CERN-AS-97-005

The implementation of Security for microBHT

James Purvis
2 February 1997

Summary

With the construction of LHC and the funding of up to 80% of the new experiments (ATLAS and CMS) to come from outside CERN it is important that budget responsibles have secure and instantaneous access to view their financial data which is managed by CERN. MicroBHT (μBHT)is a system specifically designed to cater for these requirements. MicroBHT provides for secure web-based access for Teams (and other budget holders) to view their financial data. The security mechanism for μBHT which is detailed in this paper uses the standards adopted by banks and other institutions who use the web with maximum security and confidentialy of for both their data and their customers.

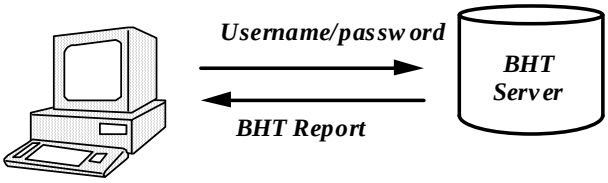
Goals

The purpose of the BHT (Budget Holders Toolkit) software is to provide Budget Holders with ergonomical access to their budget data. The purpose of μBHT (microBHT) is to provide a limited sub-set of this functionality to budget holders not normally present on the CERN site (e.g. RAL in the UK, MIT in the US, JINR in the SU). Given the sensitive nature of this data and the requirements for accessing it outside of the CERN site, the purpose of this memorandum is to define the security mechanism which will be implemented in BHT.

Background

The current BHT system has two key variants:

1. Intranet Excel Based BHT Client (running on Mac and PC).
This is what most people call "BHT". It runs on the Macintosh and PC and only works inside the CERN environment. It implements the following security schema:

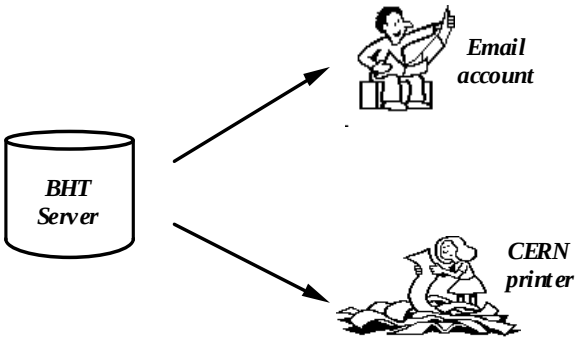


To access BHT data in the above fashion users must :

1. Complete a BHT registration form
2. Have the form signed by their DPO
3. Send the form to AS

The username & password will allow them access to the transactions for their budget codes and no others. Currently around 600 people use this system.

2. Batch based BHT Server.
For people do not have access to Macintosh or PC they can request that their budget information be sent to a local printer. In 1995, on request from FI division, this mechanism was extended to include the ability to send the data to email accounts for Team Budget Holders. This schema is illustrated below.



Users following this system do not "connect" as such to BHT. They simply receive an email, or a printed statement (with email notification) once a month after the bookclosing. This system effectively replaces the printing of the S-lists which existed prior to 1992. Currently around 300 people use this mechanism.

Weaknesses with the current system(s)

There are many weaknesses of the current systems, namely :

- Team Leaders cannot use standard BHT client outside of CERN
- Team Leaders only have their figures updated once a month
- BHT runs only on the Mac and PC (and not on Unix etc)
- Email poses a security risk
- Printouts left on printers are a security risk

What is *µBHT*?

The World Wide Web was invented at CERN with the goal of aiding the dissemination of information amongst physicists. MicroBHT is a secure Web based version of a subset of the Budget Holders Toolkit.

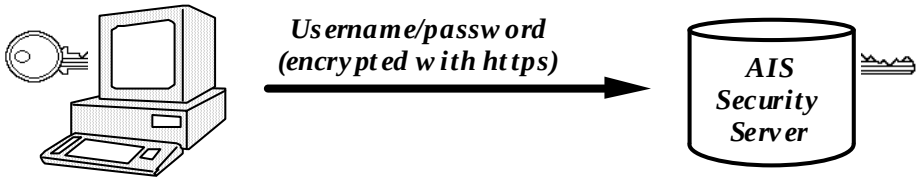
Security implementation in *µBHT*

MicroBHT implements a three-tier security architecture for :

- User authentication (is the user who they say they are?)
- Authorisation (does the user have access to BHT?)
- Data Protection (does the user have the right to see these accounts?)

Step 1 : Logon

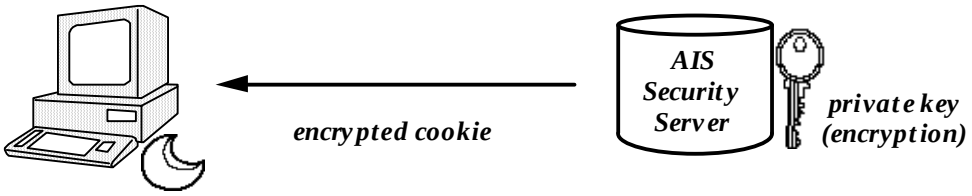
A micro BHT user must first identify themselves with their username and password. This information is transferred using the https protocol (for secure communications) which means that the data which is transmitted is encrypted over the net using an asymmetric key algorithm.



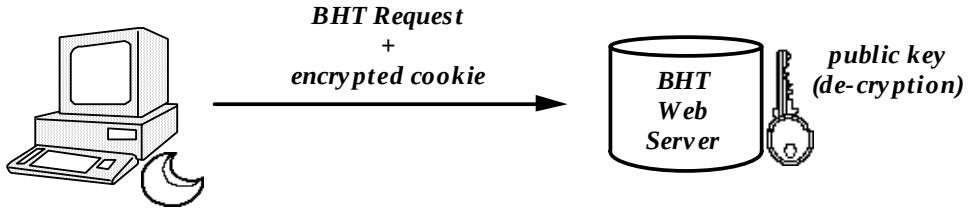
Even if somebody "listened" to the network and copied down the encrypted password, they could not use this encrypted password themselves because the "key" to decrypt and encrypt the password changes each time a communication is re-established. This is the same security mechanism used to implement secure credit card transactions on the web.

Step 2: Authentication

The security server verifies the username and password, and if valid, will encrypt a "cookie" using an asymmetric key algorithm. This cookie is effectively an "authentication stamp" which is given to the client that has successfully logged on. Every time the client wishes to perform a microBHT operation, the client must show this authentication stamp (i.e send the encrypted cookie) to the server.



Step 3: Authorisation
The BHT user now asks to see his/her account by making a BHT request. This request is sent to the BHT Web Server together with the encrypted cookie. If the encrypted cookie is not present, then the user will not be able to connect to the Web Server.

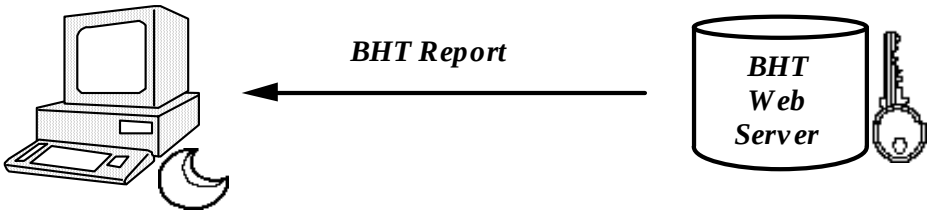


The BHT web server will decrypt the cookie and determine the userid of the requester from the decrypted cookie. This cernid is used to determine and apply BHT access control to the data based upon the CERN organic hierarchy.

Step 4: Protection
If and only if:

- the user has connected with a valid username and password
- an encrypted cookie has been sent with the BHT request
- the BHT request is for a cost centre to which the user has access

then the results of the query will be transmitted to the user.



Conclusion
The security mechanism implemented for microBHT is considerably tighter than the mechanism which exists for the current version of BHT. The current version of BHT users a single tier architecture and makes no use of data encryption whatsoever. MicroBHT users a three tier architecture and uses an asymmetric key algorithm to protect the data being communicated, as well as to protect the authentication of the user. With the web being established as a means of dissemination of confidential as well as public information, it is felt that these additional security constraints are necessary in order to protect the interests of our users who are financing a large part of the LHC experiments.

Additional Security Features

In accordance with the guidelines lay down in Administrative Circular Number 10 Revision 2, particularly section IV (general principals related to computerised files), a logging mechanism will guarantee that all access to BHT data may be traced. All data will be read-only and hence non-modifiable by the BHT user. Any discrepancies should be reported to FI division.