Wireless Security Perspectives

Cellular Networking Perspectives

Editors: Les Owens, David Crowe. Email: wsp@cnp-wireless.com Vol. 3, No. 4. May, 2001

Designing Security Systems for Biometric Authentication

Biometrics, the statistical study of biological phenomena, has been used for more than 100 years in law enforcement for the identification of criminals, most notably through the use of fingerprints. Recently, electronic biometric analysis has become fast enough and devices to implement it small enough for use in commercial authentication products. Several types of biometric devices are available today, including:

- Fingerprint matching
- Retinal scan
- Face scan, and
- Handprint.

Research is even underway to develop a DNA authentication device on a chip.

The data that is distilled from biometric authentication devices is referred to as authentication material. A password is a type of authentication material consisting of user entered text.

Password Problems

Passwords are inferior to biometric methods of authentication for several reasons, including:

- They are often written down in unsecured locations,
- They may be given away,
- If not carefully chosen, they are easily guessed,
- They are often forgotten,
- System administrator's can be tricked into revealing them by social engineering.

Biometric authentication material, such as a fingerprint, cannot be forgotten, loaned to another person and is usually difficult, if not impossible, to change.

Authentication Costs

It is estimated that the annual cost of password maintenance on internal IT systems for companies is between US$100 and $300 per year, per user. Several companies have tried to develop systems to reduce this, in an attempt to achieve the holy grail of password administration – single sign-on – a single password or biometric authentication type that controls user access to all of an organization's systems. Rather than having different authentication and access systems for a company database, payroll system, accounting system, and distribution system, a single sign-on system would allow centralized administration while interfacing transparently with all of the internal systems.

Standards such as kerberos have been around for years but have failed to gain traction in the market. Single sign-on systems are very complex because they must interface with various, non-standard legacy systems. Interfacing to each of

About *Wireless Security Perspectives*

Price

The basic subscription price for *Wireless Security Perspectives* is $300 for one year (12 issues) for delivery by emailed PDF file or by first class mail within the US or Canada. International subscriptions are US$350 per year. The basic subscription allows for distribution to up to 10 people within one organization. Contact us for license fees to allow more readers.

We provide discounts to educational institutions and small businesses (less than 10 employees).

Back issues are available individually, or in bulk at reduced prices.

Delivery is by first class mail or by email (Acrobat PDF file).

Complete pricing information for both publications is available at:

www.cnp-wireless.com/prices.html

To obtain a subscription, please contact us at:

cnpaccts@cnp-wireless.com

Next Issue Due…

June 15th, 2001.

Future Topics

Wireless Packet Data Security • AES (Rijndael) • m-commerce security • PKI • IP Security • Public Keys & Wireless

Wireless Security Perspectives (ISSN 1492-806X (print) and 1492-8078 (email)) is published monthly by Cellular Networking Perspectives Ltd., 2636 Toronto Cresc. NW, Calgary, Alberta T2N 3W1, Canada. **Phone**: 1-800-633-5514 (+1-403-274-4749) **Fax**: +1-403-289-6658 **Email**: cnpsales@cnp-wireless.com **Web**: http:/www.cnp-wireless.com/wsp.html. **Subscriptions**: $300 for delivery in the USA or Canada, US$350 elsewhere. **Payment**: accepted by cheque, bank transfer, American Express, Diners Club, MasterCard or Visa. **Delivery**: Email or 1st class mail. **Back Issues**: Available individually for $35 in the US and Canada and US$40 elsewhere, or in bulk at reduced rates. **Discounts**: Educational and small business discount: 25% off any order. **Copies**: Each subscriber is licensed to make up to 10 copies of each issue or back issue. Call for rates to allow more copies.

Technical Editor: Les Owens.
Article Sourcing: Betsy Harter.
Production: Doug Scofield.
Distribution: Debbie Brandelli.
Marketing: Muneerah Vasanji.
Accounts: Evelyn Goreham.
Publisher: David Crowe.

these systems may involve significant development costs.

Biometric authentication methods can be used as part of a single sign-on system, but they only replace the password and do not alleviate all of the complex interfacing with disparate systems that is required to implement single sign-on. Biometric authentication may be more secure, but it does not solve the cost problems.

Enrollment

All authentication services require enrollment. A new user must be identified, an account must be set up, and the authentication data must be associated with this account. This is the process of enrollment, and it is required whether a traditional password or a more advanced system is used.

Enrollment is often a weak link in an authentication system. *Social Engineering* can be used to persuade a person that an account should be set up, that a password should be reset, or that additional account privileges should be granted.

Enrollment is necessary because authentication does not necessarily provide identification. You can say that a fingerprint left at a crime scene is the same as the one left on a glass at a restaurant, but you still do not know whose fingerprint it is. You must identify the person and tie them to the fingerprint.

Biometric authentication only indicates that the biometric material presented at authentication is the same biometric material that was presented during enrollment. Identification of the person being enrolled must be done when the original authentication material is stored in the database. This issue must be resolved through administration of the enrollment process by a trusted third party.

For example, if a company wishes to enroll employees into an authentication service with biometric material, the Human Resources department could be entrusted with enrollment. It would be their responsibility to positively identify each employee assigning them any access privileges.

Supervision of enrollment is necessary to ensure that stored authentication material is valid. Only then can transactions authenticated by it be trusted. The level of trust required during enrollment is directly proportional to the level of transactions that will be executed using this authentication system.

For example, to create an account on America Online, all you need is one of the handy coasters that the AOL marketing department is constantly mailing out and giving away at retail points of sale. Signing on is simply a matter of inserting the disk or CD and typing a screen name such as JohnDoe358. This is now your official AOL screen name. Authentication merely requires access to this screen name and a password. AOL has no idea if you are really John Doe, his 8-year-old son or someone who saw the name and password on a sticky-note on a computer screen. Enrollment data such as credit card numbers and street addresses are not secure when transmitted over an Internet connection.

This weak enrollment system can be justified because AOL has only the $9.95 monthly fee at risk if you are not who you say you are and you therefore contest the charge on your credit card. In many other cases, such as large on-line sales, such as B2B equipment purchases, transactions can be worth millions of dollars and therefore authentication must be much more secure. For authentication to be fully trusted, the enrollment process must be provably secure.

Protecting Authentication

Securing authentication material starts at enrollment and continues on through transmission to a storage facility, storage and later retrieval. It must be protected at all points of the system in order to guard against attacks such as replay, authentication material theft, and potential alteration of data.

Most authentication systems involve three parties:

1. The user being authenticated,
2. The service provider, and
3. The authenticator.

A complete authentication system protects all three parties of a transaction and guards against possible compromise of the system from within any of the three parties. With a three-party authentication service, the transaction cannot be broken without collaboration by at least two of the parties. This makes the system more robust and allows for a high degree of certainty that the authentication event actually identifies the user.

Securing Authentication Services

The authentication service provider must design their authentication system so that no system administrator can have access to authentication material. Password systems often solve this problem by storing passwords only in an encrypted form. When users enter a password, their input is encrypted and compared with the stored, encrypted password.

For biometric data, security can be accomplished by splitting the authentication material and storing it in multiple databases, using algorithms chosen for speed and security. Splitting for storage and recombination for authentication should be done only on a highly secure system.

One solution that is often chosen is to use a commercial, certified secure operating system. However, a more secure approach is to design a computer system that does not have a user shell, or any remote access except through the authentication application, eliminating all static internal storage such as a hard-drive and flash-memory.

The system that Ethentica has designed boots from a CD and configures itself to the other nodes in the system at run-time. The only place that the authentication material appears whole and unencrypted is in memory on the cryptographic node for a moment of time. During enrollment the software splits the incoming data and purges the original from memory. During authentication, the software combines parts of the stored data for comparison with the authentication material delivered by the client and returns only an answer (i.e. it either matches or it does not). Once data comes into the system at enrollment, it never leaves.

Security of the split databases can be provided in several ways. Each database can have different passwords and administrators, though moving the databases to geographically separate data centers with different systems administrators may be easier to implement from a human standpoint. Security policies and procedures can be broken. If two system administrators have access to a system, they are likely to provide backup for each other and can break the security model by trading access passwords. The ideal situation would be separate data centers hosted by different companies. That way, in addition to the policies put into place, the possibility of a system administrator gaining access to both pieces of the key can be minimized. Another method to increase the security is to cryptographically split the data into more than two pieces and store them in more than two data centers.

Secure Transmission

Once the authenticated material is securely encrypted and stored, the data must be delivered to the authentication provider in a secure manner. Communications among all parties in the transaction should be encrypted. In addition to encrypting the transmissions, the authentication material can be super-encrypted within the data stream.

Super-encryption is used to describe the encryption of the authentication material within the encrypted digital transmission. This data is *never* seen by administrators. The authentication system stores the biometric material and compares it to biometric material gathered at an authentication event. The material is only decrypted in the cryptographic engine and only exists in memory long enough to make a comparison with the stored material. This is to ensure that no administrator can reproduce the original material unless they were to compromise multiple data centers (databases).

The datastream is encrypted with SSL. However, due to known flaws in SSL, we chose to further encrypt the biometric authentication material using PKCS #7. In this way, we can be sure that only the final destination, the cryptographic device controlled by the authentication provider, can decrypt it.

Another reason to super-encrypt biometric authentication data is so that other machines within the authentication server cluster and the network connecting the cluster do not have unencrypted material where system administrators might be able to obtain it.

There are connections among all three parties during an authentication transaction. The data flow should be designed to further enhance the security of the system. For example, the authentication material should pass directly from the client to the authentication service, so that a dishonest party at the transaction vendor cannot record the data passing by on the network and attempt a replay attack. Similarly, the transaction vendor should begin the transaction and initiate contact with the authentication provider so that a client cannot execute a replay attack.

Figure 1 illustrates the three party client server architecture and some of the security that protects data in transit among the three parties.

Conclusions

Security and vigilance against outside attack must be designed into an authentication service at every point in the system. Multi-layered security through carefully designed data flow, encryption at all stages of communication, and implementation of strict policies and procedures is required to build a secure service.

An authentication system must have a trusted enrollment system, and each authentication must protect the client, the authenticator and the service provider.

Because biometric authentication material is more permanent than passwords, greater care must be taken to protect it from internal and external threats at all points in the system. Equal care must be taken to secure data in motion as is done to secure data at rest within the system.

Glossary

Secure Sockets Layer (SSL) • A protocol designed by Netscape Communications Corporation to provide encrypted communications on the Internet. SSL is layered beneath application protocols such as HTTP, SMTP, Telnet, FTP, Gopher, and NNTP and above the connection protocol TCP/IP. It is used by the HTTPS (secure http) access method.

kerberos • The authentication system of MIT's Project Athena. It is based on symmetric key cryptography. Adopted by OSF as the basis of security for DME.

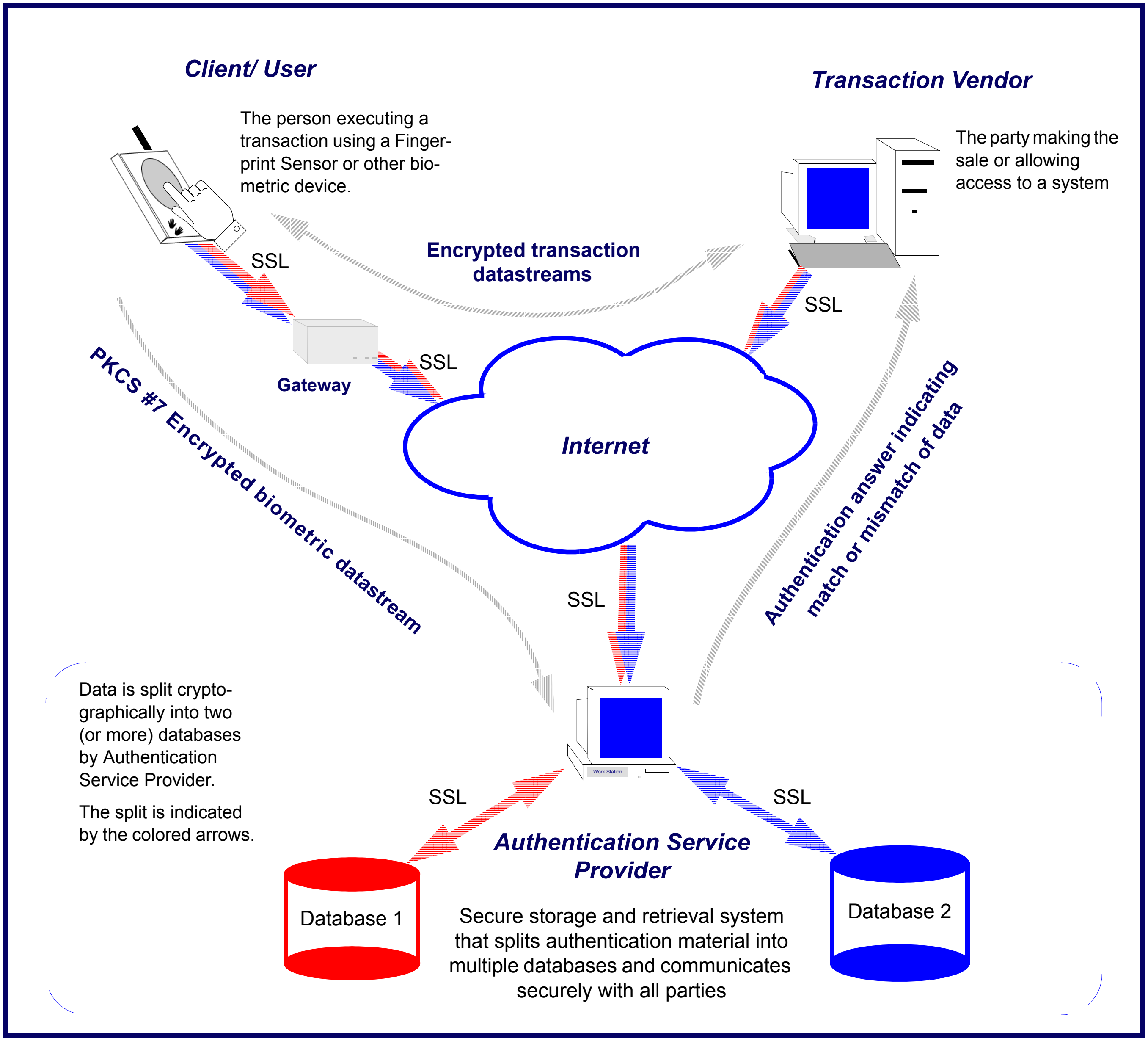
Public Key Cryptography Standards (PKCS) • Public-Key Cryptography Standards are produced by RSA Laboratories in cooperation with secure systems developers worldwide for the purpose of accelerating the deployment of public-key cryptography.

PKCS #7 • Cryptographic Message Syntax Standard. This standard describes a general syntax for data that may have cryptography applied to it, such as digital signatures and digital envelopes.

About Ethenticator

Ethenticator's primary hardware product, the Ethenticator 3000 is a PCMCIA card incorporating a fingerprint sensor, designed to be installed in laptop computers, which are often used remotely. Fingerprints are reduced from an image captured at the CCD (Charge Coupled Device) to a small template that can later be compared to templates generated by the same finger, even if the original image is different – for example, if a finger is placed at different angles. This company's primary software product, the Trust Engine, is a 16-node multiply-redundant server cluster that incorporates many of the security concepts discussed in this article. The Trust Engine is deployed in four data centers, and biometric material is cryptographically split into four parts, of which any two can reproduce the original material. Biometric devices such as these will work their way into the PDA and Wireless phone market as demand for secure m-commerce functions using these clients increases.

Figure 1: Three-Party Client Server Architecture


Client/ User
The person executing a transaction using a Fingerprint Sensor or other biometric device.
Transaction Vendor
The party making the sale or allowing access to a system
Encrypted transaction datastreams
SSL
Gateway
SSL
SSL
Internet
PKCS #7 Encrypted biometric datastream
Authentication answer indicating match or mismatch of data
SSL
Data is split cryptographically into two (or more) databases by Authentication Service Provider.
The split is indicated by the colored arrows.
Work Station
SSL
SSL
Authentication Service Provider
Database 1
Database 2
Secure storage and retrieval system that splits authentication material into multiple databases and communicates securely with all parties

About the Author

Aaron Brooks is currently Director of Software Development for Ethentica. He has over 10 years of Information Technology experience in Telecommunications, B2B Transaction processing, and E-Commerce industries. Aaron has built several high volume E-Commerce clusters using various dynamic web development technologies. At Ethentica, Aaron manages the software development group that designed, developed and implemented the Trust Engine authentication cluster. The Trust Engine's primary biometric device is the Ethenticator 3000, but it is capable of implementing any type of authentication material from any biometric vendor.