Vijay Varadharajan
Yi Mu (Eds.)

LNCS 2119

Information Security and Privacy

6th Australasian Conference, ACISP 2001
Sydney, Australia, July 2001
Proceedings

Springer

Vijay Varadharajan Yi Mu (Eds.)

Information Security and Privacy

6th Australasian Conference, ACISP 2001
Sydney, Australia, July 11-13, 2001
Proceedings

Springer

Volume Editors

Vijay Varadharajan
Yi Mu
Macquarie University, Department of Computing
North Ryde, NSW 2109, Australia
E-mail: {vijay,ymu}@ics.mq.edu.au

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Information security and privacy : 6th Australasian conference ; proceedings / ACISP 2001, Sydney, Australia, July 11 - 13, 2001. Vijay Varadharajan ; Yi Mu (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo : Springer, 2001
(Lecture notes in computer science ; Vol. 2119)
ISBN 3-540-42300-1

CR Subject Classification (1998): E.3, K.6.5, D.4.6, C.2, E.4, F.2.1, K.4.1

ISSN 0302-9743
ISBN 3-540-42300-1 Springer-Verlag Berlin Heidelberg New York

Springer-Verlag Berlin Heidelberg New York
a member of BertelsmannSpringer Science+Business Media GmbH

http://www.springer.de

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Boller Mediendesign
Printed on acid-free paper SPIN: 10839883 06/3142 5 4 3 2 1 0

Lecture Notes in Computer Science 2119

Edited by G. Goos, J. Hartmanis and J. van Leeuwen

Springer
Berlin
Heidelberg
New York
Barcelona
Hong Kong
London
Milan
Paris
Singapore
Tokyo

Preface

ACISP 2001, the Sixth Australasian Conference on Information Security and Privacy, was held in Sydney, Australia. The conference was sponsored by Information and Networked System Security Research (INSSR), Macquarie University, the Australian Computer Society, and the University of Western Sydney. I am grateful to all these organizations for their support of the conference.

The aim of this conference was to draw together researchers, designers, and users of information security systems and technologies. The conference program addressed a range of aspects from system and network security to secure Internet applications to cryptography and cryptanalysis. This year the program committee invited two international keynote speakers Dr. Yačov Yacobi from Microsoft Research (USA) and Dr. Clifford Neumann from the University of Southern California (USA). Dr. Yacobi's talk addressed the issues of trust, privacy, and anti-piracy in electronic commerce. Dr. Neumann's address was concerned with authorization policy issues and their enforcement in applications.

The conference received 91 papers from America, Asia, Australia, and Europe. The program committee accepted 38 papers and these were presented in some 9 sessions covering system security, network security, trust and access control, Authentication, cryptography, cryptanalysis, Digital Signatures, Elliptic Curve Based Techniques, and Secret Sharing and Threshold Schemes. This year the accepted papers came from a range of countries, including 7 from Australia, 8 from Korea, 7 from Japan, 3 from UK, 3 from Germany, 3 from USA, 2 from Singapore, 2 from Canada and 1 from Belgium, Estonia, and Taiwan.

Organizing a conference such as this one is a time-consuming task and I would like to thank all the people who worked hard to make this conference a success. In particular, I would like to thank Program Co-chair Yi Mu for his tireless work and the members of the program committee for putting together an excellent program, and all the session chairs and speakers for their time and effort. Special thanks to Yi Mu, Laura Olsen, Rajan Shankaran, and Michael Hitchens for their help with local organization details. Finally, I would like to thank all the authors who submitted papers and all the participants of ACISP 2001. I hope that the professional contacts made at this conference, the presentations, and the proceedings have offered you insights and ideas that you can apply to your own efforts in security and privacy.

July 2001 Vijay Varadharajan

AUSTRALASIAN CONFERENCE ON INFORMATION SECURITY AND PRIVACY ACISP 2001

Sponsored by
Macquarie University
Australian Computer Society

General Chair:

Vijay Varadharajan	*Macquarie University, Australia*

Program Chairs:

Vijay Varadharajan	*Macquarie University, Australia*
Yi Mu	*Macquarie University, Australia*

Program Committee:

Ross Anderson	*Cambridge University, UK*
Colin Boyd	*Queensland University of Technology, Australia*
Ed Dawson	*Queensland University of Technology, Australia*
Yvo Desmedt	*Florida State University, USA*
Paul England	*Microsoft*
Yair Frankel	*Columbia University, USA*
Ajoy Ghosh	*UNISYS, Australia*
Dieter Gollman	*Microsoft*
John Gordon	*ConceptLabs, UK*
Kwangjo Kim	*ICU, Korea*
Chuchang Liu	*DSTO, Australia*
Masahiro Mambo	*Tohoku University, Japan*
Wenbo Mao	*Hewlett-Packard Lab., UK*
Yi Mu	*Macquarie University, Australia*
Chris Mitchell	*London University, UK*
Eiji Okamoto	*University of Wisconsin, USA*
Joe Pato	*Hewlett-Packard Lab., USA*
Josef Pieprzyk	*Macquarie University, Australia*
Bart Preneel	*Katholieke University, Belgium*
Qing Sihan	*Academy of Science, China*
Rei Safavi-Naini	*University of Wollongong, Australia*
Jennifer Seberry	*University of Wollongong, Australia*
Yuliang Zheng	*Monash University, Australia*

Referees:

Joonsang Baek, Yun Bai, Gareth Brisbane, Mike Burmester, Andrew Clark, Jung Hee Cheon, Hyun-Jin Choi, Stephen Crane, Mark Crosbie, Peter Duffett, Steven Galbraith, Juanma Gonzalez-Nieto, Marie Henderson, Tri V. Le, Byoungcheon Lee, Mark Looi, Greg Maitland, Marco Casassa Mont, Yuichi Nakai, Maris A Ozols, Marcus Peinado, Jakob Rehof, Jason Reid, Rajan Shankaran, Nickolas Sheppard, Leonie Simpson, Jeff Stehlin, Ron Steinfeld, Frederik Vercauteren, Kapali Viswanathan, Yejing Wang, Chuan Kun Wu, Jianxin Yan, and John Yesberg.

Lecture Notes in Computer Science

For information about Vols. 1–2013
please contact your bookseller or Springer-Verlag

Vol. 2014: M. Moortgat (Ed.), Logical Aspects of Computational Linguistics. Proceedings, 1998. X, 287 pages. 2001. (Subseries LNAI).

Vol. 2015: D. Won (Ed.), Information Security and Cryptology – ICISC 2000. Proceedings, 2000. X, 261 pages. 2001.

Vol. 2016: S. Murugesan, Y. Deshpande (Eds.), Web Engineering. IX, 357 pages. 2001.

Vol. 2018: M. Pollefeys, L. Van Gool, A. Zisserman, A. Fitzgibbon (Eds.), 3D Structure from Images – SMILE 2000. Proceedings, 2000. X, 243 pages. 2001.

Vol. 2019: P. Stone, T. Balch, G. Kraetzschmar (Eds.), RoboCup 2000: Robot Soccer World Cup IV. XVII, 658 pages. 2001. (Subseries LNAI).

Vol. 2020: D. Naccache (Ed.), Topics in Cryptology – CT-RSA 2001. Proceedings, 2001. XII, 473 pages. 2001

Vol. 2021: J. N. Oliveira, P. Zave (Eds.), FME 2001: Formal Methods for Increasing Software Productivity. Proceedings, 2001. XIII, 629 pages. 2001.

Vol. 2022: A. Romanovsky, C. Dony, J. Lindskov Knudsen, A. Tripathi (Eds.), Advances in Exception Handling Techniques. XII, 289 pages. 2001

Vol. 2024: H. Kuchen, K. Ueda (Eds.), Functional and Logic Programming. Proceedings, 2001. X, 391 pages. 2001.

Vol. 2025: M. Kaufmann, D. Wagner (Eds.), Drawing Graphs. XIV, 312 pages. 2001.

Vol. 2026: F. Müller (Ed.), High-Level Parallel Programming Models and Supportive Environments. Proceedings, 2001. IX, 137 pages. 2001.

Vol. 2027: R. Wilhelm (Ed.), Compiler Construction. Proceedings, 2001. XI, 371 pages. 2001.

Vol. 2028: D. Sands (Ed.), Programming Languages and Systems. Proceedings, 2001. XIII, 433 pages. 2001.

Vol. 2029: H. Hussmann (Ed.), Fundamental Approaches to Software Engineering. Proceedings, 2001. XIII, 349 pages. 2001.

Vol. 2030: F. Honsell, M. Miculan (Eds.), Foundations of Software Science and Computation Structures. Proceedings, 2001. XII, 413 pages. 2001.

Vol. 2031: T. Margaria, W. Yi (Eds.), Tools and Algorithms for the Construction and Analysis of Systems. Proceedings, 2001. XIV, 588 pages. 2001.

Vol. 2032: R. Klette, T. Huang, G. Gimel'farb (Eds.), Multi-Image Analysis. Proceedings, 2000. VIII, 289 pages. 2001.

Vol. 2033: J. Liu, Y. Ye (Eds.), E-Commerce Agents. VI, 347 pages. 2001. (Subseries LNAI).

Vol. 2034: M.D. Di Benedetto, A. Sangiovanni-Vincentelli (Eds.), Hybrid Systems: Computation and Control. Proceedings, 2001. XIV, 516 pages. 2001.

Vol. 2035: D. Cheung, G.J. Williams, Q. Li (Eds.), Advances in Knowledge Discovery and Data Mining – PAKDD 2001. Proceedings, 2001. XVIII, 596 pages. 2001. (Subseries LNAI).

Vol. 2037: E.J.W. Boers et al. (Eds.), Applications of Evolutionary Computing. Proceedings, 2001. XIII, 516 pages. 2001.

Vol. 2038: J. Miller, M. Tomassini, P.L. Lanzi, C. Ryan, A.G.B. Tettamanzi, W.B. Langdon (Eds.), Genetic Programming. Proceedings, 2001. XI, 384 pages. 2001.

Vol. 2039: M. Schumacher, Objective Coordination in Multi-Agent System Engineering. XIV, 149 pages. 2001. (Subseries LNAI).

Vol. 2040: W. Kou, Y. Yesha, C.J. Tan (Eds.), Electronic Commerce Technologies. Proceedings, 2001. X, 187 pages. 2001.

Vol. 2041: I. Attali, T. Jensen (Eds.), Java on Smart Cards: Programming and Security. Proceedings, 2000. X, 163 pages. 2001.

Vol. 2042: K.-K. Lau (Ed.), Logic Based Program Synthesis and Transformation. Proceedings, 2000. VIII, 183 pages. 2001.

Vol. 2043: D. Craeynest, A. Strohmeier (Eds.), Reliable Software Technologies – Ada-Europe 2001. Proceedings, 2001. XV, 405 pages. 2001.

Vol. 2044: S. Abramsky (Ed.), Typed Lambda Calculi and Applications. Proceedings, 2001. XI, 431 pages. 2001.

Vol. 2045: B. Pfitzmann (Ed.), Advances in Cryptology – EUROCRYPT 2001. Proceedings, 2001. XII, 545 pages. 2001.

Vol. 2047: R. Dumke, C. Rautenstrauch, A. Schmietendorf, A. Scholz (Eds.), Performance Engineering. XIV, 349 pages. 2001.

Vol. 2048: J. Pauli, Learning Based Robot Vision. IX, 288 pages. 2001.

Vol. 2051: A. Middeldorp (Ed.), Rewriting Techniques and Applications. Proceedings, 2001. XII, 363 pages. 2001.

Vol. 2052: V.I. Gorodetski, V.A. Skormin, L.J. Popyack (Eds.), Information Assurance in Computer Networks. Proceedings, 2001. XIII, 313 pages. 2001.

Vol. 2053: O. Danvy, A. Filinski (Eds.), Programs as Data Objects. Proceedings, 2001. VIII, 279 pages. 2001.

Vol. 2054: A. Condon, G. Rozenberg (Eds.), DNA Computing. Proceedings, 2000. X, 271 pages. 2001.

Vol. 2055: M. Margenstern, Y. Rogozhin (Eds.), Machines, Computations, and Universality. Proceedings, 2001. VIII, 321 pages. 2001.

Vol. 2056: E. Stroulia, S. Matwin (Eds.), Advances in Artificial Intelligence. Proceedings, 2001. XII, 366 pages. 2001. (Subseries LNAI).

Vol. 2057: M. Dwyer (Ed.), Model Checking Software. Proceedings, 2001. X, 313 pages. 2001.

Vol. 2059: C. Arcelli, L.P. Cordella, G. Sanniti di Baja (Eds.), Visual Form 2001. Proceedings, 2001. XIV, 799 pages. 2001.

Vol. 2060: T. Böhme, H. Unger (Eds.), Innovative Internet Computing Systems. Proceedings, 2001. VIII, 183 pages. 2001.

Vol. 2062: A. Nareyek, Constraint-Based Agents. XIV, 178 pages. 2001. (Subseries LNAI).

Vol. 2064: J. Blanck, V. Brattka, P. Hertling (Eds.), Computability and Complexity in Analysis. Proceedings, 2000. VIII, 395 pages. 2001.

Vol. 2065: H. Balster, B. de Brock, S. Conrad (Eds.), Database Schema Evolution and Meta-Modeling. Proceedings, 2000. X, 245 pages. 2001.

Vol. 2066: O. Gascuel, M.-F. Sagot (Eds.), Computational Biology. Proceedings, 2000. X, 165 pages. 2001.

Vol. 2068: K.R. Dittrich, A. Geppert, M.C. Norrie (Eds.), Advanced Information Systems Engineering. Proceedings, 2001. XII, 484 pages. 2001.

Vol. 2070: L. Monostori, J. Váncza, M. Ali (Eds.), Engineering of Intelligent Systems. Proceedings, 2001. XVIII, 951 pages. 2001. (Subseries LNAI).

Vol. 2071: R. Harper (Ed.), Types in Compilation. Proceedings, 2000. IX, 207 pages. 2001.

Vol. 2072: J. Lindskov Knudsen (Ed.), ECOOP 2001 – Object-Oriented Programming. Proceedings, 2001. XIII, 429 pages. 2001.

Vol. 2073: V.N. Alexandrov, J.J. Dongarra, B.A. Juliano, R.S. Renner, C.J.K. Tan (Eds.), Computational Science – ICCS 2001. Part I. Proceedings, 2001. XXVIII, 1306 pages. 2001.

Vol. 2074: V.N. Alexandrov, J.J. Dongarra, B.A. Juliano, R.S. Renner, C.J.K. Tan (Eds.), Computational Science – ICCS 2001. Part II. Proceedings, 2001. XXVIII, 1076 pages. 2001.

Vol. 2075: J.-M. Colom, M. Koutny (Eds.), Applications and Theory of Petri Nets 2001. Proceedings, 2001. XII, 403 pages. 2001.

Vol. 2076: F. Orejas, P.G. Spirakis, J. van Leeuwen (Eds.), Automata, Languages and Programming. Proceedings, 2001. XIV, 1083 pages. 2001.

Vol. 2077: V. Ambriola (Ed.), Software Process Technology. Proceedings, 2001. VIII, 247 pages. 2001.

Vol. 2078: R. Reed, J. Reed (Eds.), SDL 2001: Meeting UML. Proceedings, 2001. XI, 439 pages. 2001.

Vol. 2081: K. Aardal, B. Gerards (Eds.), Integer Programming and Combinatorial Optimization. Proceedings, 2001. XI, 423 pages. 2001.

Vol. 2082: M.F. Insana, R.M. Leahy (Eds.), Information Processing in Medical Imaging. Proceedings, 2001. XVI, 537 pages. 2001.

Vol. 2083: R. Goré, A. Leitsch, T. Nipkow (Eds.), Automated Reasoning. Proceedings, 2001. XV, 708 pages. 2001. (Subseries LNAI).

Vol. 2084: J. Mira, A. Prieto (Eds.), Connectionist Models of Neurons, Learning Processes, and Artificial Intelligence. Proceedings, 2001. Part I. XXVII, 836 pages. 2001.

Vol. 2085: J. Mira, A. Prieto (Eds.), Bio-Inspired Applications of Connectionism. Proceedings, 2001. Part II. XXVII, 848 pages. 2001.

Vol. 2086: M. Luck, V. Mařík, O. Stěpánková, R. Trappl (Eds.), Multi-Agent Systems and Applications. Proceedings, 2001. X, 437 pages. 2001. (Subseries LNAI).

Vol. 2089: A. Amir, G.M. Landau (Eds.), Combinatorial Pattern Matching. Proceedings, 2001. VIII, 273 pages. 2001.

Vol. 2091: J. Bigun, F. Smeraldi (Eds.), Audio- and Video-Based Biometric Person Authentication. Proceedings, 2001. XIII, 374 pages. 2001.

Vol. 2092: L. Wolf, D. Hutchison, R. Steinmetz (Eds.), Quality of Service – IWQoS 2001. Proceedings, 2001. XII, 435 pages. 2001.

Vol. 2093: P. Lorenz (Ed.), Networking – ICN 2001. Proceedings, 2001. Part I. XXV, 843 pages. 2001.

Vol. 2094: P. Lorenz (Ed.), Networking – ICN 2001. Proceedings, 2001. Part II. XXV, 899 pages. 2001.

Vol. 2095: B. Schiele, G. Sagerer (Eds.), Computer Vision Systems. Proceedings, 2001. X, 313 pages. 2001.

Vol. 2096: J. Kittler, F. Roli (Eds.), Multiple Classifier Systems. Proceedings, 2001. XII, 456 pages. 2001.

Vol. 2097: B. Read (Ed.), Advances in Databases. Proceedings, 2001. X, 219 pages. 2001.

Vol. 2098: J. Akiyama, M. Kano, M. Urabe (Eds.), Discrete and Computational Geometry. Proceedings, 2000. XI, 381 pages. 2001.

Vol. 2099: P. de Groote, G. Morrill, C. Retoré (Eds.), Logical Aspects of Computational Linguistics. Proceedings, 2001. VIII, 311 pages. 2001. (Subseries LNAI).

Vol. 2105: W. Kim, T.-W. Ling, Y-J. Lee, S.-S. Park (Eds.), The Human Society and the Internet. Proceedings, 2001. XVI, 470 pages. 2001.

Vol. 2106: M. Kerckhove (Ed.), Scale-Space and Morphology in Computer Vision. Proceedings, 2001. XI, 435 pages. 2001.

Vol. 2110: B. Hertzberger, A. Hoekstra, R. Williams (Eds.), High-Performance Computing and Networking. Proceedings, 2001. XVII, 733 pages. 2001.

Vol. 2118: X.S. Wang, G. Yu, H. Lu (Eds.), Advances in Web-Age Information Management. Proceedings, 2001. XV, 418 pages. 2001.

Vol. 2119: V. Varadharajan, Y. Mu (Eds.), Information Security and Privacy. Proceedings, 2001. XI, 522 pages. 2001.

Vol. 2121: C.S. Jensen, M. Schneider, B. Seeger, V.J. Tsotras (Eds.), Advances in Spatial and Temporal Databases. Proceedings, 2001. XI, 543 pages. 2001.

Vol. 2126: P. Cousot (Ed.), Static Analysis. Proceedings, 2001. XI, 439 pages. 2001.

Table of Contents

A Few Thoughts on E-Commerce
Keynote Lecture

Yacov Yacobi

Microsoft Research, USA

Abstract. I discuss a few notions related to e-commerce, such as: trust, privacy, and the economies of piracy and anti-piracy.

Trust

We have been using the term trust without any quantification for a long time. We need a technical term that will capture some of its meaning and enable quantification. The parallel may be Shannon's quantification of Information. It does not capture all of the meaning of information, but is useful enough. I suggest equating the amount of trust that a system needs with the value that this system is supposed to protect. It seems to me that we cannot get around this. We may push trust in different directions, we may distribute it, but we cannot do without it. For example, one important difference between symmetric and asymmetric key cryptography, is that the latter assigns trust to potentially more trustworthy entities.

Privacy

ID theft is the major issue; much more so than exposure of shopping patterns. ID-theft occurs when somebody issues a credit card on my name, max it out, and disappears, leaving me with the tedious task of salvaging my credit profile (most of the $$ damage is eaten by the credit card company). It happens because today when we want to prove that we know some secret, we expose it. The annual dollar amount in damages is already in many Billions, and rapidly increasing.

Public Key cryptosystems make it possible to prove knowledge of secrets without exposing them. Widespread deployment of PKI will solve most of this problem.

But the privacy issue that gets the headlines is exposure of shopping patterns. Long ago we traded this kind of privacy for credit. Credit card companies know what, where and when we buy, in real time. They can trace us better than the KGB in their heydays could trace citizens of the Soviet Union. We could use cash and avoid it, but we overwhelmingly chose the convenience of credit. Later we chose to trade even more of our location privacy, for mobility. The cell phone companies can now trace our physical location to within a few hundred feet on a continuous basis.

V. Varadharajan and Y. Mu (Eds.): ACISP 2001, LNCS 2119, pp. 1–2, 2001.

Now we have to choose a tradeoff between privacy and bandwidth. The bandwidth bottleneck is in our heads; there is only so much that we can absorb in a day. Some knowledge of our shopping patterns can help in targeted ads that will alleviate this bottleneck. My bet is that if done well, and if users are free to choose, most of them will choose to trade some privacy for this service.

On the Economies of Piracy and Anti-piracy

We consider the following players in the piracy game: Defense and offense which is further subdivided into transmitters and receivers of piracy. We assume that all the players are economically rational, and try to maximize their profits. With each player we associate an inequality of the general type costs ¡ profits. We scale the inequality per a client machine. Let v denote the average aggregate value of protected objects on a client machine. Each offense player has a different cost of attack per machine, which is compared to v. A system for which the inequality holds for every player is sound. We consider active and passive protected objects (SW and content, respectively). We consider two types of protecting systems: open and closed systems. The former can run protected and unprotected objects. The latter runs only protected objects. A non-protecting system is promiscuous.

Napster-like systems are covered in the sense that if the Napster offense were economically motivated (either receivers or transmitters) then sound systems would deter them. Offenders who are not economically motivated (vandals) would not be deterred by a sound system no matter what the delivery mechanism is. We outline a few open problems on the way to sound anti-piracy systems.

New CBC-MAC Forgery Attacks

Karl Brincat*[1] and Chris J. Mitchell[2]

[1] Visa International EU, PO Box 253, London W8 5TE, UK,
brincatk@visa.com

[2] Information Security Group, Royal Holloway, University of London, Egham, Surrey
TW20 0EX, UK,
c.mitchell@rhul.ac.uk

Abstract. This paper is concerned with a particular type of attack against CBC-MACs, namely *forgery attacks*, i.e. attacks which enable an unauthorised party to obtain a MAC on a data string. Existing forgery attacks against CBC-MACs are briefly reviewed, together with the effectiveness of various countermeasures. This motivates the main part of the paper, where a family of new forgery attacks are described, which raise serious questions about the effectiveness of certain countermeasures.

1 Introduction

1.1 Use of MACs

MACs, i.e. *Message Authentication Codes*, are a widely used method for protecting the integrity and guaranteeing the origin of transmitted messages and stored files. To use a MAC it is necessary for the sender and recipient of a message (or the creator and verifier of a stored file) to share a secret key K, chosen from some (large) keyspace. The data string to be protected, D say, is input to a MAC function f, along with the secret key K, and the output is the MAC. We write MAC $= f_K(D)$. The MAC is then sent or stored with the message.

1.2 A Model for CBC-MACs

MACs are most commonly computed using a block cipher in a scheme known as a CBC-MAC (for *Cipher Block Chaining* MAC). This name derives from the CBC 'mode of operation' for block ciphers, and a CBC-MAC is computed using the same basic process. There are several variants of the CBC-MAC, although the following general model (see [1,9]) covers most of these.

The computation of a CBC-MAC on a bit string D using a block cipher with block length n, uses the following six steps.

1. *Padding.* The data string D is subjected to a padding process, involving the addition of bits to D, the output of which (the *padded string*) is a bit string of length an integer multiple of n (say qn).

[*] The views expressed in this paper are personal to the author and not necessarily those of Visa International

V. Varadharajan and Y. Mu (Eds.): ACISP 2001, LNCS 2119, pp. 3–14, 2001.

2. *Splitting.* The padded string is divided (or 'split') into a series of n-bit blocks, $D_1, D_2, \ldots, D_q$.
3. *Initial transformation.* Initial transformation I, which may be key-controlled, is applied to D_1 to give the first *chaining variable* H_1, i.e.

$$H_1 = I(D_1).$$

4. *Iteration.* Successive chaining variables are computed as

$$H_i = e_K(D_i \oplus H_{i-1})$$

for $i := 2, 3, \ldots, q$, where, as throughout, K is a block cipher key, $e_K(X)$ and $d_K(X)$ denote block cipher encryption and decryption of block X with key K, and $\oplus$ denotes bit-wise exclusive-or of blocks.
5. *Output transformation.* The n-bit *Output block* G is computed as

$$G = g(H_q)$$

where g is the output transformation (which may be key-controlled).
6. *Truncation.* The MAC is set equal to the leftmost m bits of G.

Most CBC-MACs adhere to this model, and such MACs will be the main focus of this paper.

1.3 Types of CBC-MAC Scheme

The latest version of the relevant international standard, namely ISO/IEC 9797-1, [1], contains six different CBC-MAC variants. These are based on combinations of two Initial transformations and three Output transformations.

- Initial transformation 1 is defined as:

$$I(D_1) = e_K(D_1)$$

where K is the same key as used in the Iteration step. I.e. Initial transformation 1 is the same as the Iteration step, and is the one used in both the original CBC-MAC, as defined in ANSI X9.9, [4], and CBC-MAC-Y (also known as the *ANSI Retail MAC*), standardised in ANSI X9.19, [3].
- Initial transformation 2 is defined as:

$$I(D_1) = e_{K''}(e_K(D_1))$$

where K is the same key as used in the Iteration step, and K'' is a block cipher key distinct from K.
- Output transformation 1 is defined as:

$$g(H_q) = H_q,$$

i.e. Output transformation 1 is the identity transformation, and is the one used in the original CBC-MAC, [4].