Marcin Gogolewski, Michał Ren, Łukasz Nitschke, Tomasz Tyksiński

Bezpieczne systemy zdalnego egzaminowania w e-learningu i gospodarce opartej na wiedzy

Ekonomiczne Problemy Usług nr 68, 204-212

2011

ZESZYTY NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO

NR 651 EKONOMICZNE PROBLEMY USŁUG NR 68 2011

MARCIN GOGOLEWSKI, MICHAŁ REN, ŁUKASZ NITSCHKE
Uniwersytetu im. Adama Mickiewicza
TOMASZ TYKSIŃSKI
Wyższa Szkoła Nauk Humanistycznych i Dziennikarstwa w Poznaniu

BEZPIECZNE SYSTEMY ZDALNEGO EGZAMINOWANIA W E-LEARNINGU I GOSPODARCE OPARTEJ NA WIEDZY

Wprowadzenie

Rosnące wymagania wobec pracowników, pojawiające się głównie w sektorze nowych technologii, powodują konieczność budowania różnego rodzaju programów certyfikacji (obsługa systemów zarządzania, znajomość języków obcych, znajomość podstawowych leków w przypadku lekarzy czy choćby certyfikowanie umiejętności podstawowej obsługi komputera – ECDL), kształcenia ustawicznego i wielu innych działań, których wspólnym elementem jest proces przeprowadzania egzaminu. W wielu przypadkach to właśnie egzamin jest najbardziej kosztownym i kłopotliwym z organizacyjnego punktu widzenia elementem całego procesu, gdyż wymaga czasu na dojazd, miejsca oraz odpowiedniego nadzoru. Oczywiście każdy proces egzaminowania może być obarczony także innymi niedoskonałościami, takimi jak faworyzowanie przez przeprowadzających egzaminy jednych grup studentów kosztem innych czy nawet „sprzedawanie" różnego rodzaju certyfikatów przez pracowników organizacji egzaminujących. W niniejszym artykule będziemy używali określenia „student" wobec wszystkich egzaminowanych (bez względu na to, czy będą to istotnie studenci, czy pracownicy lub uczniowie).

Jako panaceum na część wymienionych problemów chcielibyśmy zaproponować egzaminy, które mogą być przeprowadzane w sposób elektroniczny na stanowiskach pracy (zakładając oczywiście, że wyposażone są one w niezbędny sprzęt) bądź nawet na prywatnym komputerze pracownika w miejscu jego zamieszkania. Egzaminy takie są już pilotażowo przeprowadzane w niektórych szkołach, a koszt

ich wprowadzenia jest stosunkowo niewielki w porównaniu z korzyściami, które można osiągnąć. Wystarczy wspomnieć, że istniejące już systemy pozwalają na anonimowe zdawanie egzaminów (egzaminator nie może zidentyfikować studenta), a cały proces, od tworzenia pytań, poprzez ich publikację, zdawanie egzaminu i ocenę aż do ogłoszenia wyników, jest dokładnie rejestrowany, by umożliwić jego kontrolę także w późniejszym terminie.

1. Podstawowe pojęcia

W celu głębszego zrozumienia systemu potrzebujemy określić kilka podstawowych pojęć pojawiających się w dalszej części artykułu. W przypadkach gdy tłumaczenie mogłoby być wieloznaczne, podajemy wersję oryginalną. We wszystkich proponowanych rozwiązaniach występują (czasami pod nieco innymi nazwami) co najmniej następujące role:

- *student* – osoba zdająca egzamin; zakładamy, że może być nieuczciwy i próbować wykorzystać zarówno luki w samym systemie, jak też stosować nieuczciwe praktyki będące poza kontrolą systemu;
- *nauczyciel* – sprawdza egzaminy i wystawia oceny; w niektórych systemach jest także odpowiedzialny za przygotowanie pytań; zwykle, podobnie jak w przypadku studenta, nie zakładamy, że zawsze jest uczciwy, i uwzględniamy w systemie pewien stopień kontroli;
- *zarządzający egzaminem* (*exam authority*) – zaufany uczestnik pośredniczący w komunikacji pomiędzy studentem a nauczycielem; zakres jego kompetencji różni się znacznie w różnych systemach.

Poza podstawowymi rolami, służącymi do przedstawienia działania systemu, konieczne okazuje się także określenie pewnych wspólnych wymagań dotyczących systemów egzaminowania:

- *autentyczność* (*authenticity*) – na każdym etapie egzaminu niezbędne jest zapewnienie autoryzacji zarówno studentów i nauczycieli, jak też samego systemu. W szczególności należy sprawdzić, czy np. student może zdawać dany egzamin, a nauczyciel ma uprawnienia do przeprowadzania egzaminów z danego przedmiotu[1, 2, 3];
- *tajność* (*secrecy*) – pytania, poprawne odpowiedzi, a także odpowiedzi udzielone przez studentów muszą być utrzymane w tajemnicy przez cały

[1] J. Castella-Roca, A. Dorca-Josa, J. Herrera-Joancomarti: *A Secure E-Exam Management System*, ARES 2006, s. 864–871.

[2] A. Huszti, A. Petho: *A Secure Electronic Exam System*, 2008, www.inf.unideb.hu/~pethoe/cikkek/4682-Huszti-Petho.pdf

[3] I. Jung, H. Yeom: *Enhanced Security for Online Exams Using Group Cryptography*, IEEE Transactions on education 2009, vol. 52, no. 3.

okres trwania egzaminu (a zwykle nawet dłużej; czasami lepiej nawet nie przechowywać odpowiedzi udzielanych przez studentów po zakończeniu procesu weryfikacji i ewentualnej procedury odwoławczej)[4, 5];

- *odporność na oszustwa* (*copy prevention and detection*) – wymaganie to jest czasami nazywane także *kontrolą (monitoring)* – brane pod uwagę są różnego rodzaju oszustwa[3]:
  - zdawanie egzaminu przez inną osobę (podszywanie się),
  - pomaganie egzaminowanemu w trakcie egzaminu,
  - konsultowanie odpowiedzi z innymi egzaminowanymi,
  - używanie nieautoryzowanych materiałów,
  - przechwytywanie lub zakłócanie komunikacji pomiędzy egzaminowanym a systemem;
- *integralność* (*integrity*) – konieczne jest sprawdzenie zarówno pytań, jak i odpowiedzi pod kątem nieautoryzowanych modyfikacji (zmiany udzielonych odpowiedzi po zakończeniu egzaminu czy ingerencji w same pytania);
- *dostępność* (*accessibility*) – wymagania dotyczące sprzętu czy lokalizacji nie powinny być ograniczające[6], niektóre podejścia umożliwiają przystępowanie do egzaminu z prywatnego komputera, bez ograniczenia co do lokalizacji;
- *anonimowość* (*anonymity*) – niektóre rozwiązania[7] zakładają, że student nie wie, kto jest egzaminatorem, a egzaminator nie ma informacji o tym, którego studenta odpowiedzi sprawdza;
- *rozproszone zaufanie* (*distributed trust*) – tym pojęciem określamy sytuację, w której żaden (z wielu) zarządzający nie ma pełnej informacji o systemie, np. żaden nie zna przypisania studentów do egzaminatorów;
- *niezawodność* (*robustness*) – wymaganie z pracy[8] – funkcjonalnie prawie identyczne z pojęciem integralności z pracy[9], ale bez uwzględnienia ograniczenia liczby podejść studenta do tego samego egzaminu;
- *potwierdzenie* (*receipt*) – student po zakończeniu egzaminu otrzymuje potwierdzenie wysłania odpowiedzi[10];

---

4 A. Huszti, A. Petho: *A Secure Electronic…*, *op. cit.*

5 I. Jung, H. Yeom: *Enhanced Security…*, *op. cit.*

6 *Ibidem.*

7 A. Huszti, A. Petho: *A Secure Electronic…*, *op. cit.*

8 *Ibidem*.

9 I. Jung, H. Yeom: *Enhanced Security…*, *op. cit.*

10 *Ibidem*.

- *poprawność* (*correctness*) – oznacza sprawdzenie, czy student nie próbuje podejść jeszcze raz do tego samego egzaminu (po skasowaniu poprzednich wyników);
- *niewypieralność* (*non-repudiation*) – własność zapewniająca, że wykonawca pewnej czynności (np. podpisu) nie może się jej wyprzeć, nawet jeżeli byłoby to w jego interesie (np. w większości schematów podpisu nie można rozróżnić czy podpis jest oryginalny, czy został podrobiony przez osobę o wystarczającej mocy obliczeniowej – w tym przypadku chcielibyśmy móc rozróżnić poprawny podpis sfałszowany od poprawnego oryginalnego).

Część powyższych wymagań można spełnić, wykorzystując metody kryptograficzne. Praktycznie wszystkie proponowane i implementowane rozwiązania zdalnego egzaminowania wymagać będą różnych metod zabezpieczania przesyłanych danych oraz sprawdzania tożsamości egzaminowanych osób z jednoczesnym zachowaniem ich anonimowości na etapie sprawdzania egzaminów przez egzaminatorów. Należy też zapewnić integralność danych przesyłanych w trakcie zdawania egzaminu oraz potwierdzić autentyczność osoby zdającej nie tylko w momencie rozpoczęcia egzaminu, lecz również w czasie trwania całego egzaminu.

Samo zabezpieczanie przesyłanych danych jest już standardem w dobie elektronicznego społeczeństwa. W sposób w miarę prosty jesteśmy w stanie, używając np. standardowego szyfrowania danych (AES), przesłać dane bezpiecznym kanałem, zaszyfrowane tajnym kluczem. W tym przypadku wspólny klucz służy zarówno do szyfrowania, jak i do odszyfrowywania danych. Nieco trudniejszą sprawą jest samo ustanowienie takiego kanału. Klucz służący do szyfrowania przesyłanych danych musi zostać rozesłany do wszystkich uczestników protokołu. Do tego celu wykorzystywane są szyfry asymetryczne (często wraz z infrastrukturą klucza publicznego opisaną w ustawie o podpisie elektronicznym – DzU 2001, nr 130, poz. 1450, z późniejszymi zmianami i rozporządzeniami wykonawczymi) lub dedykowany protokół Diffie–Hellmanna służący do tworzenia klucza sesyjnego[11].

Szyfry asymetryczne wykorzystują pary kluczy, z których jeden – publiczny jest ogólnodostępny, drugi – prywatny, trzymany w sekrecie. W celu rozdystrybuowania uprzednio wygenerowanego klucza sesyjnego dla pewnego szyfru symetrycznego rozsyłana jest jego zaszyfrowana kluczem publicznym wartość. Gwarantuje nam to, że jedynie dany odbiorca, posiadający odpowiedni klucz prywatny, będzie w stanie poznać jego wartość. Przy takim podejściu przyjmujemy, że klucz sesyjny jest tworzony wyłącznie u nadawcy. Można zwiększyć bezpieczeństwo tworzenia kluczy sesyjnych poprzez współtworzenie ich przez obie strony bezpiecznego kanału. Metoda ta, znana jako protokół Diffie–Hellmanna, polega na

[11] P. Oorschot, A. Menezes, S. Vanstone: *Handbook of Applied Cryptography*, CRC Press, Boca Raton, FL, USA 1996.

naprzemiennej wymianie części klucza sesyjnego, ukrytych przed niepowołanymi osobami. Po zakończeniu protokołu obie strony mogą zrekonstruować wspólną wartość klucza sesyjnego, a zarazem na podstawie przesyłanych danych nikt inny nie jest w stanie ich wyznaczyć.

Parę kluczy szyfru asymetrycznego można również wykorzystać do potwierdzania autentyczności źródła wysyłanej wiadomości. Dodając do wiadomości podpis elektroniczny złożony z wykorzystaniem klucza prywatnego, odbiorca, wykorzystując publiczny klucz nadawcy, może zweryfikować, czy rzeczywiście wiadomość została wysłana przez oczekiwanego użytkownika, a zarazem (w odróżnieniu od klasycznego podpisu odręcznego) może sprawdzić autentyczność otrzymanej wiadomości. Uzyskujemy w ten sposób własność integralności przesyłanych danych.

Ważne z punktu bezpieczeństwa jest również potwierdzanie autentyczności klucza publicznego. Realizowane jest to poprzez hierarchiczną strukturę urzędów certyfikujących takie klucze. Potwierdzone dane są podpisywane przez urząd certyfikujący. Powyższą hierarchę nazywamy infrastrukturą klucza publicznego (PKI). Dodatkowo, dzięki zastosowaniu kluczy publicznych i szyfrowania przez wiele tzw. serwerów mieszających, możliwe jest stworzenie sieci mieszającej pozwalającej przesyłać anonimowo wiadomości. Anonimowość mogą zapewnić systemy MIX-serwerów, znane m.in. z prac dotyczących wyborów elektronicznych[12].

2. Metody oszustwa

Jak można się domyślić, zdalna edukacja daje wiele możliwości oszustwa na testach, przy zadaniach domowych itp. Każdy nauczyciel i uczeń wie, że edukacja tradycyjna również w takie możliwości obfituje. Motywacją studenta jest najczęściej chęć uniknięcia wysiłku i zaoszczędzenia czasu związanego z opanowaniem danego materiału czy zrobieniem danego zadania. Niestety, problem ściągania jest bardzo powszechny i szeroko akceptowany – powinien być traktowany jak coś niemoralnego, a dochodzi nawet do tego, że pisane są poradniki, jak oszukiwać. W szkołach średnich 97% uczniów deklaruje, że widziało, jak koledzy i koleżanki ściągali[13]. Co więcej, odsetek ściągających na przestrzeni ostatnich dekad stale wzrasta[14].

---

[12] D. Chaum: *Secret-ballot: True voter verifiable elections*, IEEE Security and Privacy 2004, vol. 2, s. 38–47.

[13] G. Clabaugh, E. Rozycki: *Preventing Plagiarism & Cheating, An Instructor's Guide*, 2nd ed., NewFoundations, Oraland, PA, USA, 2009, s. 5.

[14] F. Schab: *Schooling without learning: Thirty years of cheating in high School*, „Journal of Youth and Adolescence" 1991, vol. 26, s. 839–848.

Egzaminy przeprowadzane zdalnie stwarzają szczególne możliwości zawyżania swoich wyników nieetycznymi metodami; jest ich więcej niż podczas egzaminów, w których występuje pilnujący, a nie wszystkie metody zdalnego egzaminowania uwzględniają tego typu problem. W tym miejscu omówimy pokrótce metody tradycyjnie wykorzystywane przez egzaminowanych:

- ściągi – polegają na korzystaniu w czasie testu z wcześniej przygotowanego źródła informacji i ukryciu tego faktu przed sprawdzającym; przy czym miejsca ukrycia zapisków są różne, od kartek papieru, przez długopisy, etykiety butelek, powierzchnię stołu aż do własnego ciała czy odzieży[15];
- przekazywanie informacji – uzyskiwanie pomocy od innych (również innych egzaminowanych) w trakcie egzaminu poprzez zaglądanie w ich prace, rozmowę, podawanie karteczek czy nawet używanie umówionych kodów lub łączności radiowej (SMS-y, specjalne, ukryte słuchawki bluetooth);
- zastępstwo na egzaminie – podstawienie na egzamin kogoś innego, szczególnie łatwe, jeśli pilnujący nie znają pilnowanych;
- odwołanie testu za pomocą symulacji awarii sprzętu lub wywołania alarmu pożarowego, bombowego itp.;
- znalezienie klucza testu lub poznanie pytań wykorzystanych wcześniej;
- manipulacja oprogramowaniem oceniającym – od zaznaczenia wszystkich odpowiedzi po to, żeby maszyna zarejestrowała punkt niezależnie od tego, która jest właściwa, aż po włamanie się do elektronicznego dziennika i bezpośrednią zmianę ocen;
- zmowa ze sprawdzającym – od zapewnienia dużej gazety do czytania w czasie egzaminu, przez przekupstwo czy szantaż aż po działania nauczyciela chcącego poprawić wyniki podopiecznych bez ich udziału.

Jak widać, problemy z uczciwością samego procesu egzaminowania nie są specyficzne dla egzaminów zdalnych, a tylko w ich przypadku dostępne są dodatkowe rozwiązania (rejestracja obrazu i dźwięku, monitorowanie komputera studenta itp.).

3. Proponowane rozwiązania

Aby zapewnić punkt odniesienia do rozważań, przedstawimy w tym miejscu jeden z proponowanych systemów egzaminowania na odległość. Jeden z takich protokołów, SeCOnE, został zaproponowany w pracy[16] jako metoda przeprowadza-

[15] M. Gogolewski, Ł. Nitschke, M. Ren, T. Tyksiński: *Przegląd systemów egzaminowania elektronicznego pod względem bezpieczeństwa*, Raport techniczny 137/2010, Uniwersytet im. Adama Mickiewicza, Poznań 2010.

[16] I. Jung, H. Yeom: *Enhanced Security…*, *op. cit.*

nia egzaminów z matematyki oraz języka angielskiego w gimnazjach i szkołach średnich. W rozwiązaniu tym zakłada się, że komputer ucznia jest wyposażony w mikrofon i kamerę internetową. Uczeń instaluje także specjalne oprogramowanie, które między innymi blokuje pozostałe programy, dostęp do sieci (poza systemem egzaminującym), jednocześnie przesyłając zrzuty ekranu oraz obraz z kamery (2 obrazy na sekundę). Środowisko takie umożliwia przynajmniej częściową kontrolę nad procesem zdawania egzaminu poza szkołą (np. w domu ucznia). Odpowiednio ustawiona kamera wraz z programami monitorującymi komputer umożliwia wykrywanie oszustw.

Zapewnienie skutecznego monitoringu wymaga jednak utrzymywania połączenia o dużej przepustowości (ok. 700 MB na studenta w ciągu godziny egzaminu) oraz znacznej przestrzeni dyskowej do celów archiwizacji. System jest dość skomplikowany, szczególnie jeżeli weźmie się pod uwagę liczbę ról użytkowników oraz podziały kompetencyjne między nimi. Kolejnym, także dość skomplikowanym, rozwiązaniem jest schemat systemu HP, zaproponowany w pracy[17]. Autorzy zwrócili uwagę przede wszystkim na anonimizację dwustronnej komunikacji pomiędzy nauczycielem a studentem. Dzięki temu nauczyciel i student pozostają anonimowi wobec siebie. Dodatkowo dzięki zastosowaniu sieci mieszających proces anonimizacji realizowany jest przez wielu uczestników – nie trzeba polegać na jednym zaufanym uczestniku. Cecha ta odróżnia to rozwiązanie od znacznie prostszego protokołu CHD[18], który korzysta z pojedynczego pośrednika zwanego menedżerem. Wadą tego podejścia jest wymóg pełnego zaufania do menedżera. Na prostotę rozwiązania postawili twórcy systemu CHP[19]. Przyjęli oni, że studenci będą zdawać egzamin w pomieszczeniach kontrolowanych przez instytucję egzaminującą. Zdający będą odpowiadać na pytania za pomocą przenośnych terminali wyposażonych w łączność bezprzewodową (PDA, tablety itp.). Zakłada się, że terminal jest kontrolowany przez przeprowadzającego egzamin, a nie studenta. Wadą tego rozwiązania jest brak anonimowości. Porównanie wspomnianych wyżej systemów przedstawione zostało w tabeli 1.

Analiza cech opisanych rozwiązań prowadzi do dość oczywistego wniosku – polepszenie bezpieczeństwa systemu odbywa się kosztem zwiększenia stopnia jego skomplikowania. Rozwiązania, które okazały się spełniać najwięcej kryteriów bezpieczeństwa, wymagały zaangażowania wielu ról uczestników po stronie organizującego egzamin, wykorzystania zaawansowanych i złożonych narzędzi krypto-

---

[17] A. Huszti, A. Petho: *A Secure Electronic…*, *op. cit.*

[18] J. Castella-Roca, A. Dorca-Josa, J. Herrera-Joancomarti: *A Secure E-Exam…*, *op. cit.*

[19] J. Castella-Roca, J. Herrera-Joancomarti, J. Prieto-Blazquez: *A Secure Electronic Examination Protocol using Wireless Networks*, ITCC ’04: Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC ’04), vol. 2, IEEE Computer Society 2004.

graficznych, a w konsekwencji zwiększenia ilości informacji i liczby komunikatów wymienianych przez sieć komputerową.

Tabela 1

Porównanie systemów zdalnego egzaminowania

	Liczba ról	Kontrola	Potwierdzenie	Anonimowość		Rozproszenie zaufania
				Student	Nauczyciel	
CHD	3	nie	nie	nie	nie	nie
CHP	3	nie	tak	tak	nie	nie
HP	5	nie	tak	tak	tak	tak
Se-	7	tak	tak	tak	tak	nie

Podsumowanie

Wiele obecnych trendów w dziedzinie *e-learningu*, kształcenia ustawicznego oraz systemów certyfikacji wskazuje zapotrzebowanie na rozwiązania umożliwiające sprawdzanie wiedzy na odległość. Analiza obecnej wiedzy na temat systemów zdalnego egzaminowania prowadzi do wniosku, że brak jest obecnie w pełni satysfakcjonującego rozwiązania. Bardziej zaawansowane systemy wydają się zbyt skomplikowane, co może wpływać na ich niezawodność. Należy zwrócić uwagę na fakt, że zorganizowanie prawdziwie zdalnych egzaminów wymaga wyrafinowanego systemu monitoringu. Co więcej, wskazane wydaje się skorzystanie z możliwości biometrii. Autorzy niniejszego opracowania skupili się głównie na technicznym aspekcie przeprowadzania tego typu egzaminów. Otwartym problemem pozostaje analiza psychologiczna (np. jak „zachęcić" do uczciwości poprzez system kontroli).

Literatura

1. Castella-Roca J., Dorca-Josa A., Herrera-Joancomarti J.: *A Secure E-Exam Management System*, ARES 2006.
2. Castella-Roca J., Herrera-Joancomarti J., Prieto-Blazquez J.: *A Secure Electronic Examination Protocol using Wireless Networks*, ITCC '04: Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC '04) vol. 2, IEEE Computer Society 2004.
3. Chaum D.: *Secret-ballot: True voter verifiable elections*, IEEE Security and Privacy 2004, vol. 2.

4. Clabaugh G., Rozycki E.: *Preventing Plagiarism & Cheating, An Instructor's Guide*, 2nd ed., NewFoundations, Oraland, PA, USA 2009.
5. Gogolewski M., Nitschke Ł., Ren M., Tyksiński T.: *Przegląd systemów egzaminowania elektronicznego pod względem bezpieczeństwa*, Raport techniczny 137/2010, Uniwersytet im. Adama Mickiewicza, Poznań 2010.
6. Huszti A., Petho A.: *A Secure Electronic Exam System*, 2008, www.inf.unideb.hu/~pethoe/cikkek/4682-Huszti-Petho.pdf
7. Jung I., Yeom H.: *Enhanced Security for Online Exams Using Group Cryptography*, IEEE Transactions on education 2009, vol. 52, no. 3.
8. Oorschot P., Menezes A., Vanstone S.: *Handbook of Applied Cryptography*, CRC Press, Boca Raton, FL, USA 1996.
9. Schab F.: *Schooling without learning: Thirty years of cheating in high School*, „Journal of Youth and Adolescence" 1991, vol. 26.

SECURE REMOTE EXAM SYSTEMS IN E-LEARNING AND KNOWLEDGE ECONOMY

Summary

Various forms of e-learning have gained popularity in recent years due to growing demand for certification programs, lifelong learning and long-distance learning. A common requirement is the necessity of conducting exams remotely, as traditional examinations would increase costs to unacceptable levels. This article presents solutions that enable remote exams while ensuring fairness, by enforcing honesty of students and exam authorities.

Translated by Michał Ren