Proceedings of the 13th Australasian conference on Information Security and Privacy

Table of Contents

attacks such as phishing as it turned out that average Internet users are unable to authenticate servers based on their certificates.

In this paper we address security of cookie-based authenticationusing the concept of strong locked same originpolicy for browsers introduced at ACM CCS'07. We describe a cookie-based authentication protocol between human users and TLS-servers and prove its security in the extended formal model for browser-based mutual authenticationintroduced at ACM ASIACCS'08. It turns out that the small modification of the browser's security policy is sufficient to achieve provably secure cookie-based authentication protocols considering the ability of users to recognize images, video, or audio sequences.

expand

Secure Biometric Authentication with Improved Accuracy

Manuel Barbosa, Thierry Brouard, Stéphane Cauchie, Simão Melo Sousa

Pages: 21 - 36

doi>10.1007/978-3-540-70500-0_3

We propose a new hybrid protocol for cryptographically secure biometric authentication. The main advantages of the proposed protocol over previous solutions can be summarised as follows: (1) potential for much better accuracy using different types of ...

We propose a new hybrid protocol for cryptographically secure biometric authentication. The main advantages of the proposed protocol over previous solutions can be summarised as follows: (1) potential for much better accuracy using different types of biometric signals, including behavioural ones; and (2) improved user privacy, since user identities are not transmitted at any point in the protocol execution. The new protocol takes advantage of state-of-the-art identification classifiers, which provide not only better accuracy, but also the possibility to perform authentication without knowing who the user claims to be. Cryptographic security is based on the Paillier public key encryption scheme.

expand

A Critical Analysis and Improvement of AACS Drive-Host Authentication

Jiayuan Sui, Douglas R. Stinson

Pages: 37 - 52

doi>10.1007/978-3-540-70500-0_4

This paper presents a critical analysis of the AACS drive-host authentication scheme. A few weaknesses are identified which could lead to various attacks on the scheme. In particular, we observe that the scheme is susceptible to unknown key-share and ...

This paper presents a critical analysis of the AACS drive-host authentication scheme. A few weaknesses are identified which could lead to various attacks on the scheme. In particular, we observe that the scheme is susceptible to unknown key-share and man-in-the-middle attacks. Modifications of the scheme are suggested in order to provide better security. A proof of security of the modified scheme is also presented. The modified scheme achieves better efficiency than the original scheme.

expand

Comparing the Pre- and Post-specified Peer Models for Key Agreement

Alfred Menezes, Berkant Ustaoglu

Pages: 53 - 68

doi>10.1007/978-3-540-70500-0_5

In the pre-specified peer model for key agreement, it is assumed that a party knows the identifier of its intended communicating peer when it commences a protocol run. On the other hand, a party in the post-specified peer model for key agreement does ...

In the pre-specified peer model for key agreement, it is assumed that a party knows the identifier of its intended communicating peer when it commences a protocol run. On the other hand, a party in the post-specified peer model for key agreement does not know the identifier of its communicating peer at the outset, but learns the identifier during the protocol run. In this paper we compare the security assurances provided by the Canetti-Krawczyk security definitions for key agreement in the pre- and post-specified peer models. We give examples of protocols that are secure in one model but insecure in the other. We also enhance the Canetti-Krawczyk security models and definitions to encompass a class of protocols that are executable and secure in both the pre- and post-specified peer models.

expand

Efficient One-Round Key Exchange in the Standard Model

Colin Boyd, Yvonne Cliff, Juan Gonzalez Nieto, Kenneth G. Paterson

Pages: 69 - 83

doi>10.1007/978-3-540-70500-0_6

We consider one-round key exchange protocols secure in the standard model. The security analysis uses the powerful security model of Canetti and Krawczyk and a natural extension of it to the ID-based setting. It is shown how KEMs can be used in a generic ...

We consider one-round key exchange protocols secure in the standard model. The security analysis uses the powerful security model of Canetti and Krawczyk and a natural extension of it to the ID-based setting. It is shown how KEMs can be used in a generic way to obtain two different protocol designs with progressively stronger security guarantees. A detailed analysis of the performance of the protocols is included; surprisingly, when instantiated with specific KEM constructions, the resulting protocols are competitive with the best previous schemes that have proofs only in the random oracle model.

expand

On the Improvement of the BDF Attack on LSBS-RSA

Hung-Min Sun, Mu-En Wu, Huaxiong Wang, Jian Guo

Pages: 84 - 97

doi>10.1007/978-3-540-70500-0_7

An $\left(\alpha ,\beta ,\gamma \right) $-LSBS RSA denotes an RSA system with primes sharing ¿least significant bits, private exponent dwith βleast significant bits leaked, and public ...

An $\left(\alpha ,\beta ,\gamma \right) $-LSBS RSA denotes an RSA system with primes sharing ¿least significant bits, private exponent dwith βleast significant bits leaked, and public exponent ewith bit-length ¿. Steinfeld and Zheng showed that LSBS-RSA with small eis inherently resistant to the BDF attack, but LSBS-RSA with large eis more vulnerable than standard RSA. In this paper, we improve the

BDF attack on LSBS-RSA by reducing the cost of exhaustive search for k, where kis the parameter in RSA equation: $ed=k\cdot \varphi \left(N\right) +1$. Consequently, the complexity of the BDF attacks on LSBS-RSA can be further reduced. Denote ¿as the multiplicity of 2 in k. Our method gives the improvements, which depend on the two cases:

<OrderedList><ListItem><ItemNumber>1</ItemNumber>

 In the case $\gamma \leq \min \left\{ \beta ,2\alpha \right\} -\sigma $, the cost of exhaustive search for kin LSBS-RSA can be simplified to searching kin polynomial time. Thus, the complexity of the BDF attack is independent of ¿, but it still increases as ¿increases.</ListItem><ListItem><ItemNumber>1</ItemNumber>

 In the case $\gamma >\min \left\{ \beta ,2\alpha \right\} -\sigma $, the complexity of the BDF attack on LSBS-RSA can be further reduced with increasing ¿or β.</ListItem></OrderedList>More precisely, we show that an LSBS-RSA is more vulnerable under the BDF attack as $\max \left\{ 2\alpha ,\beta \right\} $ increases proportionally with the size of N. In the last, we point out that although LSBS-RSA benefits the computational efficiency in some applications, one should be more careful in using LSBS-RSA.

expand

Public-Key Cryptosystems with Primitive Power Roots of Unity

Takato Hirano, Koichiro Wada, Keisuke Tanaka

Pages: 98 - 112

doi>10.1007/978-3-540-70500-0_8

We first consider a variant of the Schmidt-Samoa---Takagi encryption scheme without losing additively homomorphic properties. We show that this variant is secure in the sense of IND-CPA under the decisional composite residuosity assumption, and of OW-CPA ...

We first consider a variant of the Schmidt-Samoa---Takagi encryption scheme without losing additively homomorphic properties. We show that this variant is secure in the sense of IND-CPA under the decisional composite residuosity assumption, and of OW-CPA under the assumption on the hardness of factoring n= p2q. Second, we introduce new cryptographic properties "affine" and "pre-image restriction", which are closely related to homomorphism. Intuitively, "affine" is a tuple of functions which have a special homomorphic property, and "pre-image restriction" is a function which can restrict the receiver to having information on the encrypted message. Then, we propose an encryption scheme with primitive

power roots of unity in $({\mathbb Z}/n^{s+1})^{\times}$. We show that our scheme has the above cryptographic properties.

expand

Relationship between Two Approaches for Defining the Standard Model PA-ness

Isamu Teranishi, Wakaha Ogata

Pages: 113 - 127

doi>10.1007/978-3-540-70500-0_9

There are two approaches to define Plaintext Awareness (PA). The first one is a classical approach to define the PA security and is used to define the PA security of the random oracle model. This approach enables us to define the PA-ness simply, but ...

There are two approaches to define Plaintext Awareness (PA). The first one is a classical approach to define the PA security and is used to define the PA security of the random oracle model. This approach enables us to define the PA-ness simply, but no one know whether we can define the standard model PA security based on this approach. In contrast, the second approach is a current approach to define the PA security. It enables us to define the standard model PA security formally, but it is more elaborate than the overwhelming-based approach. In this paper, we aim to clarify relations between the two approaches. We define the standard model PA security based on the first approach. Then we show that, under a very weak condition, it is equivalent to the known definition of the standard model PA security based on the second approach.

expand

Distributed Verification of Mixing - Local Forking Proofs Model

Jacek Cichoń, Marek Klonowski, Mirosław Kutyłowski

Pages: 128 - 140

doi>10.1007/978-3-540-70500-0_10

One of generic techniques to achieve anonymity is to process messages through a batch of cryptographic mixes. In order to guarantee proper execution verifiable mixes are constructed: each mix provides a proof of correctness together with its output. ...

One of generic techniques to achieve anonymity is to process messages through a batch of cryptographic mixes. In order to guarantee proper execution verifiable mixes are constructed: each mix provides a proof of correctness together with its output. However, if a mix is working on a huge number of messages at a time, the proof itself is huge since it concerns processing all messages. So in practice only a few verifiers would download the proofs and in turn we would have to trust what they are saying.

We consider a different model in which there are many verifiers, but each of them is going to download only a limited number of bits in order to check the mixes. Distributed character of the process ensures effectiveness even if many verifiers are dishonest and do not report irregularities found.

We concern a fully distributed and intuitive verification scheme which we call local forking proofs. For each intermediate ciphertext a verifier may ask for a proof that its re-encrypted version is in the output of the mix concerned. The proof shows that the re-encrypted version is within some subset of kciphertexts from the output of the mix, and it can be performed with strong zero-knowledge or algebraic methods. They should work efficiently concerning communication complexity, if kis a relatively small constant.

There are many issues concerning stochastic properties of local forking proofs. In this paper we examine just one: we estimate quite precisely how many mixes are required so that if a local proof is provided for each message, then a plaintext hidden in an input message can appear on any position of the final output set.

expand

Fully-Simulatable Oblivious Set Transfer

Huafei Zhu

Pages: 141 - 154

doi>10.1007/978-3-540-70500-0_11

In this paper, a new notion which we call oblivious set transfer is introduced and formalized. An oblivious set transfer in essence, is an extension of the notions of oblivious bit transfer and oblivious string transfer protocols. The security of oblivious ...

In this paper, a new notion which we call oblivious set transfer is introduced and formalized. An oblivious set transfer in essence, is an extension of the notions of oblivious bit transfer and oblivious string transfer protocols. The security of oblivious set transfer protocols is defined in the

real/ideal world simulation paradigm. We show that oblivious set transfer protocols that are provably secure in the full simulation model can be efficiently implemented assuming the existence of semantically secure encryption schemes, perfectly hiding commitments and perfectly binding commitments.

expand

Efficient Disjointness Tests for Private Datasets

Qingsong Ye, Huaxiong Wang, Josef Pieprzyk, Xian-Mo Zhang

Pages: 155 - 169

doi>10.1007/978-3-540-70500-0_12

We present efficient protocols for private set disjointness tests. We start from an intuition of our protocols that applies Sylvester matrices. Unfortunately, this simple construction is insecure as it reveals information about the cardinality of the ...

We present efficient protocols for private set disjointness tests. We start from an intuition of our protocols that applies Sylvester matrices. Unfortunately, this simple construction is insecure as it reveals information about the cardinality of the intersection. More specifically, it discloses its lower bound. By using the Lagrange interpolation we provide a protocol for the honest-but-curious case without revealing any additional information. Finally, we describe a protocol that is secure against malicious adversaries. The protocol applies a verification test to detect misbehaving participants. Both protocols require O(1) rounds of communication. Our protocols are more efficient than the previous protocols in terms of communication and computation overhead. Unlike previous protocols whose security relies on computational assumptions, our protocols provide information theoretic security. To our knowledge, our protocols are first ones that have been designed without a generic secure function evaluation. More importantly, they are the most efficient protocols for private disjointness tests for the malicious adversary case.

expand

Efficient Perfectly Reliable and Secure Message Transmission Tolerating Mobile Adversary

Arpita Patra, Ashish Choudhary, Madhu Vaidyanathan, C. Pandu Rangan

Pages: 170 - 186

doi>10.1007/978-3-540-70500-0_13

In this paper, we study the problem of Perfectly Reliable Message Transmission(PRMT) and Perfectly Secure Message Transmission(PSMT) between two nodes <Emphasis Type="Bold">S</Emphasis>and <Emphasis ...

In this paper, we study the problem of Perfectly Reliable Message Transmission(PRMT) and Perfectly Secure Message Transmission(PSMT) between two nodes <Emphasis Type="Bold">S</Emphasis>and <Emphasis Type="Bold">R</Emphasis>in an undirected synchronous network, a part of which is under the influence of an all powerful mobile Byzantineadversary. We design a threephase bit optimalPSMT protocol tolerating mobile adversary, whose communication complexity matches the existing lower bound on the communication complexity of any multi phase PSMT protocol, tolerating mobile adversary. This significantly reduces the phase complexity of the existing O(t) phase bit optimal PSMT protocol tolerating mobile adversary, where tdenotes the number of nodes corrupted by the mobile adversary. Furthermore, we design a three phase bit optimalPRMT protocol which achieves reliability with constant factoroverhead against a mobile adversary. These are the firstever constant phase bit optimalPRMT and PSMT protocols against mobile Byzantine adversary. We also characterize PSMT protocols in directednetworks tolerating mobile adversary. Finally, we derive tight bound on the number of rounds required to achieve reliable communication from <Emphasis Type="Bold">S</Emphasis>to <Emphasis Type="Bold">R</Emphasis>tolerating a mobile adversary with arbitrary roaming speed.Finally, we show how our constant phase PRMT and PSMT protocols can be adapted to design round optimaland bit optimalPRMT and PSMT protocols, provided the network is given as collection of vertex disjoint paths.

expand

Methods for Linear and Differential Cryptanalysis of Elastic Block Ciphers

Debra L. Cook, Moti Yung, Angelos D. Keromytis

Pages: 187 - 202

doi>10.1007/978-3-540-70500-0_14

The elastic block cipher design employs the round function of a given, b-bit block cipher in a black box fashion, embedding it in a network structure to construct a family of ciphers in a uniform manner. The family is parameterized ...

The elastic block cipher design employs the round function of a given, b-bit block cipher in a black box fashion, embedding it in a network structure to construct a family of ciphers in a uniform manner. The family is parameterized by block size, for any size between band 2b. The design assures that the overall workload for encryption is proportional to the block size. When considering the approach taken in elastic block ciphers, the question arises as to whether cryptanalysis results, including methods of analysis and bounds on security, for the original fixed-sized cipher are lost or, since original components of the cipher are used, whether previous analysis can be applied or reused in some manner.

With this question in mind, we analyze elastic block ciphers and consider the security against two basic types of attacks, linear and differential cryptanalysis. We show how they can be related to the corresponding security of the fixed-length version of the cipher. Concretely, we develop techniques that take advantage of relationships between the structure of the elastic network and the original version of the cipher, independently of the cipher.

This approach demonstrates how one can build upon existing components to allow cryptanalysis within an extended structure (a topic which may be of general interest outside of elastic block ciphers). We show that any linear attack on an elastic block cipher can be converted efficiently into a linear attack on the fixed-length version of the cipher by converting the equations used to attack the elastic version to equations for the fixed-length version. We extend the result to any algebraic attack. We then define a general method for deriving the differential characteristic bound of an elastic block cipher using the differential bound on a single round of the fixed-length version of the cipher. The structure of elastic block ciphers allows us to use a state transition method to compute differentials for the elastic version from differentials of the round function of the original cipher.

expand

Multidimensional Linear Cryptanalysis of Reduced Round Serpent

Miia Hermelin, Joo Yeon Cho, Kaisa Nyberg

Pages: 203 - 215

doi>10.1007/978-3-540-70500-0_15

Various authors have previously presented different approaches how to exploit multiple linear approximations to enhance linear cryptanalysis. In this paper we present a new truly multidimensional approach to generalise Matsui's Algorithm 1. We derive ...

Various authors have previously presented different approaches how to exploit multiple linear

approximations to enhance linear cryptanalysis. In this paper we present a new truly multidimensional approach to generalise Matsui's Algorithm 1. We derive the statistical framework for it and show how to calculate multidimensional probability distributions based on correlations of one-dimensional linear approximations. The main advantage is that the assumption about statistical independence of linear approximations can be removed. Then we apply these new techniques to four rounds of the block cipher Serpent and show that the multidimensional approach is more effective in recovering key bits correctly than the previous methods that use a multiple of one-dimensional linear approximations.

expand

Cryptanalysis of Reduced-Round SMS4 Block Cipher

Lei Zhang, Wentao Zhang, Wenling Wu

Pages: 216 - 229

doi>10.1007/978-3-540-70500-0_16

SMS4 is a 128-bit block cipher used in the WAPI standard. WAPI is the Chinese national standard for securing Wireless LANs. Since the specification of SMS4 was not released until January 2006, there have been only a few papers analyzing this cipher. ...

SMS4 is a 128-bit block cipher used in the WAPI standard. WAPI is the Chinese national standard for securing Wireless LANs. Since the specification of SMS4 was not released until January 2006, there have been only a few papers analyzing this cipher. In this paper, firstly we present a kind of 5-round iterative differential characteristic of SMS4 whose probability is about 2¿ 42. Then based on this kind of iterative differential characteristic, we present a rectangle attack on 16-round SMS4 and a differential attack on 21-round SMS4. As far as we know, these are the best cryptanalytic results on SMS4.

expand

On the Unprovable Security of 2-Key XCBC

Peng Wang, Dengguo Feng, Wenling Wu, Liting Zhang

Pages: 230 - 238

doi>10.1007/978-3-540-70500-0_17

There has been extensive research focusing on improving CBC-MAC to operate on variable length messages with less keys and less blockcipher invocations. After Black and Rogaway's XCBC, Moriai and Imai proposed 2-Key XCBC, which replaced the third key ...

There has been extensive research focusing on improving CBC-MAC to operate on variable length messages with less keys and less blockcipher invocations. After Black and Rogaway's XCBC, Moriai and Imai proposed 2-Key XCBC, which replaced the third key of XCBC with its first key. Moriai and Imai "proved" that 2-Key XCBC is secure if the underling blockcipher is a pseudorandom permutation (PRP). Our research shows that it is not the case. The security of 2-Key XCBC can not be proved under the solo assumption of PRP, even if it is a RPR-RK secure against some related-key attack. We construct a special PRP (PRP-RK) to show that the main lemma in [14] is not true and 2-Key XCBC using this PRP (PRP-RK) is totally insecure.

expand

Looking Back at a New Hash Function

Olivier Billet, Matthew J. Robshaw, Yannick Seurin, Yiqun Lisa Yin

Pages: 239 - 253

doi>10.1007/978-3-540-70500-0_18

We present two (related) dedicated hash functions that deliberately borrow heavily from the block ciphers that appeared in the final stages of the AES process. We explore the computational trade-off between the key schedule and encryption in a block ...

We present two (related) dedicated hash functions that deliberately borrow heavily from the block ciphers that appeared in the final stages of the AES process. We explore the computational trade-off between the key schedule and encryption in a block cipher-based hash function and we illustrate our approach with a 256-bit hash function that has a hashing rate equivalent to the encryption rate of AES-128. The design extends naturally to a 512-bit hash function.

expand

Non-linear Reduced Round Attacks against SHA-2 Hash Family

Somitra Kumar Sanadhya, Palash Sarkar

Pages: 254 - 266

doi>10.1007/978-3-540-70500-0_19

Most of the attacks against (reduced) SHA-2 family in literature have used local collisions which are valid for linearized version of SHA-2 hash functions. Recently, at FSE '08, an attack against reduced round SHA-256 was presented by Nikolić and ...

Most of the attacks against (reduced) SHA-2 family in literature have used local collisions which are valid for linearized version of SHA-2 hash functions. Recently, at FSE '08, an attack against reduced round SHA-256 was presented by Nikolić and Biryukov which used a local collision which is valid for the actual SHA-256 function. It is a 9-step local collision which starts by introducing a modular difference of 1 in the two messages. It succeeds with probability roughly 1/3. We build on the work of Nikolić and Biryukov and provide a generalized nonlinear local collision which accepts an arbitrary initial message difference. This local collision succeeds with probability 1. Using this local collision we present attacks against 18-step SHA-256 and 18-step SHA-512 with arbitrary initial difference. Both of these attacks succeed with probability 1. We then present special cases of our local collision and show two different differential paths for attacking 20-step SHA-256 and 20-step SHA-512. One of these paths is the same as presented by Nikolić and Biryukov while the other one is a new differential path. Messages following both these differential paths can be found with probability 1. This improves on the previous result where the success probability of 20-step attack was 1/3. Finally, we present two differential paths for 21-step collisions for SHA-256 and SHA-512, one of which is a new path. The success probabilities of these paths for SHA-256 are roughly 2¿ 15and 2¿ 17which improve on the 21-step attack having probability 2¿ 19reported earlier. We show examples of message pairs following all the presented differential paths for up to 21-step collisions in SHA-256. We also show first real examples of colliding message pairs for up to 20-step reduced SHA-512.

expand

Collisions for Round-Reduced LAKE

Florian Mendel, Martin Schläffer

Pages: 267 - 281

doi>10.1007/978-3-540-70500-0_20

LAKE is a family of cryptographic hash functions presented at FSE 2008. It is an iterated hash function and defines two main instances with a 256 bit and 512 bit hash value. In this paper, we

present the first security analysis of LAKE. We show how collision ...

LAKE is a family of cryptographic hash functions presented at FSE 2008. It is an iterated hash function and defines two main instances with a 256 bit and 512 bit hash value. In this paper, we present the first security analysis of LAKE. We show how collision attacks, exploiting the non-bijectiveness of the internal compression function of LAKE, can be mounted on reduced variants of LAKE. We show an efficient attack on the 256 bit hash function LAKE-256 reduced to 3 rounds and present an actual colliding message pair. Furthermore, we present a theoretical attack on LAKE-256 reduced to 4 rounds with a complexity of 2109. By using more sophisticated message modification techniques we expect that the attack can be extended to 5 rounds. However, for the moment our approach does not appear to be applicable to the full LAKE-256 hash function (with all 8 rounds).

expand

Preimage Attacks on Step-Reduced MD5

Yu Sasaki, Kazumaro Aoki

Pages: 282 - 296

doi>10.1007/978-3-540-70500-0_21

In this paper, we propose preimage attacks on step-reduced MD5. We show that a preimage of a 44-step MD5 can be computed to a complexity of 296. We also consider a preimage attack against variants of MD5 where the round order is modified from ...

In this paper, we propose preimage attacks on step-reduced MD5. We show that a preimage of a 44-step MD5 can be computed to a complexity of 296. We also consider a preimage attack against variants of MD5 where the round order is modified from the real MD5. In such a case, a preimage of a 51-step round-reordered MD5 can be computed to a complexity of 296. Our attack uses "local collisions" of MD5 to create a degree of message freedom. This freedom enables us to match the two 128-bit intermediate values efficiently.

expand

Linear Distinguishing Attack on Shannon

Risto M. Hakala, Kaisa Nyberg

Pages: 297 - 305

doi>10.1007/978-3-540-70500-0_22

In this paper, we present a linear distinguishing attack on the stream cipher Shannon. Our distinguisher can distinguish the output keystream of Shannon from 2107keystream words while using an array of 232counters. The distinguisher ...

In this paper, we present a linear distinguishing attack on the stream cipher Shannon. Our distinguisher can distinguish the output keystream of Shannon from 2107keystream words while using an array of 232counters. The distinguisher makes use of a multidimensional linear transformation instead of a one-dimensional transformation, which is traditionally used in linear distinguishing attacks. This gives a clear improvement to the keystream requirement: we need approximately 25times less keystream than when a one-dimensional transform is used.

expand

Recovering RC4 Permutation from 2048 Keystream Bytes if j Is Stuck

Subhamoy Maitra, Goutam Paul

Pages: 306 - 320

doi>10.1007/978-3-540-70500-0_23

In this paper, we study the behaviour of RC4 when the index jis stuck at a certain value not known to the attacker. Though it seems quite natural that RC4 would be weak if jdoes not change, it has never been ...

In this paper, we study the behaviour of RC4 when the index jis stuck at a certain value not known to the attacker. Though it seems quite natural that RC4 would be weak if jdoes not change, it has never been studied earlier in a disciplined manner. This work presents the nontrivial issues involved in the analysis, identifying how the information regarding Sstarts leaking with as low as 258 keystream output bytes. The leakage of information increases as more bytes are available and finally the complete Sis recovered with 211bytes in around 225time complexity. The attack considers that "the deterministic index iat the point when jgot stuck" and "the value at which jremains stuck" are unknown. Further, the study presents a nice combinatorial structure that is relevant to the fault analysis of RC4.

expand

Related-Key Chosen IV Attacks on Grain-v1 and Grain-128

Yuseop Lee, Kitae Jeong, Jaechul Sung, Seokhie Hong

Pages: 321 - 335

doi>10.1007/978-3-540-70500-0_24

The slide resynchronization attack on Grain was proposed in [6]. This attack finds related keys and initialization vectors of Grain that generate the 1-bit shifted keystream sequence. In this paper, we extend the attack proposed in [6] and propose related-key ...

The slide resynchronization attack on Grain was proposed in [6]. This attack finds related keys and initialization vectors of Grain that generate the 1-bit shifted keystream sequence. In this paper, we extend the attack proposed in [6] and propose related-key chosen IV attacks on Grain-v1 and Grain-128. The attack on Grain-v1 recovers the secret key with 222.59chosen IVs, 226.29-bit keystream sequences and 222.90computational complexity. To recover the secret key of Grain-128, our attack requires 226.59chosen IVs, 231.39-bit keystream sequences and 227.01computational complexity. These works are the first known key recovery attacks on Grain-v1 and Grain-128.

expand

Signature Generation and Detection of Malware Families

V. Sai Sathyanarayan, Pankaj Kohli, Bezawada Bruhadeshwar

Pages: 336 - 349

doi>10.1007/978-3-540-70500-0_25

Malware detection and prevention is critical for the protection of computing systems across the Internet. The problem in detecting malware is that they evolveover a period of time and hence, traditional signature-based malware detectors ...

Malware detection and prevention is critical for the protection of computing systems across the Internet. The problem in detecting malware is that they evolveover a period of time

and hence, traditional signature-based malware detectors fail to detect obfuscated and previously unseen malware executables. However, as malware evolves, some semantics of the original malware are preserved as these semantics are necessary for the effectiveness of the malware. Using this observation, we present a novel method for detection of malware using the correlation between the semantics of the malware and its API calls. We construct a base signature for an entire malware class rather than for a single specimen of malware. Such a signature is capable of detecting even unknown and advanced variants that belong to that class. We demonstrate our approach on some well known malware classes and show that any advanced variant of the malware class is detected from the base signature.

expand

Reducing Payload Scans for Attack Signature Matching Using Rule Classification

Sunghyun Kim, Heejo Lee

Pages: 350 - 360

doi>10.1007/978-3-540-70500-0_26

Network intrusion detection systems rely on a signature-based detection engine. When under attack or during heavy traffic, the detection engines need to make fast decision whether a packet or a sequence of packets is normal or malicious. However, if ...

Network intrusion detection systems rely on a signature-based detection engine. When under attack or during heavy traffic, the detection engines need to make fast decision whether a packet or a sequence of packets is normal or malicious. However, if packets have a heavy payload or the system has a great deal of attack patterns, the high cost of payload inspection severely diminishes the detection performance. Therefore, it would be better to avoid unnecessary payload scans by checking the protocol fields in the packet header first, before executing their heavy operations of payload inspection. Furthermore, when payload inspection is necessary, it is better to compare attack patterns as few as possible. In this paper, we propose a method which reduces payload scans by an integration of processing protocol fields and classifying payload signatures. While performance improvements are dependent on a given networking environment, the experimental results with the DARPA data set show that the proposed method outperforms the latest Snort over 6.5% for web traffic.

expand

Implicit Detection of Hidden Processes with a Feather-Weight Hardware-Assisted Virtual Machine Monitor

Yan Wen, Jinjing Zhao, Huaimin Wang, Jiannong Cao

Pages: 361 - 375

doi>10.1007/978-3-540-70500-0_27

Process hiding is a commonly used stealth technique which facilitates the evasion from the detection by anti-malware programs. In this paper, we propose a new approach called Ariesto implicitly detect the hidden processes. Aries ...

Process hiding is a commonly used stealth technique which facilitates the evasion from the detection by anti-malware programs. In this paper, we propose a new approach called Ariesto implicitly detect the hidden processes. Aries introduces a novel feather-weight hardware-assisted virtual machine monitor (VMM) to obtain the True Process List (TPL). Compared to existing VMM-based approaches, Aries offers three distinct advantages: dynamic OS migration, implicit introspection of TPLand non-bypassable interfacesfor exposing TPL. Unlike typical VMMs, Aries can dynamically migrate a booted OS on it. By tracking the low-level interactions between the OS and the memory management structures, Aries is decoupled with the explicit OS implementation information which is subvertable for the privileged malware. Our functionality evaluation shows Aries can detect more process-hiding malware than existing detectors while the performance evaluation shows desktop-oriented workloads achieve 95.2% of native speed on average.

expand

FormatShield: A Binary Rewriting Defense against Format String Attacks

Pankaj Kohli, Bezawada Bruhadeshwar

Pages: 376 - 390

doi>10.1007/978-3-540-70500-0_28

Format string attacks allow an attacker to read or write anywhere in the memory of a process. Previous solutions designed to detect format string attacks either require source code and recompilation of the program, or aim to defend only against write ...

Format string attacks allow an attacker to read or write anywhere in the memory of a process. Previous solutions designed to detect format string attacks either require source code and

recompilation of the program, or aim to defend only against write attempts to security critical control information. They do not protect against arbitrary memory read attempts and non-control data attacks. This paper presents FormatShield, a comprehensive defense against format string attacks. FormatShield identifies potentially vulnerable call sites in a running process and dumps the corresponding context information in the program binary. Attacks are detected when malicious input is found at vulnerable call sites with an exploitable context. It does not require source code or recompilation of the program and can defend against arbitrary memory read and write attempts, including non-control data attacks. Also, our experiments show that FormatShield incurs minimal performance overheads and is better than existing solutions.

expand

Advanced Permission-Role Relationship in Role-Based Access Control

Min Li, Hua Wang, Ashley Plank, Jianming Yong

Pages: 391 - 403

doi>10.1007/978-3-540-70500-0_29

Permission-role assignment is an important issue in role-based access control (RBAC). There are two types of problems that may arise in permission-role assignment. One is related to authorization granting process. Conflicting permissions may be granted ...

Permission-role assignment is an important issue in role-based access control (RBAC). There are two types of problems that may arise in permission-role assignment. One is related to authorization granting process. Conflicting permissions may be granted to a role, and as a result, users with the role may have or derive a high level of authority. The other is related to authorization revocation. When a permission is revoked from a role, the role may still have the permission from other roles. In this paper, we discuss granting and revocation models related to mobile and immobile memberships between permissions and roles, then provide proposed authorization granting algorithm to check conflicts and help allocate the permissions without compromising the security. To our best knowledge, the new revocation models, local and global revocation, have not been studied before. The local and global revocation algorithms based on relational algebra and operations provide a rich variety. We also apply the new algorithms to an anonymity scalable payment scheme.

expand

Enhancing Micro-Aggregation Technique by Utilizing Dependence-Based Information in Secure Statistical Databases

B. John Oommen, Ebaa Fayyoumi

Pages: 404 - 418

doi>10.1007/978-3-540-70500-0_30

We consider the Micro-Aggregation Problem (MAP) in secure statistical databases which involves partitioning a set of individual records in a micro-data file into a number of mutually exclusive and exhaustive groups. This problem, ...

We consider the Micro-Aggregation Problem (MAP) in secure statistical databases which involves partitioning a set of individual records in a micro-data file into a number of mutually exclusive and exhaustive groups. This problem, which seeks for the best partition of the micro-data file, is known to be NP-hard, and has been tackled using many heuristic solutions. In this paper, we would like to demonstrate that in the process of developing Micro-Aggregation Techniques (MATs), it is expedient to incorporate information about the dependence between the random variables in the micro-data file. This can be achieved by pre-processing the micro-data beforeinvoking any MAT, in order to extract the useful dependence information from the joint probability distribution of the variables in the micro-data file, and then accomplishing the micro-aggregation on the "maximally independent" variables. Our results, on real life data sets, show that including such information will enhance the process of determining how many variables are to be used, and which of them should be used in the micro-aggregation process.

expand

Montgomery Residue Representation Fault-Tolerant Computation in GF(2k)

Silvana Medoš, Serdar Boztaş

Pages: 419 - 432

doi>10.1007/978-3-540-70500-0_31

In this paper, we are concerned with protecting elliptic curve computation in a tamper proof device by protecting finite field computation against active side channel attacks, i.e., fault attacks. We propose residue representation of the field elements ...

In this paper, we are concerned with protecting elliptic curve computation in a tamper proof device by protecting finite field computation against active side channel attacks, i.e., fault attacks. We

propose residue representation of the field elements for fault tolerant Montgomery residue representation multiplication algorithm, by providing fault models for fault attacks, and countermeasures to some fault inducing attacks.

expand

A Tree-Based Approach for Computing Double-Base Chains

Christophe Doche, Laurent Habsieger

Pages: 433 - 446

doi>10.1007/978-3-540-70500-0_32

We introduce a tree-based method to find short Double-Base chains. As compared to the classical greedy approach, this new method is not only simpler to implement and faster, experimentally it also returns shorter chains on average. The complexity analysis ...

We introduce a tree-based method to find short Double-Base chains. As compared to the classical greedy approach, this new method is not only simpler to implement and faster, experimentally it also returns shorter chains on average. The complexity analysis shows that the average length of a chain returned by this tree-based approach is $\frac{\log_2 n }{4.6419}\cdotp$ This tends to suggest that the average length of DB-chains generated by the greedy approach is not O(logn/loglogn). We also discuss generalizations of this method, namely to compute Step Multi-Base Representation chains involving more than 2 bases and extended DB-chains having nontrivial coefficients.

expand

Extractors for Jacobians of Binary Genus-2 Hyperelliptic Curves

Reza Rezaeian Farashahi

Pages: 447 - 462

doi>10.1007/978-3-540-70500-0_33

Extractors are an important ingredient in designing key exchange protocols and secure pseudorandom sequences in the standard model. Elliptic and hyperelliptic curves are gaining more and more interest due to their fast arithmetic and the fact that no ...

Extractors are an important ingredient in designing key exchange protocols and secure pseudorandom sequences in the standard model. Elliptic and hyperelliptic curves are gaining more and more interest due to their fast arithmetic and the fact that no subexponential attacks against the discrete logarithm problem are known.

In this paper we propose two simple and efficient deterministic extractors for $J(\mathbb{F}_q)$, the Jacobian of a genus 2 hyperelliptic curve Hdefined over $\mathbb{F}_q$, where q= 2n, called the sumand productextractors.

For non-supersingular hyperelliptic curves having a Jacobian with group order 2m, where mis odd, we propose the modified sumand productextractors for the main subgroup of $J(\mathbb{F}_q)$. We show that, if $D\in J(\mathbb{F}_q)$ is chosen uniformly at random, the bits extracted from Dare indistinguishable from a uniformly random bit-string of length n.

expand

Efficient Modular Arithmetic in Adapted Modular Number System Using Lagrange Representation

Christophe Negre, Thomas Plantard

Pages: 463 - 477

doi>10.1007/978-3-540-70500-0_34

In 2004, Bajard, Imbert and Plantard introduced a new system of representation to perform arithmetic modulo a prime integer p, the Adapted Modular Number System (AMNS). In this system, the elements are seen as polynomial of degree ...

In 2004, Bajard, Imbert and Plantard introduced a new system of representation to perform arithmetic modulo a prime integer p, the Adapted Modular Number System (AMNS). In this system, the elements are seen as polynomial of degree n¿ 1 with the coefficients of size p1/n. The best method for multiplication in AMNS works only for some specific moduli p. In this paper, we propose a novel algorithm to perform the modular multiplication in the AMNS. This method works for any AMNS, and does not use a special form of the modulo p. We also present a version of this algorithm in Lagrange Representationwhich performs the polynomial multiplication part of the first algorithm efficiently using Fast Fourier Transform.

expand