UDC 004.621.3

V. Savchenko, S. Dovbeshko, O. Matsko

COMMERCIAL ENCRYPTION PROTOCOLS FOR MILITARY APPLICATIONS

This article attempts to explore commercial encryption protocols for data transmitting within military applications. Nowadays the military means of secure communication and data transmitting cannot cover all informational requirements for combat applications because of organizational and physical security issues. At the same time the problem of secure communication on the front line grows day by day. The common idea of secure commercial-of-the-shelf protocols (PPTP, IPSec, SSL, TLS, SSH, HTTPS, PGP, DNSSEC, SMIME) usage within military domains is not new but for this moment it doesn't have any real detailed description because of vulnerabilities of these protocols. The original idea highlighted in this paper is in double-layered point-to-point commercial encryption system based on the most reliable open-source protocols in Virtual Private Networks (VPN) architecture.

Keywords Commercial-of-the-Shelf; Encryption; Virtual Private Network

Introduction

Today the information flow on the battlefield grows day by day and the problem of information assurance began global. The previous generations of military cryptography utilized secret algorithms and standalone encryption hardware. But now this approach became too expensive due to necessity of constant developing new hardware and software as well as numerous organizational issues.

Nowadays the US National Security Agency (NSA) seriously considers "Layered COTS (commercial-of-the-shelf)" approach that layers different security commercial products in a "good-enough" approach [1]. Despite of mentioned idea there is no real concept for its implementation. For many military applications with short-term information life this approach based on unclassified cryptoalgorithms could be very effective as it doesn't need personnel with security clearances and expensive facilities. So, the goal of this paper is to explore which secure protocols are better for "Layered COTS cryptography" and to suggest the prospective model of secure set for tactical units on the battlefield.

1. Knowledge Overview

The new generation of cipher algorithms theoretically can protect information from direct decoding taking work of supercomputers for billion of billions years. At the same time news about cracked algorithms appears regularly. Sometimes this news is simply a fake directed to maintain hacker's ego but from other side it drives us to think about vulnerabilities of encrypted communication.

The main types of cyber attacks in military domains are: unauthorized access and theft of proprietary information. Usage of proprietary hardware for "Type 1" security on the front line of battle is very problematic. At the same time the length of information life on tactical level can be limited by few hours that allow using not so complicated tools for encryption. Taking into account all financial issues "Layered COTS cryptography" promises to be a good solution. Created for commercial purposes some secure protocols (see Figure 1) can be used for military applications.

This is not the first time of civil approach usage in military domains: well-known German Enigma initially was born as commercial project. Obviously, all of these COTS protocols have their own limitations so the perfect security network should consist of the most reliable tools.

2. Limitations

Limitations of highlighted protocols for military applications are closely connected with their vulnerabilities discovered by hackers and sometimes ordinary users as a result of massive

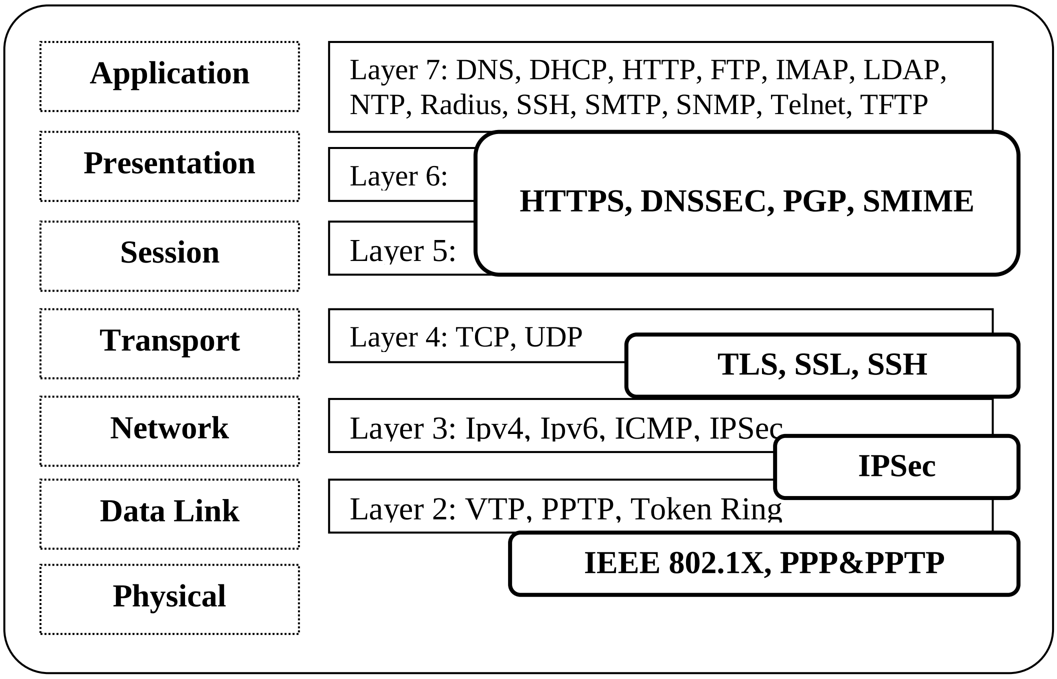
Application
Presentation
Session
Transport
Network
Data Link
Physical
Layer 7: DNS, DHCP, HTTP, FTP, IMAP, LDAP, NTP, Radius, SSH, SMTP, SNMP, Telnet, TFTP
Layer 6:
Layer 5:
HTTPS, DNSSEC, PGP, SMIME
Layer 4: TCP, UDP
TLS, SSL, SSH
Layer 3: Ipv4, Ipv6, ICMP, IPSec
IPSec
Layer 2: VTP, PPTP, Token Ring
IEEE 802.1X, PPP&PPTP

Fig. 1. Security on different layers [2]

usage of “secure” networks. Let’s consider them from the point of view of data confidentiality, integrity and authentication.

2.1. PPTP

PPTP (Point-to-Point Tunneling Protocol) is a data-link protocol for building VPN using a control channel over TCP tunnel. PPTP supports authentication, encryption, and packet filtering by incorporating PPP-based protocols like EAP, CHAP, and PAP [3]. Vulnerabilities of PPTP: unsecured CHAP-1 and CHAP-2 encryption; RC4 stream cipher doesn’t have authentication of the ciphertext stream and therefore the ciphertext is vulnerable to a *Bit-Flipping Attack* [4].

2.2. IPSec

IPSec (Internet Protocol Security) was invented for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet on the basement of mutual authentication between agents and negotiation of cryptographic keys. The main IPSec cryptographic algorithms: HMAC-SHA-1 – for integrity protection and authenticity; DES, 3DES-CBC, AES-CBC – for confidentiality; AES-GCM – for confidentiality and authentication together. The article from ‘The Austaralian’ shows that IPSec is vulnerable to *Cut-And-Past Attack*. This attack can happen on two networks that use IPSec as a tunnel between the two routers that link the networks when the attacker has access to a second machine in each of the two networks. Beside of this, the DES encryption used in IPSec is now susceptible to *Brute-Force* attacks (decryption by simply trying every possible key value) [5].

2.3. SSH

SSH (Secure Shell) is a cryptographic protocol that establishes a secure channel over an insecure network in client-server architecture. Encryption – AES, 3DES, Blowfish, Twofish, IDEA; public-key cryptography – DSS, RSA, ECDH; hash algorithm – MD5, SHA-1. Edward Snowden files indicate that the NSA can decrypt SSH. Beside of this, SSH authentication represents encrypted traffic that is not typically visible to network monitoring technologies as well as SSH keys never expire that could create back doors and make it easy for adversaries to steal information [2].

2.4. TLS

TLS (Transport Layer Security) and its predecessor, SSL (Secure Sockets Layer), are cryptographic protocols designed to provide communications security over a computer network. For the latest versions TLS-1.2, SSL-3: encryption – AES-256, DES, 3DES, ARCFOUR, Camellia, RC2, IDEA, SEED; public-key cryptography – ECDH; hash algorithm – MD5, SHA-1, SHA-2. Possible attacks against TLS/SSL: FREAK, Renegotiation, Version rollback, BEAST, CRIME and BREACH, Timing attacks on padding, POODLE, BERserk, RC4, Truncation, Heartbleed Bug. Comparing with TLS 1.0 the SSL 3.0 cipher suites have a weaker key derivation process: half of the master key that is established is fully dependent on the MD5 hash function, which is not resistant to collisions. Also, in October 2014, the vulnerability in the design of SSL 3.0 to the padding attack (POODLE) was discovered. In the result of the attack SSL 3.0 allows traffic over an encrypted connection to be intercepted [6].

2.5. HTTPS

HTTPS (“HTTP over TLS”, “HTTP over SSL”) is a set of communication protocols with especially wide deployment on the Internet to prevent wiretapping and MIM attacks. HTTPS utilizes the encryption of TLS/SSL algorithms. The level of HTTPS protection depends on the user’s skills of web browser operating, the server software and the supported cryptographic protocol. SSL in HTTPS does not prevent the site from indexing by a web crawler, and in some cases knowing only the intercepted request size the URI of the encrypted resource can be inferred. This allows an attacker to have access to the plaintext and to the encrypted text simultaneously making a cryptographic attack easier. The *Man-in-the-Middle* (MIM) type of attack can defeat the HTTPS security by enforcing users into thinking that they are using HTTPS when in fact they are using HTTP. Also it was discovered that some sensitive user data can be inferred from side channels.

2.6. PGP

PGP (Pretty Good Privacy) provides cryptographic privacy and authentication for data communication: signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions. Encryption – AES-128, AES-192, AES-256 (default), Camellia, Blowfish, CAST5, DES, IDEA, Triple DES (DESede), Twofish; public-key cryptography – ECDSA, ECDH; hash algorithm – MD2, MD5, RIPEMD-160, SHA1 (default), SHA-256, SHA-384, SHA-512. Actually, there is no known method which allows breaking PGP encryption. Possible theoretical vulnerabilities apply not just to PGP but to any other conventional encryption software. *Buffer Overflow in Outlook Plug-In* does not compromise any PGP user who does not use Outlook and unless hostile code compromises the victim's private key. *Chosen-Ciphertext Vulnerability* can be caused by weak human procedures and it does not compromise secure encryption. At the worst, only the contents of a single message can be revealed. *Unsigned Data-Injection Vulnerability* can compromise the ability to use digital signatures to verify the integrity of files and E-mail [7].

2.7. DNSSEC

DNSSEC (Domain Name System Security Extensions) is a suite of specifications for securing of information provided by the DNS: origin authentication of DNS data, authenticated denial of existence, and data integrity, but not availability or confidentiality. Encryption – ECDSAP256/SHA-256, ECDSAP384/SHA-384, RSA/SHA-1, RSA/SHA-1 (NSEC3), RSA/SHA-256, RSA/SHA-512; Key length – 256, 384, 1024-4096. For the verifying clients it is important that data from secured zones can be used to build *chains of trust* regardless of whether the data came directly from an authoritative server or a caching name server [8].

2.8. S/MIME

S/MIME (Secure/Multipurpose Internet Mail Extensions) is a standard for public key encryption and signing of MIME data. Encryption – AES-128, AES-192, AES-256, DES, Triple DES, RC2; public-key cryptography – DH; hash algorithm – RSA/MD5, RSA/SHA-1.

S/MIME is created for End-to-End security and it doesn’t imply to have a third party inspecting email for malware. Encryption will not only encrypt the messages, but also the malware. Thus, if mail is scanned for malware anywhere but at the end points, such as a company's gateway, encryption will defeat the detector and successfully deliver the malware.

3. Innovated Solutions

The analysis made in the previous section allows us to draw the necessary steps that should be made for “Layered COTS encryption” in military domains. First, it should be admitted that “Layered COTS encryption” as it uses widely-known algorithms CANNOT BE USED for classified “Type 1” information that needs “Suite A” cryptography (secret algorithms and secret hardware). In this project “Suite B” cryptography based on publicly-known algorithms is intended only for unclassified military domains where restriction requirements are not so strong but importance of information is still so high. The NSA’s idea of “Layered COTS encryption” has to be detailed taking into account considered limitations. Today there is no ideal universal cryptographic solution for military applications. So, the perfect solution is in complex utilization of existent COTS protocols and suggested steps should be considered as additional measures to standard set of information security in technical and organizational areas.

3.1. Technical Issues

The experience gained from the NSA-NIST issues [4] says that the source code for encryption software has to be free for public inspection to prevent backdoor existence. In this case protocols that use OpenXXX software are preferable. Many of considered protocols don’t have their open source version so utilization of such protocols is unreliable.

Taking into account considered vulnerabilities, technical parameters, existence of open source software the most optimal for military applications can be double-layered architecture of “Layered COTS encryption” based on OpenVPN and OpenPGP software with appropriate set of cipher algorithms (see Figure 2). In this case OpenSSL 1.0.2 includes TLS 1.2 encryption. OpenVPN should utilize not less than 128-bit encryption based on OpenSSL (TLS) protocols, allow agents to authenticate each other using shared secret key or certificate, support End-to-End communication (see Figure 3) and utilize other control features. The AES and Camellia are the most preferable symmetric ciphers for OpenVPN when RSA-2048 should be used for cipher’s keys encryption and SHA-256 and higher hash for authentication.

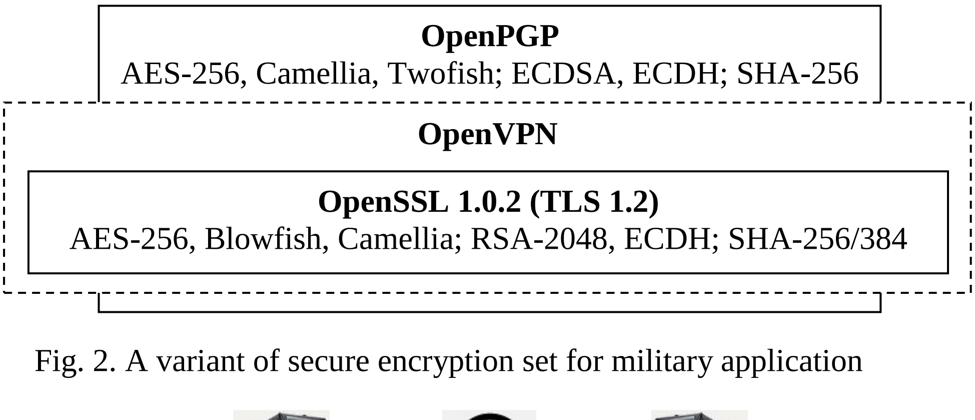
OpenPGP
AES-256, Camellia, Twofish; ECDSA, ECDH; SHA-256
OpenVPN
OpenSSL 1.0.2 (TLS 1.2)
AES-256, Blowfish, Camellia; RSA-2048, ECDH; SHA-256/384

Fig. 2. A variant of secure encryption set for military application

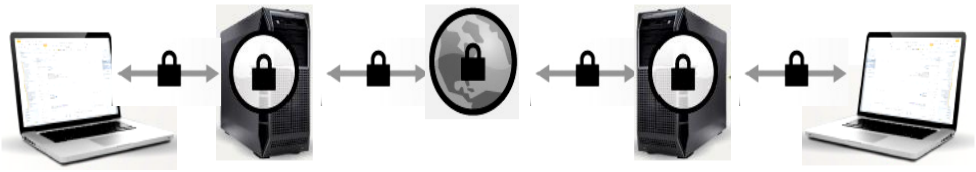

Fig. 3. End-to-end encryption on OpenPGP/OpenVPN

Key management is one of the biggest technical problems for tactical local networks. Avoiding the discussion about NIST-certified standards and NSA involvements [4] the question of key algorithm choice is the preference of system administrator. Actually reliable project of secure military local network has to avoid usage of dead and going to die encrypting algorithms: MD5 [9], RSA1024 [10], SHA-1 etc. [11]. The key size – not less than 128-bit (preferably 256 bit) for symmetric cryptography and not less than 2048 for RSA encryption. The Key validity period should be limited by few hours.

Another important issue gained from SSL/TLS consideration and connected with key infrastructure is *Forward secrecy* that should guarantee not compromised session key in the case of one of the private keys is compromised. E.g. for TLS it can be gained using Diffie-Hellman key exchange. However to implement such restrictions in military domains you have to have appropriate server infrastructure.

Building the secure tactical network you should take encryption protocols with respect to their hardware requirements. Growing key length and algorithm complexity demand more and more powerful computer infrastructure and it's enough critical for mobile tactical devices. But, using "simple" encryption algorithms (e.g. IPSec) the problem of "brute force" decryption becomes critical.

3.2. Organizational Aspects

All users and IT staff involved into a communication process are responsible for securing and protecting their networks. These measures should be reflected in appropriate policies, standards and other papers. This is absolutely critical for tactical level where user's IT security skills and cyber threats control as well as issues of physical security are quite problematic. This thesis shows the importance of training procedures for all participants of communication process.

The lesson that was learned from the study of IPSec shows the importance of user's and IT staff's understanding of their specific software. In the case of "Suite B" cryptography when requirements to the specific software are not so strong the cases of not fully compliant software with security protocols can happen. It can seriously influence the security of all communication.

Conclusion

Today modern warfare demands more and more information. Information became a new dimension and a new weapon on the battlefield. Existent military security facilities are too complicated, expensive, difficult in handling and cannot cover all informational requirements in military domains. Existent commercial cipher protocols have good algorithms but sometimes demonstrate serious vulnerabilities and are the target for numerous hackers. The NSA's idea of "Layered COTS cryptography" implies utilization of few COTS protocols overlaid on each other for vulnerabilities mitigation. For military applications this idea needs deeper consideration.

Taking into account technical parameters, limitations, existence of open source software the optimal "Layered COTS" package should consist of 2 layers: OpenPGP – for applications and OpenVPN based on OpenSSL 1.0.2 (includes TLS 1.2) – for transport layer. Advantages of such approach: allows End-to-End secure communication (email, text, data etc.); arisen time for compromise (t^2); built on open source software – no back doors; financial effectiveness – doesn't need security clearance, new hardware and software. Disadvantages: no stream encoding; key management problem (increasing number of users increase the number of keys); possible compromise of particular communication in case of end user's devise capture.

The field of future consideration should cover questions of threats modelling for "Layered COTS cryptography", key security management, physical security etc.

References

1. Keller, J. Military crypto modernization leads to applications like smartphones, tablet computers on the battlefield [on line]. Military & Aerospace Electronics**, November 28, 2011**. [cited 2016-04-16]. Available from: <http://www.militaryaerospace.com/articles/2011 /11/military-crypto-modernization.html>.

2. Ponemon 2014 SSH Security Vulnerability Report [on line]. Venafi, Inc. Ponemon Institute, 2014. [cited 2016-04-16]. Available from: <https://www.venafi.com/ assets/pdf/Ponemon_2014_SSH_Security_Vulnerability_Report.pdf./>.

3. Introduction to PPTP - Point-to-Point Tunneling Protocol [on line]. About.com, April 15, 2016. [cited 2016-04-16]. Available from: <http://compnetworking.about.com/od/vpn /l/aa030103a.htm>.

4. Crawford, D. PPTP vs L2TP vs OpenVPN vs SSTP vs IKEv2 [on line]. BestVPN, December 18, 2014. [cited 2016-04-16]. Available from: <https://www.bestvpn. com.blog/4147/pptp-vs-l2tp-vs-openvpn-vs-sstp-vs-ikev2/>/.

5. Clark, D. (March 14, 2002). Vulnerability's of IPSEC: A discussion of possible weaknesses in IPSEC implementation and protocols [on line]. SANS Institute, April 15, 2016. [cited 2016-04-16]. Available from: <http://www.sans. org/reading-room/whitepapers/vpns/vuln erabilitys-ipsec-discussion-weaknesses-ipsec-implementatio n-pro-760>.

6. Westin, K. SSL v3 "POODLE" Vulnerability Revealed (CVE-2014-3566) [on line] The State of Security, October 14, 2014. [cited 2016-04-16]. Available from: <http://www.tripwire.com/state-of-security/vulnerability-management/ssl-v3-poodle-vulnerability-revealed-cve%C2%AD-2014-%C2%AD3566/>.

7. Ross, D. E. PGP: Holes, Weaknesses, and Flaws [on line]. David Ross Page, 2010. [cited 2016-04-16]. Available from: <http://www.rossde.com/PGP/pgp_weak.html>.

8. Mitchell, C. J. Security vulnerabilities in DNS and DNSSEC [on line]. Chrismitchell.net, 2014. [cited 2016-04-16]. Available from: <http://www.chrismitchell.net/svidad.pdf>.

9. Vulnerability Note VU#836068. MD5 vulnerable to collision attacks. CERT, 2009. [cited 2016-04-16]. Available from: <www.kb.cert.org/vuls /id/836068>.

10. Cheng, J. Researchers: 307-digit key crack endangers 1024-bit RSA [on line]. ArcTechnica, May 23, 2007. [cited 2016-04-16]. Available from: <http://arstechnica. com/uncategorized/2007/05/researchers-307-digit-key-crack-endangers-1024-bit-rsa/>.

11. Walker, J. When Will We See Collisions for SHA-1? [on line] Schneijer, 2012. [cited 2016-04-16]. Available from: <https://www.schneier.com/blog/archives/2012/10/when_will_ we_se.html>.

Надійшла: 15.01.2018 Рецензент: к.т.н. Курченко О.А.