REMOTE MANAGEMENT OF FACE-TO-FACE WRITTEN AUTHENTICATED THOUGH ANONYMOUS EXAMS

Giampaolo Bella
Software Technology Research Lab, De Montfort University, Leicester, U.K.
Dip. Matematica e Informatica, Università di Catania, Catania, Italy

Gianpiero Costantino
Istituto di Informatica e Telematica, CNR Pisa, Pisa, Italy

Lizzie Coles-Kemp
Information Security Group, Royal Holloway University of London, Egham, U.K.

Salvatore Riccobene
Dip. Matematica e Informatica, Università di Catania, Catania, Italy

Keywords: University exam, Public competition, e-Learning, Secret sharing, Exclusive OR.

Abstract: Authentication and anonymity are inherently difficult to combine. In case of face-to-face, written, university exams or public competitions, the candidates should be authenticated to prevent exchange of person, but the written exams they produce should be anonymous during the marking to ensure fairness of the marking. Complications rise still when the entire exam management should take place remotely, that is via the Internet, thus involving remote publication of marks and remote consultation/acceptance of those marks. This management would be useful, for example, also for the final, face-to-face, written exam concluding lectures delivered via electronic learning techniques. To our knowledge, no software currently exists beside ours to support this delicate combination of authentication and anonymity along with other typical exam preparation utilities.
WATA2.0 (Bella et al., 2009) supports the management of Written Authenticated Though Anonymous exams non-remotely, that is by having WATA2.0 run locally on the examiner's computer. Upgrading the system towards remote management turns out far from trivial because novel though fundamental security threats arise. These have required much more than SSL-secured connections to a remote WATA server: a complete redesign. In particular, the identity of a candidate is no longer matched to a written exam through identical barcodes but, rather, through barcodes that decrypt via exclusive-OR to the candidate's details. The new system, WATA3.0, is currently used at the University of Catania, and the migration from the previous version has been seamless. The innovative design of WATA3.0, its user experience, interface and implementation are presented.

1 INTRODUCTION

Modern societies incrementally base their wealth on actual people's merits, which are normally assessed through tests, exams or public competitions. Depending on the specific context, a specific terminology and method are adopted. For example, a student normally progresses towards a university Bachelor degree by sitting for an exam, which they fill in, and which is later marked by the lecturer.

The actual notification of the marks to the examinee can be done in various ways. The main ones are two: the examiner sets an appointment to meet the examinee in person and reveal the marks; or the marks are published on the Internet, as would be more appropriate, for example, for the remote management of the final, face-to-face, written exam concluding lectures delivered via e-learning techniques. In all cases,

Bella G., Costantino G., Coles-Kemp L. and Riccobene S..
REMOTE MANAGEMENT OF FACE-TO-FACE WRITTEN AUTHENTICATED THOUGH ANONYMOUS EXAMS.
DOI: 10.5220/0003481404310437
In *Proceedings of the 3rd International Conference on Computer Supported Education* (ATTeL-2011), pages 431-437
ISBN: 978-989-8425-50-8

the examiner knows the personal details (name, surname, etc.) of the examinees as well as which mark goes to which candidate. The examinees customarily accept the examiner's knowledge of such association.

However, knowledge of such association is often considered sensitive information, such as at public competitions towards a prestigious post. Also, undergraduates may feel that disclosing that information to an examiner cannot be accepted by their righteous privacy requirements. A potential practical implication of the disclosure is the examiner's unfair marking, which could ultimately hinder meritocracy. Hence the need for anonymity. By contrast, an anonymous exam sheet might invite cheating at the examinee's side, with a realistic chance of person exchange.

WATA is a system for written, authenticated though anonymous exams (Bella et al., 2009). It runs locally on the examiner's computer, and therefore has two main limitations: the notification of marks must be carried out classically, as outlined above; the system must be installed on the machine of each examiner who wishes to use it. These motivations convinced us to upgrading the system towards a remote platform, which any student interested in being notified his mark, or any examiner wishing to use its facilities might easily access.

However, we soon realised that making the system remotely available entails new threats. Not only are these due to the obvious need to securely communicate with a server, but also to the basic design becoming flawed when hosted on a remote platform. The main security requirement to meet is examinees' remote authentication, for at least two reasons. One is to avoid a clever examinee's selling his vote to other, possibly less skilled, examinees.

Another one is due to the fact that certain exam policies allow examinees to refuse marks till the moment these are notified. Hence an examinee can refuse his mark prior to knowing it, while "fail" marks may officially be accounted for throughout the rest of his studies. However, once marks are notified, they cannot be refused and are automatically registered. The gist of such an exam policy seems to be to favour examinees' self evaluation. Therefore, from our security perspective, lack of examinee authentication would allow an examinee to illegally register another examinee's mark on behalf of the latter. This would be a serious attack in case the latter examinee, possibly after pondering his answers, did not want to have his exam marked.

In consequence, in the new setting, the existing design of WATA, which was version 2.0, has to be disposed with entirely — more explanation will follow. Various ideas were tried out towards a new design, and the exclusive-or function was found to be the right technology. The main strength of the XOR is the symmetry of its truth table, while its drawback is cancellation of the key, which implies the need of fresh keys every time a new and robust ciphertext must be built. Barcodes were used in WATA2.0 to match an examinee's credentials to his exam sheet. Their use in the new version, which we name WATA3.0, is completely different: each barcode encodes either the encrypted version of a set of credentials or the key that must be used to decipher it.

This paper fully describes the latest version of our sytem, WATA3.0. A brief history of the previous versions (§2) introduces the design and user experience of WATA3.0 (§3). Then, the new interface (§4) and implementation (§5) are outlined. Some evaluation (§6) and conclusions (§7) close up.

2 A BRIEF HISTORY OF WATA

The original goal of WATA was to mechanise in a software the classical method of the *double envelope*, which is often used during open competitions. The examinee inserts his personal details in a small envelope, and seals it. He then inserts that envelope along with his anonymous, filled-in exam sheet in a bigger envelope. The examiner is trusted to mark the exam sheet prior to opening the smaller envelope, when the association of marks and examinee can be done.

WATA stores the exam questions in a database. It offers a printing facility to generate as many exam sheets as needed, with the required number of questions. These are randomly extracted from the database and shuffled further to ensure that no two identical exam sheets exist. A typical exam sheet can be seen in Figure 1. The *security token* on the left hand side must be filled in and signed by the examinee. The examiner checks this information to match the examinee's identification card and finally authenticates the token with his overlay signature and institution stamp, to make it physically tamperproof. The two occurrences of the same barcode can be noted. They will be used later to match personal details with marks.

The examinee finally tears off the token, hands in the anonymous manuscript and walks away with the token. The examiner will mark anonymous sheets and will organise a mark notification phase as outlined above. During that phase each examinee will hand in his token, whose barcode is scanned through an appropriate scanner, entered in WATA2.0 and matched to a mark that was stored previously: the examiner stored that mark during the actual marking phase next to a barcode scanned from an exam sheet. The only

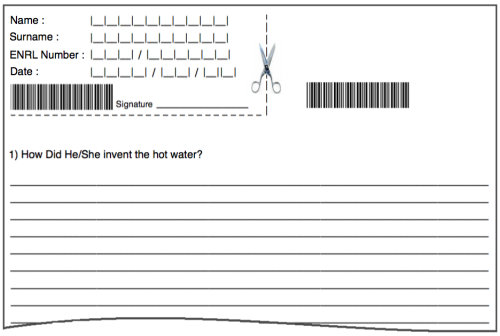

Figure 1: The exam sheet of WATA2.0.

real limitation of this system is against collusion of examinee and examiner.

These facilities were available in WATA1.0, which was written in Visual Basic and based on a Microsoft Access database. WATA2.0 (Bella et al., 2009) was a big step towards portability, being implemented in Java and over a MySQL database. However, it still had to run locally on the examiner's database.

We set out to make WATA remotely available. Examinee authentication was soon felt to be a must, otherwise a significant attack could see an examinee sell his mark. Another attack, already sketched, exists: WATA is accessible on a remote server; an examinee reads (by any means such as circumstances or theft) another examinee's barcode and enters it in the system. This is serious when it is the case that, while an examinee can decide to skip the notification phase renouncing to whatever mark and having the exam fees waived, an examinee who goes for the notification by handing his token over, cannot refuse the mark.

It is then clear why the design of WATA3.0, which works on a remote server and is immune to the previous attacks, is entirely new with respect to the design of the previous versions.

3 SPECIFICATION

We begin by describing the system requirements (§3.1) and continue by describing our solution to meet them (§3.2).

3.1 Requirements

3.1.1 System Requirements

- The entire system should be centralised on a machine that is maintained by an administrator.
- Both examiner and examinee should be able to access the system remotely and securely.

3.1.2 Examiner's Requirements

- Any number of examiners should be supported (subject to obvious machine speed/memory limitations).
- Each examiner should be able to register a number of exams, depending on exam subject/date.
- The examiner should then be allowed to upload the exam questions for each exam.
- It should be possible to upload questions interactively or as a batch in an ascii file with standard format.
- Exam questions should be securely stored in a remote database.
- A printing facility should allow the preparation of exam sheets in PDF format — any number of exam sheets, corresponding to the number of examinees, and any number of questions per sheet.
- Each exam sheet should be authenticated in the classical sense face-to-face.
- The marking facility should allow a mark to be stored for each exam sheet.
- The notification facility should allow marks to be securely accessible by their respective authors.
- Each examinee should be allowed to access his mark only or, at least, examinees should not be able to steal marks from each other or trade marks between each other.

3.1.3 Examinee's Requirements

- Each exam sheet should be anonymous when it is being marked.
- Notification should be remote.
- The same requirements about notification as the last two in the examiner's list.

3.2 Our Innovative Solution

The requirements set above can be met as described in the sequel of this section.

The system requirements can be met by hosting the WATA system on a remote and publicly accessible server, not necessarily of the institution hosting the exam. It can be assumed that the server is maintained by a dedicated administrator, as with all institutional servers. Access is done via HTTPS, which ensures that all communication is encrypted and secured via the SSL protocol. Each user registers with the server as is customary, gaining personal credentials for con-

fidential and authenticated access (this typically involves delivery of an initial password via email, and its change into a robust one at first login). This also meets the requirement for multi-user support, as the server stores the hashed versions of the passwords. Users are required to enter their role, such as 'examinee' or 'examiner', which the system can verify against an available list of examiners. This allows the system to present the right menu to each user.

3.3 Preparing the Exam Sheets

Exam registration and various forms of question upload can be achieved by equipping the server with a suitable database. The printing facility, including question re-use/re-shuffling, can be inherited from WATA2.0. However, contrarily to WATA2.0, it is no longer necessary to print the two occurrences of the same barcode, while the rest of the security token is unchanged.

The absence of the barcode simplifies the handling of the printed, blank exam sheets. They were grouped by a barcode in WATA2.0 such that an exam of three questions relied on three sheets with one question each, all having the same barcode. By contrast, WATA3.0 is dependable also against potential mixing of the unfilled exam question sheets before they are handed out to the examinees, because there exists no a priori sorting or relationship between them. This of course assumes that it is fine to ask the examinees random questions from the database.

As explained below, this simplification has some price in terms of complication of the exam experience for both parties.

3.4 Taking the Exam

The exam experience takes place as follows.

- The examiner has a laptop with connected printer.
- He feeds in the paper drawer of the printer the preprinted exam sheets using a prescribed orientation (see below).
- An examinee approaches the examiner's desk and hands his identity card over to the examiner.
- The examiner authenticates the examinee and feeds the latter's personal details (name, surname, matriculation/registration number, etc.) into the system. Alternatively, the examiner finds those details on a precompiled list of registered examinees, which may be available.
- WATA3.0 generates a random key, whose bit length matches that of the examinee's details, plus some randomness. This key is XOR-ed to the details, building the encrypted details. Key and corresponding ciphertext will be addressed as *shares* of the personal details for brevity.
- The key for each examinee is stored in the database next to the examinee's details.
- The corresponding ciphertext is *not* stored in the table to ensure anonymity during the marking phase. To remove the examinees' trust that this is actually the case, various software security measures ca be adopted, such as: publishing the code with its fingerprint to allow examinees' inspection; calculating the live fingerprint of the code used at the exam; check that the two match. In practice, we have realised that this trust issue is resolved by the examiner's using a machine belonging to a random examinee, inserting a (read-only) DVD with WATA3.0 in it, and using that machine for the rest of the process. A further level of protection from the host machine can be achieved by building a DVD with a virtual machine running WATA3.0.
- The printer then prints the key on each of the required sheets — three sheets, for example, if three questions are required per exam.
- The printer prints the corresponding ciphertext on the first exam sheet, exactly inside the security token. The ciphertext is then erased from memory.
- The examinee takes his exam sheets, walks away to fill in the security token as required, and complete the exam answers. He finally tears off the token and walks away with it, as with WATA2.0.

3.5 Marking the Exam Sheets

The marking phase is unchanged: the examiner scans the exam barcode and enters the corresponding mark. When finished, he publishes the results.

3.6 Notifying the Marks

The notification experience is now available to the examinees, and can be summarised as follows.

- An examinee logs into the system, and enters the barcode number of his token — in the assumption that barcode scanners are not widespread, the sytem can print the exadecimal version in the token so that it can be read and keyed in.
- The examinee is also required to enter his main personal details.
- After customary confirmation messages, the system reads the input, queries the database using the

personal details, and then gets the corresponding share.

- This is XOR-ed to the live share. If the outcome matches the personal details, then the vote is successfully registered, and a corresponding informative message is sent to the examinee. Otherwise, a notification of potential fraud is batched for the examiner, while a corresponding error message is sent of to the examinee.
- There exists a public time window for validity of the notification phase, such as one week. After the corresponding deadline, WATA3.0 disables the notification menu for all examinees. This is taken to mean that those who have not undergone notification wish to refuse the outcome.

It is clear that this system addresses the issue of examinees authentication. Even if security tokens are stolen or traded, no mark can be registered with the wrong personal details. A similar attempt would lead to failure of decryption of the personal details during the notification phase. All remaining requirements formulated above are therefore satisfied.

4 USER INTERFACE

The user interface for examiners features a simple menu, here omitted for brevity, with intuitive buttons described in the following.

For example, an 'Add Questions' button provides the various facilities for question upload, asking to enter a new exam name/date or select an existing one. A 'Print Exam Sheets' button opens up the printing facilities through the interface in Figure 2. The examiner can select the exam name among those for which questions are available — "Computer Security" in this case. It can be seen that the number of tests, and the number of questions per test can be entered. It can also be chosen whether to have a white page per question, for the examinee's convenience to fill in. Once a 'Create' button is clicked, the system invokes the underlying printing interface for either immediate printing or creation of a PDF file to print later.

A 'Build Shares' button opens up the menu to compute the two shares out of the examinee's full personal information (registration number alone for brevity in the current version). It can be seen in Figure 3. The two shares are treated as described in the previous Section, that is printed appropriately and respectively recorded and discarded. Text capture is forbidden to increase protection of the share that must be deleted. The risk of potential screen capture by an unfair examiner is minimised by the whole process

Figure 2: The printing interface.

taking place under the scrutiny of the examinee, who should be prevented from using mobile phone cameras. It was considered to increase public inspection by projecting the whole screen by a video projector, but this would impair the prevention of mobile phone picture taking. We have not yet evaluated examinees' response if the shares were not displayed at all, but directly sent off to the printer.

Figure 3: The sharing interface.

A 'Show Tables' buttons allows the examiner to interact with all existing tables through simplified interfaces. For example, he may like to search for a specific keyword in the question table, or delete a question. The same could be useful over the exam table after the marking phase. This is implemented behind the 'Mark Exam Sheets' button. It leads to the interface in Figure 4. It can be seen that the examiner can enter or scan the share from the exam sheet, and then select the appropriate mark — for example, "18" is the minimum required to pass in an Italian university. After selection, the mark can be saved. At completion

of the entire marking phase, the examiner may click "Publish Results" to enable the users registered with role of examinee to compute their marks.

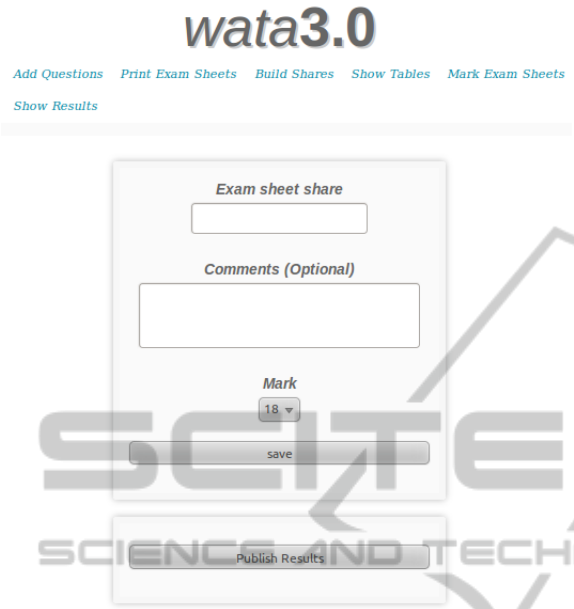

Figure 4: The marking interface.

When the deadline for notification validity has passed, the examiner can inspect which examinee has had his vote registered by clicking on 'Show Results'.

The examinee menu is simple, hence omitted here: a 'Notification' button allows the examinee to enter his personal details and share, and then outputs the corresponding mark, which is definitively registered.

5 IMPLEMENTATION

WATA3.0 is currently hosted on an Apache server with support enabled for OpenSSL. It is then entirely written in PHP and Javascript, and continues to rely on a MySQL database.

The structure of the database is the obvious one, with tables storing users with their roles, exam names, exam questions, and exam marks. The PHP code prescribes frequent accesses to the MySQL database. These can be made transparent by storing the credentials of the MySQL user 'wata' in a dedicated file, called 'wata.conf.php'. This choice may seem questionable in terms of security, but the WATA administrator will keep those files in his own disc quota.

A flavour of the implementation can be obtained by looking at the following Javascript fragments. Figure 5 shows two example functions. Function 'SecretSharing.prototype.randomString' returns an array of given length containing random bits. It will be invoked to generate the random key share by function 'SecretSharing.prototype.encode'. This computes the ciphertext share by bitwise XOR-ing the key share to the personal details given as input. It can be seen that if finally returns the share pair.

```
SecretSharing.prototype.encode = function(inText) {
    var len = inText.length;
    var share1 = this.randomString(len);
    var share2 = new Array(len);

    for (var i=0 ; i<len ; i++) {
        share2[i] = String.fromCharCode(share1.charCodeAt(i) ^
                                        inText.charCodeAt(i));
    }
    return [this.codec.encode(new String(share1)).replace('=',''),
            this.codec.encode(
                new String(share2.join(''))).replace('=','')];
    }


SecretSharing.prototype.randomString = function(length) {
    var a = new Array(length);
    for (i=0 ; i<length ; i++)
        a[i] = String.fromCharCode(Math.floor(Math.random()*256));
    return a.join('');
}
```

Figure 5: Two Javascript functions used in WATA3.0.

6 EVALUATION

WATA2.0 was released under the Creative Commons licence, "Attribution Non-Commercial No Derivatives". It has vastly been adopted at the Department of Mathematics and Informatics of the University of Catania since 2004. The migration to WATA3.0, which took place at the beginning of the present academic year, has been seamless. The students reported no irregularity and enthusiastically engaged with the web service. It is expeceted that the remote availability of a service such as WATA3.0 can only favour its acceptance and international diffusion.

WATA offers a rather unique service, hence the limited related work to the previous version (Bella et al., 2009). To the best of our knowledge, the present version seems to have none, which explains the very short bibliography. Moreover, WATA is under continuous development. Future work includes the implementation of additional roles for other members of the examining committe or for third-party inspectors.

7 CONCLUSIONS

WATA3.0 has been fully redesigned with respect to the previous version to become a web service. It can the be claimed that written exams can be now managed remotely, from sheet preparation to notification

and registration, while ensuring authentication of the examinees and anonymity during the marking.

ACKNOWLEDGEMENTS

We are grateful to Stefano D'amico and Giuseppe Gurgone for helping with the implementation.

REFERENCES

Bella, G., Costantino, G., and Riccobene, S. (2009). A system for written authenticated though anonymous exams. In Cordeiro, J. and B.Shishkov, editors, *Proc. of the 2nd International Conference on Computer Supported Education (CSEDU09)*, page 132 137. INSTICC Press.