Commented [1]: Note that the page number is flush to the right while the title is flush to the left

Commented [2]: Note that the header on the first page and the header on the subsequent pages are DIFFERENT. On the first page it needs to say in non-Caps "Running head". Click here for how-to: https://owl.english.purdue.edu/owl/resource/560/25/

Lab 1 – CertAnon Product Description

Commented [3]: APA recommends 12 pt. Times New Roman; it is easier to read than fonts without seriffs

Great Student

Old Dominion University

Commented [4]: Be sure to include name of institution per APA requirements

CS411

Janet Brunelle

October 9, 2007

Version 1

Commented [5]: Include Version # per Professor Brunelle's requirements

Table of Contents

Commented [6]: Note that Table of Contents is centered and is not bolded or in all caps

Figures and Tables

Lab 1 – CertAnon Product Description

Commented [7]: The title should be centered on the page, typed in 12- point Times New Roman Font. It should not be bolded, underlined, or italicized.

Introduction

Commented [8]: A Level 1 heading should be centered, bolded, and uppercase and lower case (also referred to as title case).

Fraud and identity theft struck 8.9 million victims in 2006. Total annual losses jumped by $2.2 billion from 2005 to 2006, and the mean resolution time per incident skyrocketed from 28 to 40 hours per victim (VeriSign, n.d.). One of the main tools in the arsenal of identity thieves is phishing, the practice of spoofing e-mail and Web sites of consumer businesses in order to trick users into divulging information such as usernames and passwords. According to the Anti-Phishing Working Group, a record high 55,643 unique phishing sites were identified in April 2007 (APWG, n.d.). Account credentials may also be disseminated through theft by insiders or through corporate network intrusions.

Commented [9]: Throughout this paper, the student uses two spaces after a period instead of one. Please use ONE space between sentences. Using two is outdated, from the era of the typewriter.

Commented [10]: 029 Wordy expression. Consider to instead.

Such crimes are occurring more frequently as Internet users move more and more of their lives online with only passwords to protect them. Online services such as banking, stock trading, shopping, and travel planning are all account-based activities that are commonly protected by passwords. This single-factor authentication method is easily compromised and endangers the security of online accounts. Passwords are insecure, difficult to manage, and increasingly vulnerable to fraud.

CertAnon is an anonymous Wide-Area Network (WAN) authentication service conceived by the Old Dominion University (ODU) CS410 Red Group. It is designed to replace the password, the weak link in online account authentication, with an enterprise-grade two-factor authentication solution that is available to the everyday Internet user. It can be integrated with any account-based Web portal to provide an instant security boost for a site's customers. It utilizes available, affordable, and proven technology within an innovative and scalable framework. CertAnon targets the large and growing markets of individual Internet users and security-conscious businesses, and it offers clear benefits to both.

1 Product Description

Commented [11]: A Level 1 heading should be centered, bolded, and uppercase and lower case (also referred to as title case).

2.1 Key Product Features and Capabilities

Commented [12]: A Level 2 heading should be flush with the left margin, bolded, and title case.

Two-factor authentication combines something a user knows, such as a short personal identification number (PIN), with something in the user's possession. In the case of a CertAnon user, that something will be a SecurID token produced by RSA, the security division of EMC. Carried as a key fob, it generates a new pseudo-random number on a digital display every 60 seconds. When logging into an account that uses two-factor authentication, a user enters his PIN followed by the token code currently displayed on the token. This combination produces a unique one-time-use passcode that is then transmitted to a remote authentication server. At any given time, the authentication server can predict the number that appears on a token. This allows the server to confirm that the user knows the correct PIN and also possesses the proper token. These two factors together provide a much higher level of security than a password alone.

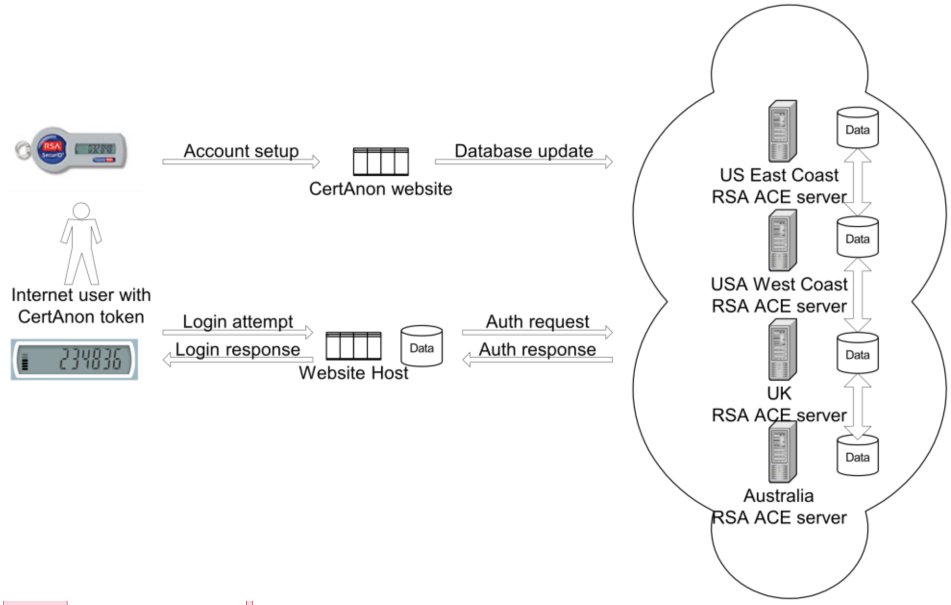
Many companies use this RSA product to secure their internal networks, and some banks and brokerages provide SecurID tokens to customers for use when accessing online accounts. Currently, many individual Internet users are reluctant to use such proprietary systems because each token only works with the account that provided it. The innovation that CertAnon provides is the ability to leverage a single token across multiple participating online accounts. A user may associate a token with any account that offers CertAnon authentication. Only one PIN needs to be remembered instead of a different password for each site. The fact that the server will only accept a given token code one time reduces the viability of phishing and keylogging attacks, providing greater security for user accounts. Also, no personal information will be collected during the token registration process. Maintaining virtual anonymity reduces the threat of data theft and offers users a high level of personal privacy.

2.2 Major Components (Hardware/Software)

Commented [13]: A Level 2 heading should be flush with the left margin, bolded, and title case.

Insert introductory text.

Commented [14]: Do not start a section with a Figure. Introduce the section with some text.



FigureFigure. Insert text.

Commented [15]: For figures, make sure to include the figure number and a title with a legend and caption. These elements appear **below** the visual display. For the figure number, type *Figure X*. Then type the title of the figure in sentence case. Follow the title with a legend that explains the symbols in the figure and a caption that explains the figure.

Commented [16]: Insert caption. Note that in the sample paper, the caption is missing. Captions serve as a brief, but complete, explanation and as a title.

Figure 1 illustrates the major functional components of the CertAnon service. It identifies four major functional pieces. The first is the RSA SecurID token possessed by an Internet user. This token will be purchased from RSA and offered for resale online.

The second functional piece is a series of synchronized authentication servers running the

RSA Authentication Manager software. When an incoming authentication request is received, an authentication server determines if the provided time-sensitive passcode (PIN + token code) is valid for the user's token. Requests can be sent to multiple authentication servers simultaneously, and the first response received will be passed back to the requestor.

The third functional piece is the CertAnon Web site. This will be written in PHP and hosted on a private server. It will utilize a MySQL database to store user account information. The site will include interfaces for token sales, token registration, account maintenance, partner site registration and encryption key exchange, and authentication module downloads.

Partner Web sites comprise the fourth functional piece of the service. They are independent online businesses that incorporate free CertAnon software modules into their Web sites. The modules will transmit login information from registered users to our authentication servers.

3 Identification of Case Study

CertAnon will be targeted at two particular markets. The first customer base consists of regular Internet users. Recent research indicates that there are 211 million consumers with Internet access in the United States alone (MMG, 2007). A primary goal will be to capture 20% of those within the next 10 years. International expansion would be a natural progression once operations in the United States are stabilized. Revenue would be derived from token sales with an anticipated unit price of approximately fifty dollars. If a critical mass of customers can be built, CertAnon could become a must-have feature for online sites to offer. Marketing materials will emphasize the increased security of the product in conjunction with the virtual anonymity of the registration process.

The second target market is comprised of security-conscious online businesses.

Commented [17]:
Passive voice: 05

CertAnon will sell batches of tokens that can be redistributed to their customers on request or as part of a concerted push to all account holders. The low implementation cost per Web site and the improved security for their customers will encourage these businesses to offer the CertAnon service. Losses from fraud reimbursements can be cut significantly without the expense of a costly proprietary system.

4 Product Prototype Description

Commented [18]: A Level 1 heading should be centered, bolded, and uppercase and lower case (also referred to as title case).

The prototype of the CertAnon service is designed to demonstrate the feasibility of using a centralized two-factor authentication system with multiple independent users and multiple independent partner Web sites.

Commented [19]: Passive voice: 05

4.1 Prototype Functional Objectives

Commented [20]: A Level 2 heading should be flush with the left margin, bolded, and title case.

The first functional objective is to successfully demonstrate the use of a middle tier, the CertAnon Web site, to extend the functionality of a two-factor authentication solution across multiple independent partner sites. Two-factor authentication credentials entered by an end user on a partner site must be linked to a particular token. These credentials will be sent to the CertAnon Web site and cross-referenced against configured accounts to identify the associated token. The token serial number and the passcode are then sent to the authentication server for validation. The authentication response is passed back through the CertAnon site and on to the partner site. It is this middle-tier innovation that allows CertAnon to offer a solution that permits a customer to securely access all participating online accounts using a single access method.

The second objective is to demonstrate the CertAnon service using a simulated hardware token that does not require any client software. In order to highlight the ease of use and crossplatform availability of our solution, we will show that the service is not limited to specific client hardware or operating systems and that it needs no special software installed by the user.

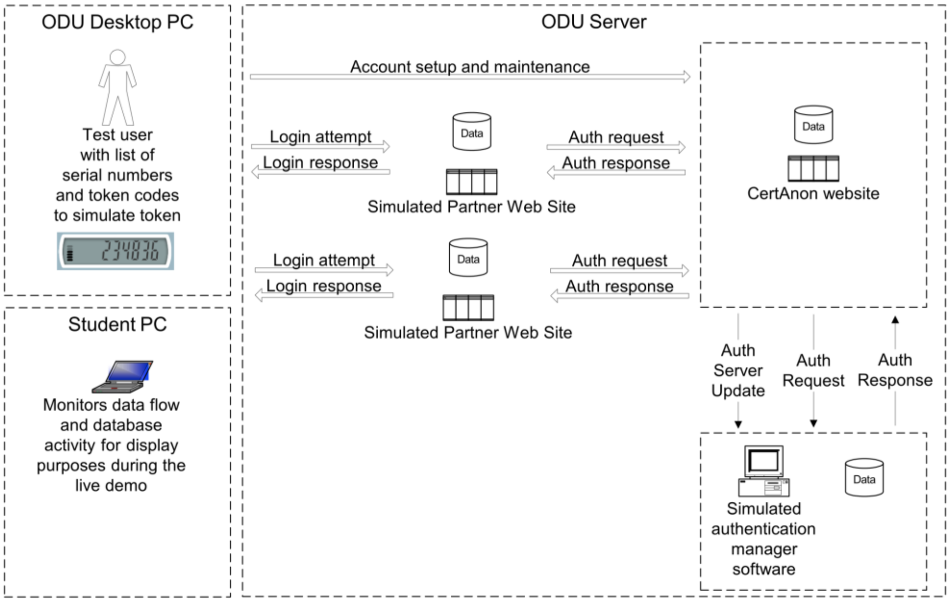
Third, we intend to demonstrate user registration and account maintenance in an anonymous fashion while still providing strong account authentication. Account access must be limited to a specific token holder without collecting or using personal information such as a real name, a street address, or a credit card number. This feature will allay consumer fears of information misuse or theft and attract additional customers who value the privacy that this provides.

The final objective is to show the ease of integration of our third party system with a potential partner Web site. Our aim is to illustrate the relative simplicity of incorporating a pre-built PHP module into an existing site in order to offer the CertAnon service. A short and straightforward integration process is an important aspect of the service and will be a valuable selling point for our commercial partners.

4.2 Prototype Architecture

Insert text.

Commented [21]: Again, a new section should begin with text, not an image.



*Figure**Figure*.

Commented [22]: For figures, make sure to include the figure number and a title with a legend and caption. These elements appear **below** the visual display. For the figure number, type *Figure X*. Then type the title of the figure in sentence case. Follow the title with a legend that explains the symbols in the figure and a caption that explains the figure.

Commented [23]: Captions serve as a brief, but complete, explanation and as a title. For example, "*Figure 4*. Population" is insufficient, whereas "*Figure 4*. Population of Grand Rapids, MI by race (1980)" is better. If the figure has a title in the image, crop it.

Figure 2 illustrates the major functional components of the CertAnon prototype and the flow of data between them. It simplifies the components shown in Figure 1 but retains the basic innovative functionality. In the prototype, the token will be simulated by a hard copy list of token serial numbers and 20-50 related token codes per serial number. An ODU desktop personal computer (PC) with Internet access and a Web browser will be used to access the CertAnon Web site and partner Web sites.

The authentication servers running the RSA Authentication Manager software will be simulated in the prototype by a Perl script running on an ODU web server. This script will be listening on a pre-defined port for authentication requests. It will utilize a MySQL database to store the same list of token serial numbers and related token codes given to the test user. It will also store the PIN chosen for each token by the user. The predefined token codes will serve to emulate the concurrent token code calculations of the RSA product while sidestepping complicated problems such as clock synchronization that lie outside of the innovative aspects of our service. When an incoming authentication request is received, the authentication server will check the database to determine if the provided passcode (PIN + token code) is valid for the given token serial number. If a correct passcode is provided, the token code that was used is flagged so that it cannot be used again. This maintains the one-time-use passcode feature of the full RSA product in our prototype.

The CertAnon Web site will be written in PHP and hosted on an ODU Web server. It will utilize a MySQL database to store user account information. The prototype site will only include interfaces for token registration and account maintenance by end users. It will also function as a middle tier between the partner sites and the authentication server. Incoming authentication requests will be associated with a token serial number based upon the partner site domain and the username. This information is then forwarded to the authentication server for validation. Authentication responses will be transmitted back to the requesting partner site.

Partner Web sites comprise the fourth functional piece of the service. Our prototype will include two simulated partner sites written in PHP and hosted on an ODU Web server. They will incorporate the plug-in module to transmit login information from registered users to our authentication server script. Each site will have a simple MySQL database to store account information.

Table 1 provides a summary of the differences between the full CertAnon service and the prototype that were discussed above.

Table 1

Commented [24]: Note the formatting for tables: Unitalicized "Table 1", new paragraph, Italicized title of table

Feature comparison between full product and prototype

Features	**Real World Project**	**Prototype**
Token	RSA SecurID key fob	Hard copy list of 20-50 valid token codes for several token serial numbers
Client Computer	Any PC with Internet access and a web browser	Lecture room PC with Internet access and a Web browser
CertAnon Web site	Hosted on an independent web server; Consists of interfaces for token sales, token registration, account maintenance, partner site registration, encryption key exchange, authentication module downloads	Hosted on an ODU server; Consists of interfaces for token registration and account maintenance
Authentication server	Four dedicated servers running RSA Authentication Manager software provide redundancy in case of hardware failure or other outage	Simulated by a Perl script running on a single ODU server with a back-end DB populated with the 20-50 valid token codes and related serial numbers; Time-sensitive generation of passcodes not simulated; One-time passcode use will be simulated; Multiple bad attempts causing account lockout will be simulated
Partner Web site	Any independent Web site incorporating our authentication modules to offer CertAnon authentication to its users	Two simulated PHP Web sites hosted on the ODU Web server and configured to use our authentication module with pre-registered user lists
Authentication modules	Plug-in modules developed for several popular technologies (PHP, .NET, etc) and made available for free on our Web site for use by partner sites	One PHP module incorporated into the two simulated partner sites
Customer support	Security questions can be answered online or by calling a supports number to unlock an account; Temporary passwords can be granted in the event of a lost/damaged token	Not simulated – these features are standard offerings of modern online services and the RSA SecurID product

TableTable

4.2 Prototype Features and Capabilities

As discussed earlier, the major innovative feature demonstrated by our prototype is the ability to permit an Internet user to securely access multiple participating online accounts using a

Commented [25]: Note the formatting: underneath the table include unitalicized "Table 1 XX title"

Commented [26]: A Level 2 heading should be flush with the left margin, bolded, and title case.

single access method. This feature eliminates the need to memorize different passwords for various online accounts. It replaces the weak link in account authentication with a secure and scalable two-factor authentication solution that is platform-independent, and it does not require a user to carry multiple tokens or install any client software. It also relieves participating Web sites of the cost and effort to implement and maintain their own proprietary two-factor solutions.

4.3 Prototype Development Challenges

Commented [27]: A Level 2 heading should be flush with the left margin, bolded, and title case.

A number of challenges and risks must be overcome during the development of the CertAnon prototype. First, the software that must be developed may not meet the required specifications. This shortfall may be due to oversight or an inability to complete it in the specified timeframe. It will be mitigated by dividing the coding labor among all team members, by following a firm development and testing schedule, and by shifting resources where necessary to avoid delays.

A second risk is that the designated ODU hardware will not support the desired software. The developers may be unable to install needed software such as Perl modules on the ODU servers. ODU system security rules may prevent certain processes from running or communicating with other network resources in the manner that has been planned. The development team will have to work closely with system administrators to achieve the desired functionality. Personal hardware might need to be provided in order to host certain functional components.

A number of other risks will be faced during the live demonstration of the prototype. The potential for corrupted or inconsistent data exists because multiple databases will be used to store token and user information. Software may also malfunction or become corrupted. Steps to mitigate this include manually validating data during testing, taking full backups of data and software needed to begin our prototype demonstration, and developing a "quick load" procedure to quickly restore everything from the backups in the event that a problem arises during the live demonstration. Additionally, adverse circumstances such as an absent team member or a network outage might be encountered during the presentation. Cross-training all team members on the various procedures for the demonstration will enable the group to overcome an absentee situation. A network outage would preclude a live demonstration of the prototype because it is essentially an Internet service. A slide show with screenshots from a prototype walk-through will be prepared as a fallback presentation mechanism.

5 Prototype Demonstration Description

Commented [28]:
A Level 1 heading should be centered, bolded, and uppercase and lower case (also referred to as title case).

Commented [29]:
Note that this section is not required for the current assignment

The CertAnon prototype demonstration will require the CertAnon Web site, two partner Web sites, and the Perl script simulating the authentication server running on an ODU server. A test user with a list of token serial numbers and token codes will be seated at the desktop PC in the presentation room. A laptop computer will be set up with software to graphically display the contents of our four databases. The demonstration will begin with an overview of the functional components and a view of the initial database contents. Code from the partner sites will also be shown to highlight the minimal coding needed to integrate the CertAnon authentication module.

Using the desktop PC, the test user will visit the CertAnon Web site and register a token using one of the serial numbers from the list. The user will choose a PIN and associate one partner account using the account maintenance interface. The user will then log into that partner site using the new PIN and one token code. Database updates will be shown after each step. Next, the user will visit the second partner site and update his account settings to use CertAnon. The user will then log into the second partner site using the PIN and a second token code.

Additional attempts will be made using a second token serial number and several invalid user names and token codes to illustrate the proper authentication behavior in each case. Log file entries will be shown on the monitoring laptop to demonstrate the data flow behind the scenes.

Glossary

Commented [30]: Note that “Glossary” is centered and not bolded or in caps

Key fob: A decorative or functional item attached to a key ring or key chain, such as an RSA SecurID token

Keylogging: The use of software or hardware to capture a computer user's keystrokes, also known as keystroke logging

Load balancing: Tuning a network to evenly distribute data among available resources

MySQL: An open source multi-user database management system

ODU: Old Dominion University

Partner Web site: Any organization with an Internet presence that contracts to use CertAnon technology for user authentication

Passcode: A type of password, often purely numeric. In the case of CertAnon, it is the combination of a user selected PIN plus the pseudo-random token code provided by the RSA token.

Perl: A high-level scripting language well-suited for process, file, and text manipulation

Phishing: The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information such as passwords and credit card, social security, and bank account numbers. The Web site is a bogus site designed to capture this user information for purposes of identity theft or other financial fraud.

Personal Identification Number (PIN): A personal identification number normally used to secure a user account

PHP: A server-side programming language designed for building dynamic Web pages

Proprietary system: A system that is used, produced, or marketed under exclusive legal right of the inventor, maker, or operator

Pseudo-random: Being or involving entities (such as numbers) that are selected by a definite computational process but that satisfy one or more standard tests for statistical randomness

RSA: The security division of EMC, a provider of corporate information infrastructure technology and solutions

RSA SecurID: A two-factor authentication solution offered by the company RSA

RSA Authentication Manager: Server-side software by RSA used to verify authentication requests and centrally administer authentication policies for enterprise networks

Single-factor authentication (SFA): The traditional security process that requires a user name and password before granting access to the user

Token: A physical device that an authorized user of computer services is given to aid in authentication, also known as a security token, hardware token, authentication token or cryptographic token

Two-factor authentication: A system of which the user provides dual means of identification, one of which is typically a physical token, such as a key fob, and the other of which is typically something memorized, such as a security code

Wide-area network (WAN): A telecommunications network with linked segments spread across a wide geographic area

References

Commented [31]: Note that "References" is centered and is not bolded or in caps

Anti-Phishing Working Group. (n.d.). *Anti-Phishing Working Group*. Retrieved September 15, 2007, from Anti-Phishing Working Group Web site: http://www.antiphishing.org/

Miniwatts Marketing Group. (2007). *America Internet usage and population statistics*. Retrieved September 17, 2007, from Internet World Stats Web site: http://www.internetworldstats.com/stats2.htm

VeriSign. (n.d.). *Online fraud stats - how safe is your e-commerce experience?* Retrieved September 17, 2007, from VeriSign Online Security Web site: http://www.verisignsecured.com/content/Default.aspx?edu_stats_body.html