Tagungsband zum 10. Kryptotag

Workshop der Fachgruppe Angewandte Kryptologie in der Gesellschaft für Informatik
Arbeitsgruppe Algebra und Zahlentheorie,
Technische Universität Berlin,
Fakultät II, Institut für Mathematik

20. März 2009

Inhaltsverzeichnis

Some Observations on Reusing One-Time Pads within Dice Codings

Sebastian Pape

Databases and Interactive Systems Research Group
University of Kassel

In [D08] a Visual Cryptography System for internet banking based on Dice Codings was presented. In this system each user has a key-transparency, working as a One-Time Pad, which allows him to decrypt the ciphertext. Key-transparency, ciphertext and plaintext consist of ten segments each with nine points. Decryption is done pointwise. Points of the key-transparency are linked by a 'NOT XOR' function with their respective ciphertext's counterparts and decrypt to a 'point' or 'no point' plaintext. Since each segment consists of nine 'points' or 'no points' digits from '0' to '9' can be represented by a plaintext segment.

If the key-transparency is used multiple times, we show that conclusions about it can be drawn. More precisely, the scope of key-transparencies can be reduced to the one used and its inverse. Our attack makes use of the fact, that each plaintext has to consist of all digits from '0' to '9'. Thus, plaintexts which include the same digit twice are invalid. Therefore, we are able to exclude key-transparencies which would decrypt to an invalid plaintext.

Since two segments can be attacked independently from the remaining eight segments, our proof of concept code only attacks two segments. 20 000 iterations suggest that 70 (90) key-transparencies are sufficient for our attack in more than 60 (95) percent. Since the proof of concept code does not make use of all information included in the observed ciphertexts, we claim that several improvements are possible.

Statistical observations show that the Visual Cryptography System presented in [D08] can be advanced by adding redundant segments. In the original system more than 18 percent of the possible plaintexts contain the same digit twice and, thus, are invalid. By adding two redundant segments it is possible to reduce the number of invalid keys below one percent. This countermeasure reduces the amount of information given per ciphertext sufficiently to counter our attack.

In the talk we discuss our attack and its improvements and we propose a simple improvement of the Visual Cryptography System presented in [D08], which counters our attack.

References

[D08] Denise Doberitz. Complete Codings for Visual Cryptography. 9. Kryptotag, Gelsenkirchen, November 2008.

Algebraic Attacks against Linear RFID Authentication Protocols

Matthias Krause and Dirk Stegemann

Theoretical Computer Science
University of Mannheim
Mannheim, Germany

RFID (radio frequency identification) tags are small devices that are equipped with only little memory and computational power. Their main application is the identification of objects, e.g., items in a shopping basket or clothes in a washing machine. Particularly, they present identification information upon a reader's request. In order to prevent cloning and tracing attacks and to preserve the tagged object's privacy, RFID tags should reveal their identities only to legitimate readers. Since most practically relevant RFID tags are too weak to execute standard authentication protocols, alternative measures are necessary. Besides technical approaches based on blocking or disturbing the communication, light weight authentication protocols and corresponding security models are intensively discussed (see, e.g., [3, 5]). One of the most promising proposals is the HB^+ protocol by Juels and Weis [4], which currently seems secure for several RFID applications, but is too slow for many practical settings.

As a possible alternative, authentication protocols based on choosing random elements from L secret n-dimensional linear subspaces of $GF(2)^{n+k}$ (so called linear (n,k,L)-protocols), have been considered. In these protocols, the secret key (the identification information in the RFID tag) consists of the specification of L n-dimensional linear subspaces $V_1,\ldots,V_L$ of $GF(2)^{n+k}$. The prover (RFID tag) chooses a random $l \in \{1,\ldots,L\}$ and sends a random $w \in V_l$. Given a message $\tilde{w} \in GF(2)^{n+k}$, the verifier (RFID reader) accepts the proof if there is some $l \in \{1,\ldots,L\}$ such that $\tilde{w} \in V_l$

We show that to a certain extent, these protocols are vulnerable to algebraic attacks. Particularly, our approach allows to break Cichoń, Klonowski and Kutyłowski's CKK^2-protocol [1], a special linear $(n,k,2)$-protocol, for practically recommended parameters by a polynomial time attack in less than a second on a standard PC, while an earlier (exponential time) attack requires a couple of hours [2]. Moreover, we show that even unrestricted (n,k,L)-protocols may be efficiently broken if L is too small.

References

[1] J. Cichoń, M. Klonowski, and M. Kutyłowski. Privacy protection for RFID with hidden subset identifiers. In *Proc. of Pervasive 2008*, volume 5013 of *LNCS*, pages 298–314. Springer, 2008.

[2] Z. Gołebięwski, K. Majcher, and F. Zagórski. Attacks on CKK family of RFID authentication protocols. In *Proc. Adhoc-now 2008*, volume 5198 of *LNCS*, pages 241–250. Springer, 2008.

[3] A. Juels. RFID privacy: A technical primer for the non-technical reader. In *Privacy and Technologies of Identity: A Cross-Disciplinary Conversation*. Springer, 2005.

[4] A. Juels and S. A. Weis. Authenticating pervasive devices with human protocols. In *Proc. of Crypto 2005*, volume 3621 of *LNCS*, pages 293–308. Springer, 2005.

[5] M. Langheinrich. A survey of RFID privacy approaches. In *Workshop on Ubicomp Privacy - Technologies, Users, Policy. Workshop at Ubicomp 2007*, 2007.

Yao's Millionaires' Problem in SMC-Systemen

Martin Franz
Technische Universität Darmstadt, Fachbereich Informatik
Security Engineering Group
Hochschulstrasse 10, D-64289 Darmstadt

Im Jahre 1982 legte Andrew C. Yao in [Ya82] den Grundstein für das was heute allgemein als Secure Multiparty Computation (SMC) bekannt ist. Yao zeigte, wie zwei Millionäre bestimmen können wer von beiden reicher ist, ohne selbst offenzulegen wieviel Vermögen sie jeweils besitzen. Seitdem erfreut sich SMC immer größerer Popularität und wurde in vielseiten Anwendungen eingesetzt. Während frühere SMC Systeme hauptsächlich mittels Boolscher Schaltkreise realisiert wurden, werden heute mehr und mehr SMC Systeme auf Homomorphen Chiffren basiert. Diese erlauben die Berechnung einer Funktion direkt mittels arithmetischen Operationen.

Bereits seit 1987 ist bekannt, dass jede berechenbare Funktion auch mittels SMC realisiert werden kann [GMW87]. Das Anwendungsspektrum moderner SMC Anwendungen reicht weit über das ursprüngliche Millionaires' Problem hinaus und es können Probleme mit mehreren 1000 teilnehmenden Parteien (wie z.B. in [DT08]) effizient gelöst werden.

In all diesen Anwendungen werden Instanzen von Yao's Problem gelöst. Während bereits viele effiziente Lösungen für das ursprüngliche Millionaires' Problem existieren (siehe z.B. [DGK07, GBV07]), stellt der Einsatz dergleichen die Entwickler von SMC-Protokollen vor neue Herausforderungen: Während in Yao's Fall jeder der zu vergleichenden Werte mindestens einer Partei bekannt ist, kommt es in SMC Systemen häufig vor, dass zwei Zwischenergebnisse miteinander verglichen werden sollen die keiner der teilnehmenden Parteien bekannt sind (und auch nicht offengelegt werden dürfen). Auch das Ergebnis eines solchen Vergleiches muss in SMC Systemen in der Regel geheim gehalten werden.

Im Vortrag werden Probleme aufgezeigt die beim Einsatz von Standard-Lösungen für Yao's Millionaires' Problem auftreten können. Weiter wird eine konkrete Lösung für ein Szenario mit zwei Parteien aufgezeigt.

Literatur

[Ya82] Andrew C. Yao. Protocols for Secure Computations.

[GMW87] O. Goldreich, S. Micali, A. Wigderson. How to play ANY mental game. Proceedings of the 19th annual ACM conference on Theory of computing, pp.218 - 229, January 1987.

[DT08] I. Damgard and T. Toft. Trading sugar beet quotas : secure multiparty computation in practice. ERCIM News, 73, 32-33.

[DGK07] I. Damgard, M. Geisler, M. Kroigaard. Efficient and Secure Comparison for On-Line Auctions. Proceedings of the Australasian Conference on Information Security and Privacy 2007.

[GBV07] J. Garay, B. Schoenmakers and J. Villegas. Practical and Secure Solutions for Integer Comparison. Public Key Cryptography - PKC ?07, 2007.

Mit Webtrust in den Browser

Ralph Knoche

FernUniversität in Hagen
Zentrum für Medien und IT (ZMI)

Die Certification Authority (CA) der FernUniversität in Hagen betreibt seit 2002 einen selbstentwickelten X.509v3 Zertifikatsserver, welcher auch erfolgreich vermarktet wird. Dieser Zertifikatsserver stellt SSL-Zertifikate für Studierende, Beschäftigte und Server aus. Anwendungsgebiete für diese Zertifikate sind beispielsweise die Online-Prüfungsauskunft der FernUniversität in Hagen oder die Nutzung von verschlüsseltem E-Mail-Verkehr. Insgesamt werden an der FernUniversität mehr als 50.000 Zertifikate verwaltet. Im Augenblick werden die SSL-Zertifikate mit einem CA-Zertifikat signiert, welches vom DFN-Verein (DFN-PCA Basic Policy) ausgestellt worden ist. Dies hat zur Folge, dass das CA-Zertifikat nicht in den gängigen Browsern implementiert ist. Nachteilig in diesem Vorgehen ist, dass das CA-Zertifikat manuell von jedem Benutzer in den Client-Browser installiert werden muss, bevor die ausgestellten Zertifikate als gültig angesehen werden. Eine Lösung für dieses Problem ist die direkte Integration des CA-Zertifikates in die gängigen Browser.

Als Voraussetzung für die Integration von Zertifikaten in Browsern wird die Webtrust-Zertifizierung angesehen. Die Webtrust-Zertifizierung wurde von der amerikanischen Vereinigung der Wirtschaftstreuhänder (AICPA) ausgearbeitet, um das Vertrauen in Internetseiten und von Zertifizierungstellen zu erhöhen. In Deutschland wird das Webtrust-Siegel durch Wirtschaftsprüfungsunternehmen verliehen. Die Webtrust-Zertifizierung stützt sich auf die „Webtrust Principles and Criteria“. Die dort aufgeführten Prinzipien sind den Bereichen „Security“, „Business Practices and Transaction Integrity“ und „Availability“ zugeordnet. Für den Erhalt der Webtrust-Zertifizierung ist die Erfüllung der „Principles and Criteria“ zwingend notwendig.

Die FernUniversität in Hagen entschloss sich im 2. Quartal 2007 solch eine Webtrust-Zertifizierung anzustreben. Nach einer Ausschreibungsphase erhielt ein Unternehmen der „Big-Four-Prüfungsgesellschaften“ den Zuschlag für die Durchführung einer Webtrust-Zertifizierung an der FernUniversität in Hagen.

In einem ersten Schritt verlangte der Wirtschaftsprüfer die Vorlage entsprechender Dokumentationen zum Thema Risikomanagement oder Change Management. Fehlende oder fehlerhafte Dokumente mussten verfasst und korrigiert werden. Nach dieser ersten Dokumentationsphase konnte im August 2007 der erste Vororttermin mit dem Wirtschaftsprüfer an der FernUniversität in Hagen stattfinden. Bei diesem einwöchigen Vororttermin wurden die Workflows und Geschäftsprozesse vom Einschreiben des Studierenden bis zur Ausstellung eines Zertifikats untersucht. Die Sicherheit des Zertifikatsservers im Hinblick auf Datensicherung, Datenarchivierung, logischer und physikalischer Zugang sowie das Keymanagement wurden begutachtet. Im Anschluss an diesen Vororttermin wurde ein erster Prüfbericht vom Wirtschaftsprüfungsunternehmen erstellt, der Schwachpunkte und Verbesserungsvorschläge erörtert.

Nachdem diese Schwachstellen von den Beschäftigten der Certification Authority (CA) beseitigt worden sind, kann die zweiwöchige Hauptprüfung zur Erteilung der Webtrust-Zertifizierung durchgeführt werden. Die Hauptprüfung findet im ersten Quartal 2009 statt, so dass im Wintersemester 2009 die FernUniversität in Hagen ein eigenes integriertes Root-Zertifikat besitzt.

Man sieht, dass das Implementieren und Betreiben einer eigenen Zertifizierungsinstanz Aufwand bedeutet. Jedoch wird dieser Aufwand um ein vielfaches erhöht, wenn für die Zertifizierungsinstanz die Herausforderung einer Webtrust-Zertifizierung angenommen werden soll. Denn erst eine Zertifizierungsinstanz mit Webtrust-Zertifizierung kann als vertrauenswürdig angesehen werden.

Computationally Secure Two-Round Authenticated Message Exchange

Henning Schnoor, Klaas Ole Kürtz, and Thomas Wilke

Christian-Albrechts-Universität zu Kiel, 24098 Kiel, Germany

A characteristic feature of web services is their restricted form of communication. These protocols only have two rounds: In the first round, a client sends a single message (request) to a server; in the second round, the server replies with a single message (response) containing the result of processing the request. A central security goal arising is that of authenticated message exchange: The server wants to be convinced that the request is new and originated from the alleged client, while the client wants to be convinced that the response originated from the intended server and is a response to his request.

The main objective of this paper is to provide a security model for such *two-round authenticated message exchange protocols (2AMEX protocols)* and to prove that a natural and practical protocol is computationally secure, assuming that the underlying signature scheme is resistant against existential forgeries.

A straight-forward approach to this problem is to use a signature scheme, and let servers store every message they have seen in order to avoid replay-attacks. In this paper, we show how to use timestamps in order to ensure security even with bounded memory (it is easy to see that timestamps, or a similar extension of the computational model, are necessary to achieve this goal). We only assume that each principal has access to a *local* clock, without any requirement of synchronization. We show that our protocol remains secure even when the adversary is given almost-complete control over all clocks in the system (we only disallow to decrease clock values), and when we allow the adversary to reset the memory of servers.

The fact that we want to devise a single protocol for implementing arbitrary services brings up the following issue. In contrast to what happens in traditional authentication protocols, say in authenticated key exchange (see, e. g., [BR93]), where the messages exchanged have a fixed format, we have to allow the messages exchanged to carry a so-called *payload*, which can be of arbitrary and to the authentication protocol unknown structure, in particular, we need to allow that a payload contains security-related data such as parts signed with the principals' private keys. Obviously, in order for the entire protocol to be secure such a use of private keys has to be restricted. To account for this, our protocol and security model is such that, on the one hand, the adversary is allowed to generate the payloads, but, on the other hand, he is only provided with a protocol-dependent signature oracle (rather than all private keys).

References

[BR93] M. Bellare and P. Rogaway. Entity authentication and key distribution. In D. Stinson, editor, *Advances in Cryptology – Crypto '93, 13th Annual International Cryptology Conference*, volume 773 of *Lecture Notes in Computer Science*, pages 232–249. Springer-Verlag, 1993.

Teilnehmer

Name	Einrichtung
Michael Beiter	Hewlett-Packard
Christoph Bayer	Technische Universität Berlin
Denise Doberitz	Ruhr-Universität Bochum
Martin Franz	Technische Universität Darmstadt
Sebastian Freundt	Technische Universität Berlin
Ramin Ghanipanah	Technische Universität Berlin
Jana Golze	Technische Universität Berlin
Florian Heß	Technische Universität Berlin
Olaf Horvath	InterComponentWare
Ralph Knoche	Fern Universität Hagen
Ronald Kraus	
Jakob Lell	Technische Universität Berlin
Daniel Löffler	Fern Universität Hagen
Maike Massierer	Technische Universität Berlin
Moritz Minzlaff	Technische Universität Berlin
Falk Nedwal	
Hannes Neumann	Technische Universität Berlin
Karsten Nohl	
Sebastian Pape	Universität Kassel
Stephan Pieper	
Yona Raekow	Fraunhofer-Institut
Daniel Reinert	Ruhr-Universität Bochum
Jeanette Schnake	Technische Universität Berlin
Hennig Schnoor	Universität Kiel
Jean-Pierre Seifert	Technische Universität Berlin
Heiko Stamer	Universität Kassel
Dirk Stegemann	Universität Mannheim
Patrick Stewin	Technische Universität Berlin
Erik Tews	Technische Universität Darmstadt
Osmanbey Uzunkol	Technische Universität Berlin
Christopher Wolf	Ruhr-Universität Bochum
Jochen Wargulski	Technische Universität Berlin

http://KryptoTag.de

Der Kryptotag ist eine zentrale Aktivität der GI-Fachgruppe „Angewandte Kryptologie“. Er ist eine wissenschaftliche Veranstaltung im Bereich der Kryptologie und von der organisatorischen Arbeit der Fachgruppe getrennt. Grundgedanke des Kryptotages ist, dass er inklusive Anreise wirklich nur einen Tag dauert und Nachwuchswissenschaftlern, etablierten Forschern und Praktikern auf dem Gebiet der Kryptologie die Möglichkeit bieten, Kontakte über die eigene Universität hinaus zu knüpfen.

Die Vorträge können ein breites Spektrum abdecken, von noch laufenden Projekten, die ggf. erstmals einem breiteren Publikum vorgestellt werden werden, bis zu abgeschlossenen Forschungsarbeiten, die zeitnah auch auf Konferenzen präsentiert wurden bzw. werden sollen oder einen Schwerpunkt der eigenen Diplomarbeit oder Dissertation bilden. Die eingereichten Abstracts werden gesammelt und als technischer Bericht veröffentlicht. Es handelt sich damit um eine zitierfähige Arbeit. Sie können von den Seiten der Fachgruppe herunter geladen werden.

Geplante Kryptotage

11. Kryptotag 30. November 2009, Universität Trier.

Bisherige Kryptotage

10. Kryptotag am 20. März 2009 Institut für Mathematik, Technische Universität Berlin. Kontakt: Florian Heß. 5 Einreichungen und 32 angemeldete Teilnehmer.
9. Kryptotag am 10. November 2008 Institut für Internet-Sicherheit, Fachhochschule Gelsenkirchen. Kontakt: MMarkus Linnemann. 5 Einreichungen und 24 angemeldete Teilnehmer.
8. Kryptotag am 11. April 2008 Universität Tübingen, WSI für Informatik, Diskrete Mathematik. Kontakt: Michael Beiter, Claudia Schmidt, Anja Korsten. 7 Einreichungen und 36 angemeldete Teilnehmer.
7. Kryptotag am 9. November 2007 Bonn-Aachen International Center for Information Technology. Kontakt: Michael Nüsken und Daniel Loebenberger. 9 Einreichungen und 36 angemeldete Teilnehmer.
6. Kryptotag am 19. Februar 2007. Universität des Saarlandes, Information Security and Cryptography Group und Sirrix AG. Kontakt: Michael Backes und Ammar Alkassar. 8 Einreichungen und 30 angemeldete Teilnehmer.
5. Kryptotag am 11. September 2006. Universität Kassel, Fachbereich Mathematik/Informatik, Theoretische Informatik. Kontakt: Heiko Stamer. 8 Einreichungen und 22 angemeldete Teilnehmer.
1. Kryptowochenende am 1.–2. Juli 2006. Tagungszentrum Kloster Bronnbach der Universität Mannheim. Kontakt: Frederik Armknecht und Dirk Stegemann. 14 Einreichungen und 21 angemeldete Teilnehmer.
4. Kryptotag am 11. Mai 2006. Ruhr Universität Bochum, Horst-Görtz Institut. Kontakt: Ulrich Greveler. 10 Einreichungen und 32 angemeldete Teilnehmer.
3. Kryptotag am 15. September 2005. Technische Universität Darmstadt, Theoretische Informatik. Kontakt: Ralf-Philipp Weinmann. 13 Einreichungen und 35 angemeldeten Teilnehmer.
2. Kryptotag am 31. März 2005. Universität Ulm, Abteilung für Theoretische Informatik. Kontakt: Wolfgang Lindner und Christopher Wolf. 10 Einreichungen und 26 angemeldeten Teilnehmer.

1. Kryptotag am 1. Dezember 2004. Universität Mannheim, Theoretische Informatik. Kontakt: Stefan Lucks und Christopher Wolf. 15 Einreichungen und 37 angemeldeten Teilnehmer.

Innerhalb der Fachgruppe für Angewandte Kryptologie sind Stefan Lucks (Universität Mannheim) und Christopher Wolf (K.U.Leuven, Belgien) verantwortlich für die Organisation der Kryptotage. Für eventuelle Rückfragen bitte an sie wenden.