Important Announcement

18 December, 2020 at 8:58 AM

Visit Back2BU for the latest updates and information on BU's response to COVID-19. Students can find additional information in the Undergraduate Student Guide and Graduate & Professional Student Guide.

Information Messages

- **Duo for Google Mail and Apps Required on November 12**

  Phishing continues to be a risk and as COVID-19 continues to impact the United States phishers are taking full advantage of the current climate. The FCC and FBI have warned of a pandemic-related surge in phishing emails and phishing websites. These campaigns prey directly on virus-related opportunities and fears. Here at BU, phishing remains our… [read more]

Understanding Authentication, Authorization, and Encryption

Authentication

- Authentication is used by a server when the server needs to know exactly who is accessing their information or site.
- Authentication is used by a client when the client needs to know that the server is system it claims to be.
- In authentication, the user or computer has to prove its identity to the server or client.
- Usually, authentication by a server entails the use of a user name and password. Other ways to authenticate can be through cards, retina scans, voice recognition, and fingerprints.

- Authentication by a client usually involves the server giving a certificate to the client in which a trusted third party such as Verisign or Thawte states that the server belongs to the entity (such as a bank) that the client expects it to.
- Authentication does not determine what tasks the individual can do or what files the individual can see. Authentication merely identifies and verifies who the person or system is.

Authorization

- Authorization is a process by which a server determines if the client has permission to use a resource or access a file.
- Authorization is usually coupled with authentication so that the server has some concept of who the client is that is requesting access.
- The type of authentication required for authorization may vary; passwords may be required in some cases but not in others.
- In some cases, there is no authorization; any user may be use a resource or access a file simply by asking for it. Most of the web pages on the Internet require no authentication or authorization.

Encryption

- Encryption involves the process of transforming data so that it is unreadable by anyone who does not have a decryption key.
- The Secure Shell (SSH) and Socket Layer (SSL) protocols are usually used in encryption processes. The SSL drives the secure part of "http**s**://" sites used in e-commerce sites (like E-Bay and Amazon.com.)
- All data in SSL transactions is encrypted between the client (browser) and the server (web server) before the data is transferred between the two.
- All data in SSH sessions is encrypted between the client and the server when communicating at the shell.
- By encrypting the data exchanged between the client and server information like social security numbers, credit card numbers, and home addresses can be sent over the Internet with less risk of being intercepted during transit.

Using authentication, authorization, and encryption

Authentication, authorization, and encryption are used in every day life. One example in which authorization, authentication, and encryption are all used is booking and taking an airplane flight.

- Encryption is used when a person buys their ticket online at one of the many sites that advertises cheap ticket. Upon finding the perfect flight at an ideal price, a person goes to buy the ticket. Encryption is used to protect a person's credit card and personal information when it is sent over the Internet to the airline. The company encrypts the customer's data so that it will be safer from interception in transit.
- Authentication is used when a traveler shows his or her ticket and driver's license at the airport so he or she can check his or her bags and receive a boarding pass. Airports need to authenticate that the person is who he or she says she is and has purchased a ticket, before giving him or her a boarding pass.
- Authorization is used when a person shows his or her boarding pass to the flight attendant so he or she can board the specific plane he or she is supposed to be flying on. A flight attendant must authorize a person so that person can then see the inside of the plane and use the resources the plane has to fly from one place to the next.

Here are a few examples of where encryption, authentication, and authorization are used by computers:

- Encryption should be used whenever people are giving out personal information to register for something or buy a product. Doing so ensures the person's privacy during the communication. Encryption is also

often used when the data returned by the server to the client should be protected, such as a financial statement or test results.
- Authentication should be used whenever you want to know exactly who is using or viewing your site. Weblogin is Boston University's primary method of authentication. Other commercial websites such as Amazon.com require people to login before buying products so they know exactly who their purchasers are.
- Authorization should be used whenever you want to control viewer access of certain pages. For example, Boston University students are not authorized to view certain web pages dedicated to professors and administration. The authorization requirements for a site are typically defined in a website's .htaccess file.
- Authentication and Authorization are often used together. For example, students at Boston University are required to authenticate before accessing the Student Link. The authentication they provide determines what data they are authorized to see. The authorization step prevents students from seeing data of other students.

Links for learning how to set up authorization, authentication, and encryption

- Using Authentication and Authorization on BU's Institutional Web Servers [www.bu.edu, people.bu.edu]
  - Restricting Access to Web Content [at Boston University]
  - Authentication and Authorization via Internet Information Server (IIS)
- Configuring Your Web Server to use encryption
  - Building a Secure RedHat Apache Server HOWTO [applicable to BU Linux]
  - Configuring SSL for Apache 2.0
  - How to Set Up SSL on a [IIS] Web Server
- SSH Clients
  - Windows (Putty)
  - MAC OS

- Web Browser Security
- Securing Windows Systems
- Securing UNIX and Linux Systems
- Securing Web Servers
- Securing Web Applications
- Securing FTP Servers
- Securing Printers
- Server Security
- Choosing and Requiring Good Passwords
- Virus Removal Advice for Guests
- Identifying and Reporting New Viruses
- Securely Using Remote Desktop
- Understanding Authentication, Authorization, and Encryption
- Implementing an Information Security Review

Contact Us

- 617-353-HELP (4357)
- ithelp@bu.edu

- •Contact Us
- •Feedback
- •Privacy Statement

- RSS
  ATOM
- @buithelp
  @bumcit
  @edtechbu
-