocol and AES-256 along with DH key generation protocol. PKI along with X.509 certificate ensures android's kernel and boot lever security [12].

Main feature of blackberry security mechanism is transport layer security (TLS) encryption. Later editions of BES-10 feature three main aspects of security: confidentiality through encryption, integrity through hashing and authenticity through device transport key. Due to having more support from desktop platform, windows phones get full advantage from cloud based service. SSL encryption is used along with AES-256 or AES-128 to protect communication sessions.

All these methods commonly provide supports for device and data encryption along with call or message encryption over the network. Only blackberry provides supports for end-to-end communications. This does not only cover infrastructure security but also provides security throughout the whole communication path [11].

V. ADVANTAGES OF ULTRAPRIVATE TECHNOLOGY

- End-to-end encryption technology throughout the whole communication medium and no keys are even shared with the service provider.
- Simultaneous key generation prevents attackers to intercept as new keys are generated throughout the phases.
- Provides stronger permission system for apps, anonymous browsing and trusted wifi communication.

VI. SECURITY FEATURES OF ULTRAPRIVATE TECHNOLOGY

As GSM carriers are in immense pressure from different government organisations to revel more customer information about their cell phone usages, privacy is being considered even more vulnerable in times. That adds up with infrustructure vulnerability of traditional PSTN based GSM architecture. Packets are captured and decoded by sniffer while passing over airwave. Even 3G and 4G subscribers are also being targetted for sniffing attacts as evesdropping softwares are higly available. As the number of user grow for internet based VOIP calls and VPN connections due to their mobility and cost effectiveness as whole internet as an infrustructure is widely under threat for different attacks. Even SSL and PKI are also vulnerable to different attacks which earlier were proven to be the latest security solutions [16].

Further researches showed that lack of integrity and continuity allowed attackers for session hijacking which resulted in compromising security of sessions [14]. Connecting to insecured wifi or access point also make the system vulnerable to different attacks as systems tend to contact with access points or wifi hotspots when coming in their range. Not all of the public hotspots or wifi access points are not secured for sure.

Ultraprivate phones technology provides best possible solutions so far available for theses vulnerabilites. Most of the GSM based carries and mobiles solutions only rely on PKI based encryption which rather than blackberry which focuses on end-to-end encryption. Yet that does not provide ultimate secrecy for blackberry as their encryption is server based and secret keys are shared with the carrier servers.

Rather blackphone ZRTP and SCIMP provides encryption solution which is truly end points encryption and even none of the keys are shared with the carrier servers. that makes this technology less vulnerable so far[15][19].

MIM attackt is the worse of these kinds for cellular or VOIP calls and messaging services. Both of these protocols are designed to prevent any evesdropping by implementing simultaneous key generation to prevent MIM attacks[3].

To provide ultimate secrecy ultraprivate technology does not allow systems to interact with unknown public access points or wifi hotspots. So no interaction happens when phones move around in different access point areas and also keeps tract of the known and saved access points defined by the users. Only when phone is within the range of those specified access points they start interacting with that networks [13].

This technology also prevnts applications to collect any user data from the system unless predefined by the user. Most of the commercial applications perform location tracking and collect phonebook listing data straight form the phone which is not allowed in silent phone networks like blackphone, boeing or zphones. This restrictions are defined at operating system level as PrivateOS of silentphone network performs the job for blackphones.

Some of the phones also use technology to auto delete shared data or information after certain time to erase records for evesdropping which also include anonymous browsing that leaves no personal records.

VII. MOBILE SECURITY IN REAL WORLD

Black phones come with secure OS and privacy enables applications. In contrast Boeing Black has hard disk encryption feature which protects data stored in the phone and hardware itself. Unlike Blackphone and Boeing black Snowden phone provides same encryption employed by building societies and government agencies with added protection against malware threats. Unlike Black Phone and Snowden phone Boeing Black comes with self-destructive features. If someone tries to open its case it deletes all data it was holding that makes it even safer then Blackphone and Snowden Phone.

Ultra private Smartphones are of course much secured compared to IOS and other Android phones as it protects us from being spied and tracked. But what about the packets that is to be sent beyond Silent Circle Network (SCN)?? When encrypted packets (for example Black Phone) are outside the range of SCN they are vulnerable again. As soon as they are out from the SCN zone they might come across other servers which hold key unlike servers with in SCN which can be compromised if security measures implemented in the server is inadequate. In this case though data is encrypted it remains vulnerable from being tempered or stolen.

Why can’t our network provider offer us something as secured as Silent Circle Network?? Vodafone is among the world biggest telecom company!! If it is too costly for Vodafone Why can’t OFCOM work together with all four main providers (EE, O2, Vodafone and 3G) to develop a shared secured network platform which will obviously be cheaper when the cost is shared! All network providers including network regulatory body OFCOM is up to higher speed spectrum not for secure connection!!

What if we have Ultra smart phone with combined capability of all three phones mentioned above?? That would be awesome. Even NSA and GCHQ would struggle breaking in to this phone. But there are always bad sides of every good thing. For example if this wonder phones goes to wrong hand for example terrorists organizations then life's around the world would be at risk as governments agencies who are supposed to protect us would struggle to their job which might result loss of life and properties.

VIII. CONCERNS AND FUTURE SCOPE

In communication mediums none of the solutions are considered full proof of attacks yet ultraprivate smartphone technology is considered being the best solution avalilable so far. As being a new trend there are only features available through this technology and further researches are going on to meet the demands of fullfilling ultimate security.

Mobile phones specially smartphones now has vast area of usages through available internet services and applications along with features calls and text messages. So far this technology is more focused to provide secured solution only for end users call and text services. Cross platform integration on different phone networks and companies are yet to be features through this technology as to use full encrypted features both the users should have similar blackphones or any of those kinds such as: zphone or boeing from same network [17][20].

Some of the encryption features are available through applications but few control feature is available when data travels through different company servers. yet again different states follow different security policy which restricts features of certain encryption protocols that results in as having less security features in certain places.

Another concern about this technology remains with the level of application usages over the smartphones as mos tof the commercial apps collects user data straight through the phones [18]. Although certain feature of ultraprivate smartphones restrict apps to collect user data but most of the apps forces user to use their services only if they accept certain terms to share their secrets such as: phone list or GPS.

Future researches can improve loopholes wilth application permissions and cross platform integrations to provide users better secured communication.

IX. CONCLUSION

Smartphone technology as a medium of phone and data communication has seen a vast increase in recent past and the graph is rising fast. As these numbers are increasing, it also poses immense security threats for the users voice and data communicaiton. This paper focus more on the security features implied in recent ultraprivate smartphone technology enabled phones like blackphone, zphone and boeing. Physical infrustructure of the backbone network are discussed along with the protocols used for voice and data communications. Then comparative overview with other smartphone platforms are also presented. Security issues of this network and existing networks have been presented along with possible solutions to overcome them.

Few more ideas been presented that can be implied for further research to strengthened this technology further and implement it on cross platform networks. Further enchancement can make ultraprivate smartphone technology to provide ultimate privacy and security for users over mobile data communication platforms.

REFERENCES

[1] Silentcircle (2014). Silent Network | Silent Circle. [online] Available at: https://silentcircle.com/silent-network [Accessed 4 Dec. 2014

[2]Boeing.com. 'Boeing: Boeing Black Smartphone'. N.p., (2015). [online] Available at: https://www.boeing.com [Accessed 23 Jan. 2015

[3] R. Bresciani and A. Butterfield, "A formal security proof for the ZRTP protocol," in *Internet Technology and Secured Transactions, 2009. ICITST 2009. International Conference for,* 2009, pp. 1-6.

[4] O. Jung, M. Petraschek, T. Hoeher and I. Gojmerac, "Using SIP identity to prevent man-in-the-middle attacks on ZRTP," in *Wireless Days, 2008. WD '08. 1st IFIP,* 2008, pp. 1-5.

[5] E. Kokkonen and M. Matuszewski, "Peer-to-peer security for mobile real-time communications with ZRTP," in *Consumer Communications and Networking Conference, 2008. CCNC 2008. 5th IEEE,* 2008, pp. 1252-1252.

[6] M. Petraschek, T. Hoeher, O. Jung, H. Hlavacs and W. N. Gansterer "Security and Usability Aspects of Man-in-the-Middle Attacks on ZRTP" *Journal of Universal Computer Science, vol. 14, no. 5, pp. 673-692, 2008*

[7] A. Singh and R. Rishi, "A novel approach towards mutual authentication and key exchange protocol based on elliptic curve," in *Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on,* 2012, pp. 404-408.

[9] A. Kaminsky, M. Kurdziel and S. Radziszowski, "An overview of cryptanalysis research for the advanced encryption standard," in *Military Communications Conference, 2010 - Milcom 2010,* 2010, pp. 1310-1316.

[10] S. Adibi, "Comparative mobile platforms security solutions," in *Electrical and Computer Engineering (CCECE), 2014 IEEE 27th Canadian Conference on,* 2014, pp. 1-6.

[11] G. Delac, M. Silic and J. Krolo, "Emerging security threats for mobile platforms," in *MIPRO, 2011 Proceedings of the 34th International Convention,* 2011, pp. 1468-1473.

[12] A. D. Keromytis, "A Comprehensive Survey of Voice over IP Security Research," *Communications Surveys & Tutorials, IEEE,* vol. 14, pp. 514-537, 2012.

[13] WEIR-JONES, T. (2014). *Blackphone: Privacy People WANT To Buy | Blackphone Blog*. [online] Blog.blackphone.ch. Available at: https://blog.blackphone.ch/2014/07/15/blackphone-privacy-people-want-to-buy/#more-46 [Accessed 16 Dec. 2014].

[14] Wanqing You, Longteng Xu and Jingyu Rao, "A comparison of TCP and SSL for mobile security," in *Sensor Network Security Technology and Privacy Communication System (SNS & PCS), 2013 International Conference on,* 2013, pp. 206-209.

[15] Yong Wang, K. Streff and S. Raman, "Smartphone Security Challenges," *Computer,* vol. 45, pp. 52-58, 2012.

[16] C. Miller, "Mobile Attacks and Defense," *Security & Privacy, IEEE,* vol. 9, pp. 68-70, 2011.

[16] Sarkar, P. and Fitzgerald, S. (2013). *ATTACKS ON SSL A COMPREHENSIVE STUDY OF BEAST, CRIME, TIME, BREACH, LUCKY 13 & RC4 BIASES*. [whitepaper][online] isecpartners. Available at: https://www.isecpartners.com/media/106031/ssl_attacks_survey.pdf [Accessed 20 Dec. 2014].

[17] P. Gupta and V. Shmatikov, "Security analysis of voice-over-IP protocols," in *Computer Security Foundations Symposium, 2007. CSF '07. 20th IEEE,* 2007, pp. 49-63.

[18] Y. Gilad, A. Herzberg and A. Trachtenberg, "Securing Smartphones: A µTCB Approach," *Pervasive Computing, IEEE,* vol. 13, pp. 72-79, 2014.

[19] V. K. Gurbani and V. Kolesnikov, "A Survey and Analysis of Media Keying Techniques in the Session Initiation Protocol (SIP)," *Communications Surveys & Tutorials, IEEE,* vol. 13, pp. 183-198, 2011.

[20] D. Jaramillo, V. Ugave, R. Smart and S. Pasricha, "Secure cross-platform hybrid mobile enterprise voice agent," in *Southeastcon 2014, Ieee,* 2014, pp. 1-6.