International Journal of Security and Its Applications
Vol. 9, No. 3 (2015), pp. 353-362
http://dx.doi.org/10.14257/ijsia.2015.9.3.27

On the Existence of Subliminal Channel in Instant Messaging Systems

Lingyun Xiang[1], Yuhua Xie[2], Gang Luo[3] and Weizheng Wang[1]

[1]*School of Computer and Communication Engineering, Changsha University of Science and Technology, Changsha 410114, China*
[2]*Loudi Municipal Office, SAT, Loudi 417000, China*
[3]*College of Information Science and Engineering, Hunan University, Changsha 410082, China*
xiangly210@163.com, hades9527@163.com, 18812309@qq.com

Abstract

Subliminal channel is a covert communication channel that can securely exchange secret information. By analyzing the communication protocols and encryption algorithms of two popular instant messaging systems QQ and Skype, this paper devotes the efforts to find whether they satisfy the condition of establishing subliminal channel or not. The broad-band subliminal channel can be established in Skype and QQ messages. Therefore, two subliminal channel schemes are proposed to embed and extract subliminal information. Finally, performances of the proposed subliminal channels are compared with those of the ones based on ElGamal digital signature and Newton channel. Experimental results and theoretical analysis show that they are easy to be implemented with large bandwidth and execute fast.

Keywords: *subliminal channel, covert communication, instant messaging, Skype, QQ*

1. Introduction

Subliminal channel is a covert communication channel constructed in public channel. It hides additional message mainly in public-key cryptosystem, authentication, and digital signature schemes. The sender and the designated receiver can transmit secret information by the subliminal channel without arousing suspicion from the public or channel warden.

Since the concept of subliminal channel was first proposed by Simmons [1] in 1983, it played a significant role in covert communication. In covert communication, subliminal channel has prominent advantages. One is that the attackers cannot intuitively discover the existence of subliminal information, as the host of subliminal channel is innocent and legitimate. The other is that the attacks cannot retrieve the transmitted secret information, which is computationally infeasible even if they learned the existence of the subliminal information.

Currently, many researchers have studied on subliminal channel and designed plenty subliminal channel protocols [2-13]. Simmons not only proposed some narrow-band subliminal channels [2] but also a broad-band one [3] in DSA signature schemes. Subsequently, Anderson, *et al.*, [5] constructed a more secure broad-band subliminal channel named Newton channel in ElGamal signature scheme. Many subliminal channels were also constructed based on elliptic curves cryptosystem [6, 7], NTRU public-key cryptosystem [8], RSA-PSS signature scheme [9], Lamport's one-time signature schemes [10], and so on.

ISSN: 1738-9976 IJSIA

Subliminal channel severs as an important kind technology of information security, it can be widely applied. Chen, *et al.*, [14] took the concept of subliminal channel to propose a fair online payment system to protect the customer's ownership. Zhao, *et al.*, [15] adopted the subliminal channel to propose a variant of the reversible watermarking scheme with improved security.

Reviewed the related work, subliminal channels constructed in signature schemes are the main trend, which embedded secret information into signatures, whereas, they had the disadvantages of low transmission efficiency, limited subliminal capacity, and no real time. Moreover, frequently transmitted signatures are easily suspected. To overcome these shortcomings, instead of generating a new signature, a subliminal channel is suggested to be established in an existing natural legitimate host like instant messages. On the other hand, with the population of instant messaging (IM), and gradually development from the individual applications extended to enterprise application and commercial applications in today, the messages of IM have become the ideal carrier of subliminal information.

IM is a type of online chat which offers real-time communication over the Internet. The main typically transmitted messages include real-time text, images, audio, video, clickable hyperlinks, etc. Due to security concerns, secure IM platforms always encrypt the contents of the messages. The use of encryption algorithms provides the possibility of establishing subliminal channel. As the existing monitoring systems can only monitor the communication of public channel, but not take effective detection on communication of subliminal channel. So it's essential to deploy in-depth research and analysis on the existence of subliminal channel in IM messages.

In this paper, the existence of subliminal channel in two popular IM systems QQ and Skype has be analyzed by studying their communication protocols and encryption algorithms. In addition, embedding and extraction algorithms of subliminal information in QQ and Skype messages have been designed. Finally, the comparison with the other typical subliminal channels based on digital signature is made from the aspects of bandwidth, embedding/extraction algorithmic efficiency and accuracy.

2. Existence Analysis on Subliminal Channel in Popular IM Systems

Most cryptographic algorithms of public-key cryptosystem have the probabilistic characteristic. One plaintext may correspond to several ciphertexts. This randomness of the cryptosystem is a necessary condition for existence of the subliminal channel. Thus, the cryptographic algorithms with randomness can serve as the host of subliminal channels, and the subliminal information can be hidden in the randomness.

For the warden in the Prisoners' problem introduced by Simmons [1], the randomness of a cryptosystem mainly includes three categories: 1) the stochastic parameters inputted from the cryptosystem, such as the session key in a probabilistic digital signature scheme. They are the main source of randomness; 2) the randomness caused by the redundancy of the representation of the plaintext. The same semantic can be expressed into several possible message symbols; 3) the semantic randomness of the sent messages, namely, the warden is uncertain to the content of the being sent messages. If the equivocation in different semantics is not 0, then the corresponding output encrypted data is randomness for the warden. As long as the encrypted data has the aforementioned randomness for the warden, the subliminal channel exists.

The cryptographic algorithms of conventional symmetric key cryptosystem are always only used for encryption. One plaintext can be only encrypted to a unique cipher text for the same key. In this case, usually no random redundant information can be utilized, so there is generally no practical subliminal channel existing in a symmetric cryptographic algorithm.

At present, there are many available IM systems (Skype, Tencent QQ, Facebook Messenger, Twitter, Ubique, *etc*.,). Most of them are non-standard systems with their own different cryptosystem and communication protocols. In addition, the developers of IM systems treat their own technologies in confidence due to their interests. Because the used protocols and cryptosystems are not unified standard and public, it makes the existence of subliminal channel has its own particularity in all kinds of IM systems. Therefore, the researches on the existence of subliminal channels in IM systems should be separately carried out for different ones. In this paper, two representative IM systems Skype and QQ have been analyzed.

2.1. Existence of subliminal channel in Skype

Skype is a freemium voice-over-IP service and instant messaging client, originally developed from Europe and currently developed by Microsoft-owned Skype technologies. Due to its good voice transmission quality and high security, it has huge amount of registered users from all over the world, 663 million at the end of 2010 [16]. In order to securely communicate, Skype uses standard cryptographic primitives including the AES, RSA, the ISO 9796-2 signature padding scheme, the SHA-1 hash function, RC4 stream cipher, and so on [17]. In conclusion, Skype reportedly uses two encryption techniques. One is RSA for key negotiation; the other is the AES to encrypt conversations. The instant messages transmitted through a session are encrypted by AES algorithm from Skype-end to Skype-end without passing through any intermediary node. The AES implemented by Skype does not completely the same with the standard AES. It is impossible to know the details of the implementation of Skype AES.

All packet data in a session in Skype are served as the plaintext and placed in a buffer. The plaintext except for the last two bytes in a Skype buffer is encrypted by the followed encryption protocol [17]:

1) Successive blocks of plaintext are XORed to AES cipher blocks with a key established for the session. The size of an input block is 128 bits. Its structure is: *salt*:*salt*:*packet_index*:*block#*, where *packet_index* is a 48-bit value, *block#* is a 16 bit value. The size of the used key is 256 bits.

2) A CRC checksum is calculated on the contents of the encrypted buffer. The mod 2 sum of the CRC with the low order 2 bytes of the *packet_index* is stored in the last 2 bytes of the buffer.

3) Note: Only the low order bits of the AES counter change from block to block while encrypting a buffer. The *packet_index* changes from buffer to buffer. The salts are contributed by each Skype client and are random values.

Although Skype uses AES, which is a symmetrical block cipher algorithm, it pads random numbers into the packet data before encryption. So there is a certain amount of random redundancy in Skype encryption protocol, this provides the condition of establishing subliminal channel in Skype messages. Set subliminal information is *U*, then the sender can replace the random number *salt* in the input block with *U*; while the receiver can extract the subliminal information by separating random number *salt* in the received input block. Therefore, the subliminal channel is successfully established in Skype messages, and its bandwidth is the total length of the used random number *salt*. According to the definition of broad-band subliminal channel[3], if a subliminal channel uses all or almost all the subliminal space in the channel, it is defined as a broad-band one, so the subliminal channel constructed in Skype messages belongs to broad-band subliminal channel.

2.2 Analysis of the existence of subliminal channel in QQ

Tencent QQ, popularly known as QQ, is an IM system service developed by Chinese company. It is the most popular IM system in China with the largest number of users. As of 20 March 2013, there are 798.2 million active QQ accounts. QQ uses 16-R Tiny Encryption Algorithm (TEA) to encrypt the text message in a session. TEA is a block cipher algorithm invented by David Wheeler and Roger Needham of Cambridge Computer Laboratory in 1994. Its security can be improved by increasing the number of its encryption rounds. Due to the length of the instant messages required to be encrypted by TEA in QQ communication is variable, a stuffing technique is used to transform the message before encryption. A message will be transformed into a plaintext named as the QQ message packet. The details of the stuffing process are described as follows:

1) Let $a = (len + 10) \bmod 8$, where len is the length of the sent instant message.

2) Let $b = a \mid 0xF8$, and then stuff b into the first byte of the plaintext.

3) Stuff the second to the $(a + 3)$-th bytes of the plaintext by random numbers.

4) Stuff the content of the transmitted QQ message into the plaintext starting from the $(a + 4)$-th byte.

5) Stuff successive $'0'$ into the end of the plain text until the length of the plain text in bytes is a multiple of 8.

Thus, the structure of the plaintext transformed from a message of QQ can be expressed as: *b#:random number #:message#:0#.*

The using of random number creates a condition for subliminal channel existing in QQ messages. The form of subliminal channel existing in QQ messages is similar to that in Skype messages, but the former has its own characteristic in aspect of the bandwidth. The amount of subliminal information in each QQ message is limited by the length of the sent message. According to the stuffing process, we can calculate the bandwidth of the corresponding subliminal channel $B = a + 2$, namely, $B = (len + 10) \bmod 8 + 2$. Therefore, it can obtain a conclusion that the maximum bandwidth is 9 bytes, while the minimum bandwidth is 2 bytes. The relationship between len and the band width is shown in Table1, where k is an arbitrary integer. As a result, in order to take full advantage of the subliminal channel bandwidth in each QQ message, the length of the sent message must be 8**k*+5 bytes. In this case, the subliminal channel bandwidth can reach the maximum. Similar to the Skype, the subliminal channel in QQ messages is broad band.

Table 1. The Relationship between the Message Length and the Subliminal Channel Bandwidth in QQ Messages

Message length(Byte)	8**k*	8**k*+1	8**k*+2	8**k*+3	8**k*+4	8**k*+5	8**k*+6	8**k*+7
Subliminal channel bandwidth(Byte)	4	5	6	7	8	9	2	3

3 Subliminal Channel Schemes in IM Systems

According to the above analysis, when the sender wants to send secret information to the receiver, he/she can embed it into the instant messages via subliminal channel. The secret information can be recovered from the received instant messages without suspicion. Thus, we design subliminal channel schemes in IM Skype and QQ messages to transmit secret information, respectively.

3.1 Subliminal Channel Scheme in IM Skype

The precondition of embedding subliminal information via Skype messages is the random number in the data structure before Skype encryption. The subliminal channel scheme includes two algorithms: subliminal information embedding algorithm and subliminal information extraction algorithm. A user of Skype uses the embedding algorithm to send instant messages with subliminal information while the other user uses the extraction algorithm to recover the subliminal information when he/she receives the messages. The two communicating users will share a key for encrypting the subliminal information. The details of the algorithm are as follows.

Algorithm 1: Embedding Algorithm of Subliminal Information in the Skype Messages

Step1: Calculate the bit length of subliminal information U and denote it as Len_u, then stuff meaningless dada into U until Len_u is divisible by 64.

Step2: Chaotic modulate and encrypt U with a shared key K in order to obtain a pseudo-randomized information U'. It should be noted that U' must have the same length with U.

Step3: Estimate the bit length of the required Skype message Len_M by $Len_M = Len_u / 4$, if the bit length of Skype message M $Len < Len_M$, then stuff meaningless data into M until $Len = Len_M$.

Step4: Divide M into 16 bits equal-size blocks, and denote the i-th block as M_i. Then divide U' into blocks, and denote its i-th block as U'_i, the number of blocks as $2N$.

Step 5: Initialize $i = 1$.

Step 6: Construct the input block by replacing the random number *salt* in the structure of Skype input block with the blocks from U'. Thus, the constructed i-th input block is: $U'_{2i-1} \# U'_{2i} \# packet\_index \# M_i$. $i = i + 1$.

Step7: Encrypt the constructed i-th input block by AES.

Step8: If $i \le N$, then go to step 6, otherwise end the algorithm.

The subliminal channel capacity of an instant message sent by a user of Skype is determined by the message length. As the message have a variable length, it may not have the enough subliminal space to carry the required secret information. We can deal with it by two methods. One is to stuff arbitrary meaningless data into the message to expand its length. The above Algorithm 1 uses it. The other is to partition the secret information into several segments, one can be just embedded into the current message and other segments will be embedded into next Skype messages.

Algorithm 2: Extraction Algorithm of Subliminal Information in the Skype Messages

Step1: For the encrypted message received from the Skype client, decrypt it by AES.

Step2: Sequentially extract the first 64 bits of each decrypted 128-bit block and denote the whole extracted information as D.

Step3: Obtain the subliminal information U by decrypting D using the shared key K.

3.2 Subliminal Channel Scheme in IM QQ

As the message of QQ will be stuffed by random number before being encrypted, the subliminal channel can be established in QQ messages. We design a subliminal channel scheme in QQ, which is similar to that in Skype.

Algorithm 3: Embedding Algorithm of Subliminal Information in the QQ Messages

Step1: Chaotic modulate and encrypt the subliminal information U with a shared key K, and then obtain a pseudo-randomized information U'.

Step2: Calculate the byte length Len_u of subliminal information U, where $1 < Len_u < 10$, and calculate the byte length Len_M of the sent QQ message M.

Step3: According to Table 1, estimate the subliminal channel bandwidth B of M.

Step4: If $B = Len_u$, then go to Step5; if $B < Len_u$, then $n = Len_u - B$; if $B > Len_u$, then $n = B - Len_u + 8$.

Step5: Stuff n spaces into the message M.

Step6: Use U' as the random number and M to construct a QQ message packet P.

Step7: Encrypt P by TEA.

Since each QQ message can be embedded 9 bytes at most, if the length of the secret information exceeds 9 bytes, it should partition the secret information into several segments and separately embeds them into several QQ messages.

Algorithm 4: Extraction Algorithm of Subliminal Information in the QQ Messages

Step1: Decrypt the message packet received from the QQ client by TEA and denote it as P.

Step2: Read the first byte of P and denote its value as b.

Step3: Calculate $a = b \,\&\, 0x07$.

Step4: Read the data D from the second to $(a+3)$-th bytes of P.

Step5: Decrypt D by TEA using the shared key K to obtain the subliminal information U.

3.3 Performance Analysis of the Two Schemes

3.3.1 Subliminal Capacity: By the structure of Skype input block and encryption algorithm, it can find that the subliminal space of Skype messages is increased with the increase of the message length. The sent message is divided into blocks for encryption by AES. Each 128-bit input block of AES contains 16-bit Skype message and 64-bit random numbers, which are used to embed the subliminal information. The ratio of subliminal information to the Skype message is 4 to 1. Thus, the Skype communication has a great subliminal space.

By the stuffing process of the QQ used before encryption, the subliminal channel in each QQ message can only send 2 to 9 bytes of subliminal information, which is determined by the length of the transmitted message in this communication. The subliminal space in a QQ message is limited. Long subliminal information should be segmented and be embedded into several QQ messages.

In conclusion, the embedding capacity of the subliminal channel in the IM can be enlarged by using more instant messages.

3.3.2 Security: The security of the proposed subliminal channel schemes in IM systems can be guaranteed by the following three aspects: 1) The cracker is difficult to discover the existence of subliminal channel. The subliminal information is embedded into the sent instant message in the form of pseudo legitimate data. And it will be recovered before the receiver reads the content of the instant message. 2) The subliminal information is chaotic modulated and encrypted, and the sent message with subliminal information is also be encrypted by encryption algorithm used in the IM systems, even if the IM communicates are suspected, it also cannot detect and recover the subliminal information.

3.3.3 Algorithmic Efficiency: The proposed schemes do not need to apply hash function and asymmetric encryption to the original data, and just directly encrypt secret information by symmetric encryption algorithm. Secret information with arbitrary length can be segmented to be embedded into instant messages. Thus, compared with the previous subliminal channel schemes based on digital signature algorithms, the proposed schemes cost fewer times and have a faster embedding speed to embed the same secret information.

4 Experimental Results

The subliminal channels in ElGamal digital signature schemes are broadband and the sender and receiver share a private key. The proposed subliminal channels in Skype and QQ messages belong to the same type of subliminal channel with the ones in ElGamal. Newton channel is also broadband, but the sender and receiver do not share a private key, a receiver can just calculate a part of the private key. At the same time, it can exploit only half of signed data to embed information. Its bandwidth is slightly smaller than that of the traditional broadband subliminal channel.

We selected 10,000 random signature messages to embed subliminal information by using the subliminal channel in ElGamal digital signature scheme and in Newton channel[6]. And the experiments are also conducted on embedding subliminal information into QQ and Skype messages.

As examples, in the ELGamal digital signature scheme:

p =484833108136228085019848239601957346917539540509194627350641 79,

g =2,

x =5465481547,

k is a random number with $\gcd(k, p-1)=1$.

In the Newton channel:

p =13843541123123578945416797441689765143158 03,

x =321343208,

g =12623364660675296992132821722784595940322 0

q =10007.

The experimental results are list in Table 2.

Shown by the Table 2, the subliminal channels in QQ and Skype messages have a great advantage in the extraction speed and bandwidth. In addition, the subliminal capacity can be enlarged with the amount of the used instant messages increasing. Especially, they are simple to be realized. Therefore, they have important values in generalization and application.

Table 2. The Performance Comparison of the Different Subliminal Channels

	Skype	QQ	ElGamal	Newton
Embedding speed	High	High	High, when k satisfies the constraint condition.	High
Extraction speed	1.6KB/ms. (It shares all keys, and just decrypts using AES.)	1.5KB/ms . (It shares all keys, and just decrypts using TEA.)	0.452bit/ms. (It shares all keys, and needs to solve the equation for extraction when 382265781< k<382275781)	0.197bit/ms. (It needs to solve the discrete logarithm problem.)
Embedding	100%	100%	32.5%, when k satisfies	100%, when $p-1$

accuracy			the constraint condition.	is B smooth.
Extraction accuracy	100%	100%	100%	100%
Maximal bandwidth	4 times of the length of the sent instant message	9 bytes	$\log(p-1)$ bits	$\log q$ bits

5 Conclusions

In this paper, the subliminal channel schemes in Skype and QQ are proposed, as the existence of the random number in the data packet generated from Skype and QQ communications. Combined with IM technology, the subliminal channel has some new characteristics: simple to use, good imperceptibility, high efficiency and large bandwidth. Secret information can be securely transmitted with the Skype and QQ messages. Unfortunately, the subliminal channel can also be used by the terrorists or illegal groups for exchanging illegal information. Therefore, the future work should focus towards detecting the presence of unlawful information in the subliminal channel established in the IM messages.

ACKNOWLEDGEMENTS

This project is supported by National Natural Science Foundation of China (Nos. 61202439, 61103215, 61303042), the Scientific Research Fund of Hunan Provincial Education Department (Grant no. 12C0011), Science and technology project of Hunan Province (2012GK4006), and Scientific research projects in Colleges and universities of Hunan Province in 2012 (12C0560).

References

[1] G. J. Simmons, "The Prisoner's Problem and the Subliminal Channel", Proceedings of CRYPTO '84, **(1984)**, August 19-22, California, America.
[2] G. J. Simmons, "The Subliminal Channels of the US Digital Signature Algorithm (DSA)", Proceedings of the 3rd Symposium on: State and Progress of Research in Cryptography, **(1993)** February 15-16, Roma, Italy.
[3] G. J. Simmons, "Subliminal Communication Is Easy Using the DSA. Advances in Cryptology - EUROCRYPT '93", LNCS, vol. 765, **(1994)**, pp. 218-232.
[4] G. J. Simmons, "Subliminal Channels: Past and Present", European Transactions on Telecommunications, vol. 5, no. 4, **(1994)**, pp. 459-474.
[5] G. J. Simmons, "The history of subliminal channels", IEEE Journal on Selected Area in Communication, vol. 16, no. 4, **(1998)**, pp. 452-462.
[6] R. Anderson, S. Vandeney, B. Preneel and K. Nyberg, "The Newton Channel. Third International Workshop on Information Hiding (IH'99)", **(1999)** September 29 - October 1, Dresden, Germany.
[7] X. Zhou, X. Yang, P. Wei and Y. Hu, "An Anonymous Threshold Subliminal Channel Scheme Based on Elliptic Curves Cryptosystem", The 7th International Conference on Computer-Aided Industrial Design and Conceptual Design, **(2006)** November 7-9, Hangzhou, China.
[8] Y. Xie, X. Sun, L. Xiang and G. Luo, "A Security Threshold Subliminal Channel Based on Elliptic Curve Cryptosystem", International Conference on Intelligent Information Hiding and Multimedia Signal, **(2008)** August 15-17, Harbin, China.
[9] Q. Cai and Y. Zhang, "Subliminal Channels in the NTRU and the Subliminal-free Methods", Wuhan University Journal of Natural Sciences, vol. 11, no. 6, **(2006)**, pp. 1541-1544.
[10] J. M. Bohli and R. Steinwandt, "On Subliminal Channels in Deterministic Signature Schemes", The 7th International Conference on Information Security and Cryptology (ICISC 2004), **(2004)** December 2-3, Seoul, Korea.
[11] D. R. Lin, C. Wang, Z. K. Zhang and D. J. Guan, "A Digital Signature with Multiple Subliminal Channels and Its Applications", Computers & Mathematics with Applications, vol. 60, no. 2, **(2010)**, pp. 276-284.
[12] K. Kim, F. Zhang and B. Lee, "Exploring Signature Schemes with Subliminal Channel", The 2003 symposium on cryptography and information security, **(2003)** January 26-29, Hamamastu, Japan.
[13] C. L. Yang and C. M. Li, "Subliminal Channels in the Identity-based Threshold Ring Signature", International Journal of Computer Mathematics, vol. 86, no. 5, **(2009)**, pp. 753-770.

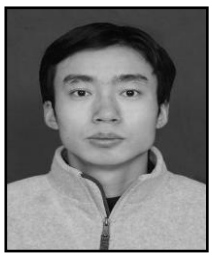
[14] X. J. Xin and Q. B. Li, "Construction of Subliminal Channel in Id-based Signatures", 2009 WASE International Conference on Information Engineering(ICIE 2009), **(2009)** July 10-11, Shanxi, China.
[15] C. L. Chen and J. J. Liao, "A Fair Online Payment System for Digital Content via Subliminal Channel", Electronic Commerce Research and Applications, vol. 10, no. 3, **(2011)**, pp. 279-287.
[16] "Skype", **(2014)**, http://en.wikipedia.org/wiki/Skype#cite_note-19.
[17] T. Berson, "Anagram Laboratories", Skype Security Evaluation, **(2005)**, http://www.skype.com/security/files/2005-031%20security%20evaluation.pdf.

Authors

Lingyun Xiang, she received her B.E. degree in computer science and technology, in 2005, and the Ph. D. degree in computer application, in 2011, Hunan University, Hunan, China. Currently, she is a Lecturer in College of Computer and Communication Engineering, Changsha University of Science & Technology, Hunan, China. Her research interests include network and information security, steganography, steganalysis, machine learning.

Yuhua Xie, he received his B.E. degree in computer science and technology, in 2005, and the M.E. degree in computer science and technology in 2009, Hunan University, Hunan, China. Currently, he is a civil servant working for the Loudi Municipal Office, SAT, Loudi, China. His research interests include network and information security.

Gang Luo, he received his B.E. degree in microelectronics technology, in 1998, the M.E. degree in software engineering, in 2004, and the Ph. D. degree in computer application, in 2008, Hunan University, Hunan, China. Currently, he is an associate professor in College of Information Science and Engineering, Hunan University, Hunan, China. His research interests include information security, steganalysis, information hiding, and cryptanalysis.+



Weizheng Wang, he received his B.S. degree in applied mathematics, in 2005, and the Ph. D. degree in computer application, in 2011, Hunan University, Hunan, China. Currently, he is a Lecturer in College of Computer & Communication Engineering, Changsha University of Science and Technology. His research interests include built-in self-test, design for testability, low-power testing, and test generation.