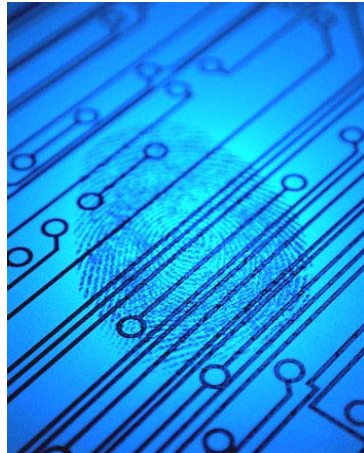


Legitim*i*

YOUR DIGITAL DNA



SECURITY WHITE PAPER

THE LEGITIMI TECHNOLOGY

Legitimi's technology is the strongest form of authentication without the need of external hardware devices. The technology associates a user with a device. This association takes into account two factors for authentication; something you know (User Password) and something you have (Trusted Device). The technology does this by providing specific internal device information from the Trusted Device and coupling it to the User.

DIGITAL DNA



The technology is based upon the premise that each computing device has unique hardware characteristics, similar to the human genome. Legitimi links the digital DNA of a specific device to a user, creating a unique system of identification that is more secure and reliable. This digital DNA may be utilized to authenticate the user and machine to specific applications without impact to pre-existing authentication processes or products.

To preserve user privacy, each of these device components is acquired and converted into a hash string, which is then wrapped in a one time 128 Bit encryption and passed to the authentication server via an SSL connection. For each Web session, the encrypted digital DNA is arranged in a unique pattern as it is sent to the server for authentication. In regular Windows applications the digital DNA may be utilized in a similar fashion for authentication purposes.

The device items that are collected include but are not limited to; hard drive serial number, CPU type/clock speed, memory type/physical location, physical MAC address,

LEGITIMI COMPONENTS

The three main components of Legitimi are:

- Legitimi Client
- Legitimi Authentication server
- Legitimi digital DNA database

Legitimi Client

The Legitimi Client is responsible for acquiring and encrypting a device's DNA and its transmission to the Legitimi Authentication Server as well as a UserID. For web deployment the Client is deployed either as an Internet Explorer Plug-in, Netscape/Mozilla-Firefox Plug-in or Apple's WebKit Plug-in used by Safari. In a Windows environment, plug-ins can be downloaded and installed by the browser (signed cab file for IE or signed xpi file for Mozilla) or it can be downloaded as an executable file.

Why Legitimi Utilizes Browser Plug-ins

Legitimi was designed to gather machine data directly from its source. It is this data that provides the basis for the absolute recognition of an individual device. In order to accomplish a strong authentication methodology it was necessary to have direct access to certain portions of the computing device internal systems that could only be touched through an on-board agent.

The intent of the design is to be able to provide an extremely strong 2 Factor authentication tool that would be scalable and cost effective for mass use in online environments. The number of options available to support this design is limited to providing a browser plugin or an executable program containing the necessary code to execute the machine data collection.

What Makes the Legitimi Plug-in Different?

Understanding that plug-ins can be exploited the developers of Legitimi have taken extreme measures to insure that this can not happen. The behavior of the Legitimi plug-ins may be described as “self-protected”. This means that the plugin has characteristics that by their nature prevent an exploitation of the object.

The DNA signed plug-in is a key part of the system and was implemented as an executable object thus allowing for a mechanism to protect sensitive information and also to give access to “hardware level” configuration data. Other implementation approaches such as the use of Java and scripting were abandoned in order to not degrade the self-protection level.

Most plugins, when installed, are actively “listening” for the application that causes them to perform. This “listening” requires that a port be open to insure the plugin does not miss the network traffic that would trigger the plugin to execute its application. A network port is a special number, ranging from 0-65535, recognized by the TCP and UDP protocols. These protocols use the ports to map incoming data to a particular process running on a computer.

The Legitimi plugin once delivered and installed in the computing device, remains inert until called by the application utilizing Legitimi. The Legitimi client is not loaded to memory and it does not consume any CPU power until an external program calls its entry point. Because of that, it is virtually impossible for someone to exploit any vulnerability, 99% of the time, of the Legitimi client simply because it is not running.

Typically, exploitation of a computing device follows a pattern of reconnaissance first; followed by probing and attacking potential known exploitable holes in the device’s applications and operating system. One of the reconnaissance techniques used is a tool that identifies what ports are open. It is these open ports that are often utilized by the attacker to probe the computing device for potential weaknesses.

It should also be noted that the calling of the Legitimi Client is conducted during a session initiated by the end user machine and using a Secure Socket Layer (SSL) connection. The resulting inbound call to a specific port results in the Legitimi Client executing its program. The SSL session protects the invocation of the Legitimi Client. While in the session it is extremely difficult for an outside party to interject themselves into the transmission to try an exploit the Legitimi Client.

When the Legitimi Client is asked to execute, it is loaded into memory, computes the computer DNA and then opens an OUTGOING HTTP or HTTPS connection. This connection may be directly with the Authentication server or with the site utilizing Legitimi. Once the connection is established the Legitimi Client sends the DNA payload and closes the connection. Typically the payload delivery takes less than one (1) second. This behavior does not permit an outside party to exploit the Client.

In addition to the behavior of the Legitimi Client the actual plugin is constructed in such a manner that makes any attempt to reverse engineer the plugin extremely difficult. The plugin is approximately 150 KB in size. The Legitimi client was developed in C/C++ with a portion of the code written in assembler and proprietary languages.

How will End Users respond to a software download?

Consider some recent demographics concerning online banking customers. The following data was presented in an article published by comScore, an Internet marketing research company. The data was derived from comScore's panel of over two million online consumers. Additional information was gathered through a survey of 2,124 consumers given in March of 2005.

“Key demographic factors affect a consumer's propensity to bank on the Web. Longtime Internet users are more likely to bank online. Banking customers with less than a year logged on the Web are 19 percent less likely to use online banking than those with five or more years of experience. Households with an income of less than \$50,000 are 10 percent less likely than households making more than \$100,000. Seniors, 65 years or older are 18 percent less likely to bank online than 25 to 34 year-olds.

Dial-up users are 18 percent less likely than broadband users to actively bank online. Additionally, broadband users are twice as likely to apply for financial service products online as dial-up subscribers.”

These factors frame a view of the consumer that has more Internet savvy than popular perception portrays. It also starts framing a better online banking consumer picture which can be filled out with additional data from the Pew Internet & American Lifestyle research group, a non-profit research group in Washington DC. In recent survey data they described the following the online banking consumer to be a group of individuals, the majority of whom (94%) were aged 25-50, with 93% having more than 4 years of Internet experience, 70% having broadband connections and 92% having household incomes of more than \$75,000. Their survey also indicated that over 90% of this online banking group indicated that they had mastered many online uses including; downloading files and programs, printing web pages, opening attachments and online searches.

A final layer to the online banking consumer profile would be the vast number of like programs that are downloaded everyday by individuals fitting this age, experience and income group. To truly understand consumer behavior one only needs to see how many downloads have occurred of the recently introduced web browser, Firefox. This particular browser was touted by many security experts as the best safeguard against certain Internet Explorer exploits in early 2005. This resulted in over 150 Million downloads of this browser in less than one year. Although, there are no hard statistics as to how well this maps to the online banking consumer profile it does suggest that many people will move to a downloadable product based on security concerns.

In addition to the Mozilla Firefox downloads many other products that have over 90% penetration in the market are downloaded as either plugins or applications such as Adobe Flash, QuickTime, RealPlayer and many others.

One last remark that has significant merit is that in a survey conducted in July 2005 by Javelin Strategy and Research found that that online consumer's second most preferred method of online authentication was computing device recognition.

Legitimi Authentication Server

The Legitimi Authentication Server is responsible for the digital DNA authentication. It receives UserID and digital DNA from the Legitimi Client and compares it against the DNA associated with that UserID stored on the database.

If a matching DNA is located, it returns a positive authentication; otherwise, authentication fails. The Authentication Server has provisions to accommodate hardware upgrades. It has a set of rules that can allow changes on a subset of hardware that identifies a device. The Authentication Server (Vault) runs on Apache Tomcat 5.5 and maybe installed on a Windows or Linux server.

Legitimi's Digital DNA Database

Legitimi is compatible with all major databases currently available in the market such as Oracle, MySQL, DB2, SQL Server, etc. The digital DNA of a device is kept in a database, which is indexed by a “Realm” and a “User ID”. This database may be encrypted using RC4, TripleDES or Blowfish.

DIGITAL DNA SECURITY

The digital DNA data transmitted over the net to the Legitimi Authentication Server is protected against hacking by using data encryption and a different encryption key for each transmission



The Legitimi DNA client is protected against various forms of hacking and has provisions to handle tracing, code injection, patching, and other attack vectors. Although it is impossible to fully protect any software from being hacked, the above techniques have been employed to make the life of a hacker extremely difficult.

In case a client's internal employee(s) gained unauthorized access into the Legitimi Database Server, where all the customer information resides, they would only be able to retrieve encrypted data. Therefore, Legitimi's protection starts behind a client's firewall, at the Authentication and Database Server level.

LEGITIMI INTEGRATION

The Legitimi technology, in a web application, is generally the last test of authentication. The scripting for the deployment and authentication calls is placed on the web login page and other pages that are deemed to be high risk. Legitimi is only called after all other authentication processes have been completed, usually the authentication of the User Name and Password. Once the existing authentication standards are met the Legitimi session is called via scripting. This starts the Legitimi process. Currently Legitimi has been integrated into VB, C#, and Java environments.

DEPLOYMENT

The Legitimi technology, used in a web application, is deployed by first having the Legitimi Client loaded to the end user device. The application recognizes the browser type and downloads the appropriate plugin. The deployment of Legitimi may vary from client to client and can be made voluntary or required dependent upon the client's environment.

In some circumstances the client may elect to insure the identity of the User by presenting a number of methods including challenge/response questions, requiring the User to contact a call center or receiving a one time password via SMS. It is up to the client to support this method.

Upon installation at the end user device the application collects the first DNA sample and returns it to the Authentication Server (Vault) where it is maintained as the original Digital DNA of that device. The installation and first collection of DNA averages approximately 7 to 9 seconds dependent upon the connection and device processing speeds. When a plugin is blocked from installation, as the case of the default IE Internet Security Medium Setting, which requires User acceptance, the process generally takes no more than 15 to 30 seconds.

AUTHENTICATION

Once the plugin is installed the next login session is seamless to the User. The web login page receives the User Name and Password, which is checked for authentication. Once authenticated and prior to opening the application, a request is sent to the Vault to open a session. The Vault opens a session and sends back to the Web Server a session ID and token. The token contains the seed number for both the one time encryption key and shuffling mechanism. This is passed to the User machine via the SSL connection established at the beginning of the session.

The receipt of the information and token invokes the Legitimi Client to collect the required DNA. During this process each of the DNA items is hashed using SHA256 hashing digest. The token

information will encrypt the entire string of ten items with a 128 Bit encryption. In addition the items will have been shuffled in a random order. This happens each and every time a request for authentication occurs. This is done to prevent replay attacks. The entire package is then delivered to the Vault for a go or no go result. This result is passed back to the Web Server where it is applied to the current session. The resultant payload is approximately 150 KB in size and the calculation and response time averages less than a second from the login to the authentication.

It should be noted that the call for authentication can be invoked at anytime during the session which makes it especially effective for preventing man-in-the-middle attacks. This is controlled by embedding scripting on the pages which contain high risk transactions, such as movement of money or adding bill payees.

The Legitimi technology also allows for sessions where no machine DNA is collected, such as cybercafé or business offices, multiple users on the same machine, multiple machines for the same users and other such control settings.

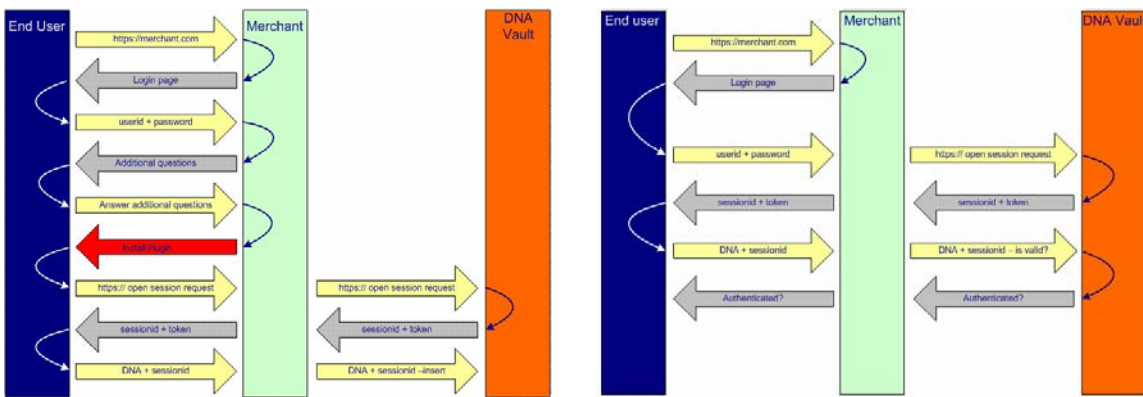
LEGITIMI FOR CELLULAR

This is a recent development of the Legitimi technology. The current population of smart phones uses Symbian OS (85%). We have developed a native Legitimi application for this OS and are also developing a Windows Mobile 2003 and 2005 Plugin for Legitimi as well. This revolutionary method of authentication will allow all online banking and ecommerce providers to extend their operations in the mobile market while still maintaining a significant security edge.

The technology works in the same manner that the standard Legitimi technology and captures device specific information including MAC address, CPU type/speed, Memory, and other unique features of the individual smart phone.

This technology will be ready for client review by 2nd Quarter 2006.

LEGITIMI DIAGRAMS



Initial Authentication

Normal Login