BIOMETRIC AUTHENTICATION FOR WEB-BASED COURSE EXAMINATIONS

Brent Auernheimer
Max J. Tsai
Digital Campus
California State University
Fresno, CA 93740 USA
brent@CSUFresno.edu, janq@CSUFresno.edu

Abstract

The paper discusses design considerations and a prototype for a biometrics (fingerprint) based identification and authentication system to support web-based course examinations. The goal of the resulting system is to be acceptable to the university culture and minimally disruptive to university procedures and processes.

Key Words

Protection and Security, Distance Learning, Education, Biometrics

1. Introduction

How does an instructor teaching on-line know who is really taking quizzes and exams? Are there ways of identifying and authenticating students thereby reducing instructor anxiety?

These questions are typical of security questions asked in society at large. Unfortunately, although technological approaches to security become increasingly sophisticated, human weaknesses continue. Professional "social engineers" such as Kevin Mitnick exploit human and organizational weaknesses to access otherwise sophisticated computer systems. Mitnick summarizes [1, p. 4] (emphasis added):

> Security is too often merely an illusion ... In the end, social engineering attacks can succeed when people are stupid, or, more commonly, simply ignorant about good security practices ... many information technology professionals hold to the misconception that they've made their companies largely immune to attack because they've deployed standard products – firewalls, intrusion detection systems *or stronger authentication devices such as time-based tokens or biometric smart cards*... It's a case of living in a world of fantasy: they will inevitably, later if not sooner, suffer a security incident.

Universities are not immune to security breaches. A spring 2004 university scandal alleged the "selling" of course grades to hundreds of students [2]. Although the grades were changed using a computer, this was clearly a "social engineering" problem.

A typical approach to identifying students intending to take an on-line exam is to reserve a computer lab and hire a proctor to check student identification cards. Unfortunately, proctors can be bribed and identification cards can be forged – or more often, forgotten.

In our larger society, a user's vested interest is protecting their identity or secret information. For example, it is in our best interest to protect both our bank card *and* our PIN. However, in the case of a student's impostor taking an exam, the user is actively trying to "give away" his or her identify. For this reason, we believe biometrics are most useful to on-line faculty as

identification, not as *authentication*. The distinction is discussed later in the paper.

Determining the appropriate level of security is an exercise in risk management. The severity of the loss (e.g., students hiring impostor test-takers), the probability of occurrence, and the cost for mitigation (e.g., hiring test proctors and dedicating computer laboratories) are considerations. The university culture defines acceptable risks, costs, and mitigation: plagiarizing a weekly exercise might result in a failing course grade, whereas compromising a faculty computer to read the final exam might result in expulsion.

This is similar to decisions we make as a larger society about "safety-critical" computer systems [3, p. 41]:

> Generally, the public at large establishes the acceptable risk for a given mishap type in terms of its willingness to tolerate the mishap as long as it occurs infrequently. Statistics for various common mishaps and their average frequency represent acceptable [risk] ... The relative rarity of such occurrences explains why, despite the tragic events underlying these statistics, most of us can feel relatively safe while driving a car or flying on an airliner.

Our goal is to incrementally develop a biometric authentication system useful for on-line education, compatible with university culture and tolerance for risk, and minimally disruptive to existing procedures. Along the way we also hope to minimize opportunities for "social engineering" exploits.

2. Biometrics

Biometric devices that read fingerprints and plug into USB ports are affordable and widely available. Our initial temptation is to reserve a computer lab and install a fingerprint reader at each computer to authenticate test-takers.

Unfortunately, that does not solve our problem. First, biometric devices can be compromised. Thalheim, Krissler, and Ziegler describe three scenarios [4]:

- tricking the biometrics system "with the aid of artificially created data whilst making use of the regular sensor technology of the system"
- spoofing the biometrics system with previously collected data (a "replay" attack)
- attacking the database of biometric data

Thalheim et al. tested eleven "biometric protection applications". Disappointingly, they conclude "we were able, aided by comparatively simple means, to outwit all the systems tested", including using printed images of an eye to fool an iris scanning biometric device.

Biometric authentication has other problems. For example, most of us have only ten fingerprints. If a fingerprint is compromised (for example, lifted from a surface and used to create an artificial fingerprint, such as done by Thalheim et al.) the legitimate user has only nine other authenticators. The authentication space can be doubled by using toes, but at a social cost that may be unacceptable.

In their insightful article about password reuse, Ives et al. describe this problem with biometrics (emphasis added) [11, p. 77]:

> ... a biometric can be seen as an another form of password, in this case generated by the interaction of a human and a scanning device. While convenient, the digital scan or pattern is vulnerable to network analyzers *and, unlike a password, cannot be changed once stolen.* This generally limits the use of biometrics to scenarios where the network and biometric capture device are secure.

Similarly, Maltoni et al. point out [12, p. 47]

Biometrics are not secrets. It is often possible to obtain biometrics samples (e.g., face) without the knowledge of the person. This permits covert recognition of previously enrolled people ... Although currently there is no technology for snooping fingerprints of sufficient quality to positively identify persons, we cannot exclude that in the future such technology might be commonplace.

We propose using biometric information for identification, and a traditional password for authentication.

2.1 Our approach

We are prototyping a biometrics-based identification system at California State University, Fresno's Digital Campus. The system integrates the existing Learning Management System (LMS), in this case, Blackboard, a commercially available fingerprint reader, and the existing university directory server (LDAP).

In particular, our prototype includes

1. using the campus LDAP directory to contain password data, and URLs for biometric data
2. employing the biometric data (fingerprints, in particular) for identification, not authentication
3. using traditional passwords for authentication
4. using secure protocols such as HTTPS, S-LDAP, and SSL

Additionally, we intend to use a simple web-quality video camera to capture a time-stamped image of students as they are using the biometric device. The time-stamped images are an audit trail that can be used in disciplinary procedures when cheating is suspected.

2.1.1 LDAP

Employing the existing campus LDAP [5] directory server is minimally disruptive to the university's systems.

LDAP allows the storage of identification and authentication data including user names, email addresses, encrypted passwords, and "binary" data such as biometric representations. Just as passwords are stored encrypted (not as cleartext), biometric data can also encrypted.

However, instead of storing biometric data in the LDAP directory, we initially propose using the existing unused LDAP attribute "knowledge information" to contain the URL of a biometric information record (BIR). The BIRs are stored in a secure database. The user's login name is used for the LDAP query key. For example, a typical LDAP command line query is:

```
# ldapsearch -x -D"cn=admin,
o=DigitalCampus, c=us" -
b"cn=georgebush, ou=BioProxy,
o=DigitalCampus, c=us" -W
uid=georgebush

# Enter LDAP Password: XXXX
```

Resulting in the following response:

```
 # extended LDIF
 #
 # LDAPv3
 # base <cn=georgebush, ou=BioProxy,
o=DigitalCampus, c=us> with scope sub
 # filter: uid=georgebush
 # requesting: ALL
 #

 # georgebush, BioProxy,
DigitalCampus, US
 dn:
cn=georgebush,ou=BioProxy,o=DigitalCam
pus,c=US
 objectClass: organizationalRole
 objectClass: simpleSecurityObject
 cn: georgebush
 description: BioProxy administrator
 userPassword::
e0NSWVBUfXNyb3ROVWlycEZBQ0U=
 uid: georgebush
```

```
knowledgeInformation:
/secret/biodata/georgebush.bir
```

```
# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

The attribute containing the URL of the biometric data is in bold type above.

Using the existing campus LDAP server, and the unused knowledgeInformation attribute, is a single point of failure. However, it is not a new failure point, and in that sense is "no worse" than the existing security situation.

2.1.2 Identification and authentication

Our prototype uses biometric data for identification, not authentication. However, our prototype is traditional in the sense that passwords are used for authentication, in the same way they are used with text-based user identifiers.

Bruce Schneier emphasizes the importance of separation of concerns [13, pp. 182-183]

> Identification, authentication, and authorization. The three concepts are closely related, but in a security system it's critical that we tell them apart. Here's the shorthand guide:
>
> - Identification: Who are you?
> - Authentication: Prove it.
> - Authorization: Here is what you are allowed to do.
>
> Conflating the three – running them together, failing to distinguish each from the others – can lead to serious security problems.

A student wishing to take an examination will sit at a workstation, place their finger on the reader (identification), and type their user name and password (authentication). If the process is successful, the student is logged into the LMS to begin the examination (authorization).

The figure below shows the architecture of our prototype. The process starts with the "user login" oval on the left. Their fingerprint is obtained from the biometric device ("FP Fetch"), and transmitted securely with authentication data to server-side processes.

For our initial prototype, the student's user name is used as the key for an LDAP query. A successful query returns stored biometric data, and a match ("FP match") is attempted. A successful match generates a proxy page to login the student to the LMS. At this point the LMS checks the user's password (authentication).
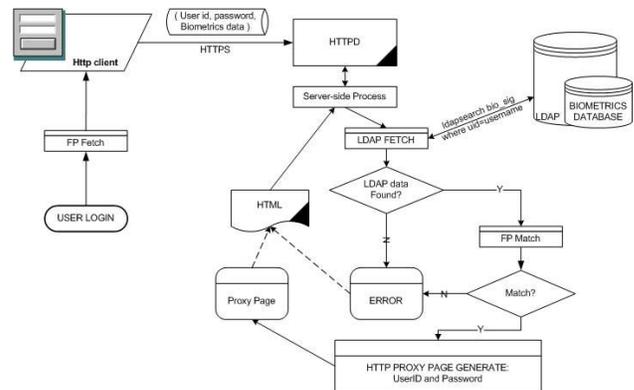
The prototype is being developed incrementally. Currently, we are running OpenLDAP (http://www.openlap.org) on Mac OS X to provide directory services. The LDAP portion of the enrollment process, as well as the retrieval portion of the authentication process are implemented.

The proxy module "front end" to the learning management system is also implemented, in PHP. Because we don't have access to source code for the LMS, the proxy module simulates a "normal" user login by presenting the username and password to the LMS.

We use the BioAPI (http://www.bioapi.org/) protocols for biometric data used in enrollment, identification, and data matching.

2.1.3 Computer labs and proctors

We believe there is no substitute for a proctored computer laboratory for examinations. Proctors can watch for real-time collaboration (i.e., cheating) and laboratory networks can restrict access to the university's LMS.

However, using our scheme, proctors need not be trusted to check student identification cards. In fact, students need not carry their identification cards. They take exams by simply identifying themselves using a fingerprint and typing their username and password.

2.2 Enrollment

Upon arriving on campus, students visit several offices to pay fees, get an email address, and complete paperwork. One office checks their government-issued identification, photographs the student, and issues a student identification card. "Enrolling" a fingerprint as part of this process would be a minor addition.

The figure below shows the enrollment process. The administrator in charge of enrolling new students initiates the process at a Web page. The biometric data is obtained from the device, and inserted into the biometrics database and the corresponding URL into the LDAP directory. Secure HTTP and LDAP protocols are used to protect transmissions.
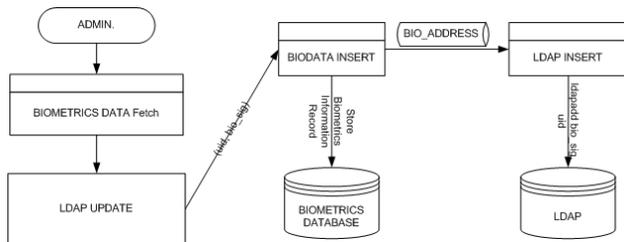
Similarly, when a student's relationship with the university is terminated, their encrypted password and encrypted biometric data can be deleted.

Enrollment of biometric data – collection, encryption, and storage in the LDAP directory or secure database – raises ethical issues. Alterman asserts [6, p. 145] "biometric data acquires a fundamental privacy interest because it has an impact on one's right to control the use and disposition of one's body", and compares biometric data with photographs:

> But if we have a special interest in controlling photographic representations, we have a stronger one in controlling biometric scans of ourselves... Unlike a photographic image, from which one can dissociate oneself by various superficial means, the features used for biometrics cannot be altered without serious physical damage, except by the aging process.

He recommends [6, p. 148] "there should be no mandatory biometric imaging for important social privileges like obtaining a driver's license or credit card, not in most cases as a condition of employment." Again, the culture of the university, and the larger society, will decide if enrollment of fingerprint data is appropriate for college students.

2.3 Future work

We are interested in industry standard interfaces to biometric devices. In particular, BioAPI [7. p.14]:

> The BioAPI is intended to provide a high-level generic biometric authentication model; one suited for any form of biometric technology. It covers the basic functions of Enrollment, Verification, and Identification, and includes a database interface to allow a biometric service provider (BSP) to manage the Identification population for optimum performance.

We also want to use CAS (Central Authentication Service, http://www.yale.edu/tp/auth/cas20.html) to

share authentication techniques and data among trusted systems. We believe combining CAS with open source learning management systems such as Sakai (http://www.sakaiproject.org) and proprietary LMS systems such as Blackboard is a powerful way to meet the university's needs.

We also want to use URL schemes (http://www.ietf.org/rfc/rfc2718.txt) to simplify dispatching of biometric data. Also, biometric data can be converted into XCBF, the XML common biometric format (http://xml.coverpages.org/xcbf.html).

Finally, using cryptographic threshold techniques for matching biometric data to stored data is intriguing. Uludag et al. [14] discuss the challenges of marrying fuzzy biometric data with cryptographic techniques that by design are sensitive to small variations. We also believe that recent developments using biometrics to streamline PKI (Public Key Infrastructure) [8] could be applied to our application.

3. Conclusion

We've presented issues considered in the design of a prototype biometric authentication system to support students taking examinations on-line.

The prototype provides proof-of-concept, and lets us prepare a trial for one or two classes. Small scale trials are necessary since a full scale university-wide rollout could involve over 1200 web-enhanced and web-based classes, and 17000 students.

We believe resisting the temptation to use fingerprints for authentication -- instead using the biometric data for identification plus a conventional password for authentication -- is a reasonable design with minimal disruptions to existing university systems and procedures.

The larger issues of who (or what) to trust remains. We can look to a classic of our field for some guidance. Ken Thompson's Turning Award Lecture "Reflections on Trusting Trust" [9] demonstrates how "you can't trust code you did not totally create yourself." Similarly, twenty years later Spinellis describes the "nearly unbroken track record of failed security technologies" [10] comparing a hack to run Linux on a Microsoft Xbox to Thompson's Trojan Horse. In light of these examples we believe an open design and implementation process, along with dialog in the university community about privacy and security, is the best approach.

4. Acknowledgements

The authors appreciate the comments and support of their colleagues. Garvin Chan was particularly insightful.

References:

[1] K.D. Mitnick and W.L. Simon. The Art of deception: Controlling the human element of security (Indianapolis, IN: Wiley Publishing, 2002).

[2] National Public Radio (NPR). Alleged grade scandal at Southern University. All Things Considered, Friday 2 April 2004. http://www.npr.org/rundowns/segment.php?wfId=1809418

[3] W.R. Dunn. Designing safety-critical computer systems. IEEE Computer. November 2003. 40-46.

[4] Lisa Thalheim and Jan Krissler, Peter-Michael Ziegler. "Body check: Biometrics defeated". c't Magazine. http://www.extremetech.com/print_article/0,3428,a=27687,00.asp 3 June 2002.

[5] J. Hodges and R. Morgan. Lightweight Directory Access Protocol (v3): Technical Specification. RFC 3377. September 2002. http://www.ietf.org/rfc/rfc3377.txt

[6] A. Alterman. "A piece of yourself": Ethical issues in biometric identification. *Ethics and information technology, 5*, 2003. 139-150.

[8] Daon. Biometrics and PKI based digital signatures: A short white paper. 2003. http://www.daon.com/white%20papers/daon_white_paper_biometrics_pki.htm

[7] BioAPI Consortium. BioAPI Specification Versuon 1.1 (26 March 2001). http://www.bioapi.org/BIOAPI1.1.pdf

[9] K. Thompson. Reflections on Trusting Trust. Communications of the ACM. 27(8), 1984. 761-763. http://www.acm.org/classics/sep95/

[10] D. Spinellis. Reflections on trusting trust revisited, *Communications of the ACM, 46*(6), 2003, 112.

[11] B. Ives, K.R. Walsh, and H. Schneider. The domino effect of password reuse, *Communications of the ACM, 47*(4), 2004, 75-78.

[12] D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar. *Handbook of fingerprint recognition* (New York: Springer, 2003).

[13] B. Schneier. *Beyond fear: Thinking sensibly about security in an uncertain world* (New York: Copernicus Books, 2003).

[14] U. Uludag, S. Pankanti, S. Prabhakar, and A.K. Jain. Biometric cryptosystems: Issue and challenges. *Proceedings of the IEEE, 92(6),* 2004, 948-960