HARDWARE PROTECTION OF WEB BASED APPLICATIONS

Ivan Haralampiev Furnadjiev

Department of Electronics, Technical University of Sofia

8, Kliment Ohridski St.,1756 Sofia, Bulgaria, phone: +359888966871, ihf@tu-sofia.bg

Keywords: Web-based software, client-server technology, hardware protection

The paper describes a system, based on hardware protection (dongle), which handles license distribution, acquisition, and management, as well as protecting software from illegal or improper use. Structure of the protected software is shown. The technology is specifically targeted towards Web based Java applications.

1. INTRODUCTION

In today's rapidly changing world of advanced technology, computers and the software to run them have become integral parts of our society. The issue of software piracy, the illegal copying or duplication of software, is rapidly growing in importance. Software piracy, precisely defined, is the unauthorized use, duplication or theft of software.

Hardware protection can offer stronger encryption schemes but the decryption process tends to be less well protected. The problem is that a potential hacker knows where the hardware is and can therefore intercept calls to it. Hardware based encryption is used for protecting highly sensitive information in transit. The CD is very difficult to read because it carries only the encrypted data, the decryption hardware is sent separately. Some dongles don't encrypt the data, they simply protect the application software. They therefore cannot protect the content of a multimedia product from piracy. Hardware meters have the advantage that they are portable. Whereas software meters are bound to one machine. Hardware systems' greatest problem is the very fact that they are hardware. Users must therefore install the hardware and vendors must buy, store and distribute it. There can also be problems if the user wants to run several encrypted programmes because they have to attach several devices to their machine. Some hardware finds it difficult to work with latest generation of fast processors and low power portables.

Currently, hardware protection is the most reliable and convenient method of protecting medium to high cost off-the-shelf software. This method is very strong to attacks and does not limit the usage options for a legal software copy. Usage of this method is economically beneficial when protecting programs that cost no less than 100 USD, since even the cheapest dongles increase the cost of software by 20 to 25 USD.

Dongles are mostly used for protection of commercial software: accounting and inventory management applications, legal and corporate systems, building construction estimates, CAD systems, electronic reference systems, analytical software, ecological and medical software, etc. Development of such software require

heavy investments, therefore the cost of software is high as well, and the loss from illegal distribution is considerable. In this case dongles present the optimal protection means.

Main question here is: "Is it possible to protect Web based application from unlicensed use with hardware protection based on dongles?", and the answer is: "Yes!".

In this paper is described a system based on hardware protection (dongle), which handles license distribution, acquisition, and management, as well as protecting software from illegal or improper use. The technology is specifically targeted towards Web based Java applications and provides following main benefits:

- Reducing unlicensed use
- Stronger encryption scheme – this system is based on WIBU-BOX dongle.
- Most reliable and convenient method of protecting software
- Making highly effective software evaluation programs possible
- Ease of use
- Platform independence.

2. IMPLEMENTATION MODEL

The protected Web system contents two functional related modules:

- Protected Web-based application
- Hardware protection module based on dongle

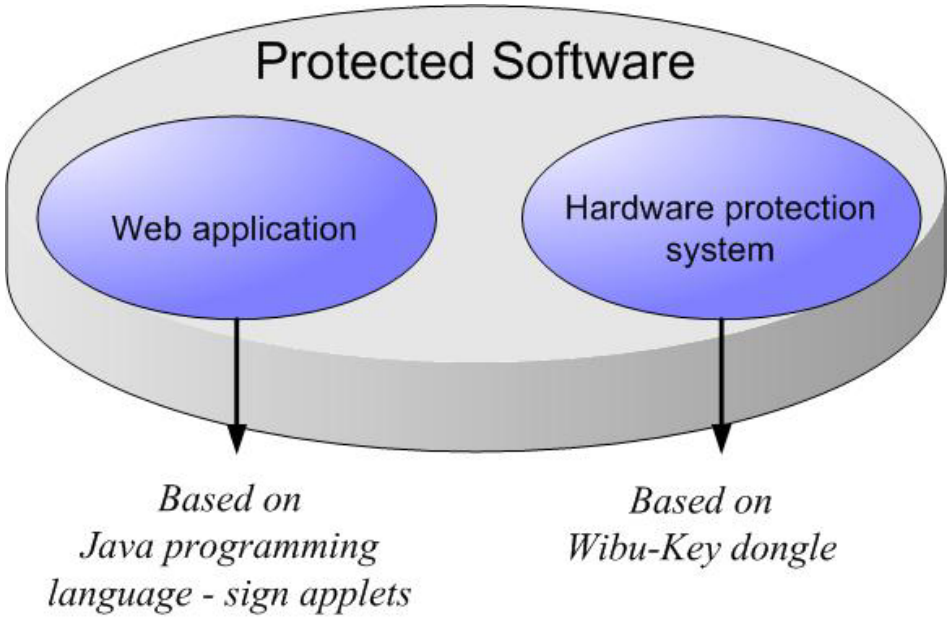

Figure 1: Protected Web-based software

The first module is a Web application based on Java programming language [1]. The protection from illegal use of the software is accomplished by embedding dongle validation applets in some key point of the Web application (e.g. menu applet, which

provides access to application content). The validation applets check trough JNI (Java Native Interface) the dongle before granting access to the requested content.

The second module is a secure protection system. In the developed protected Web-based system WIBU-BOX dongle from German company "WIBU-SYSTEMS" AG is used [2].

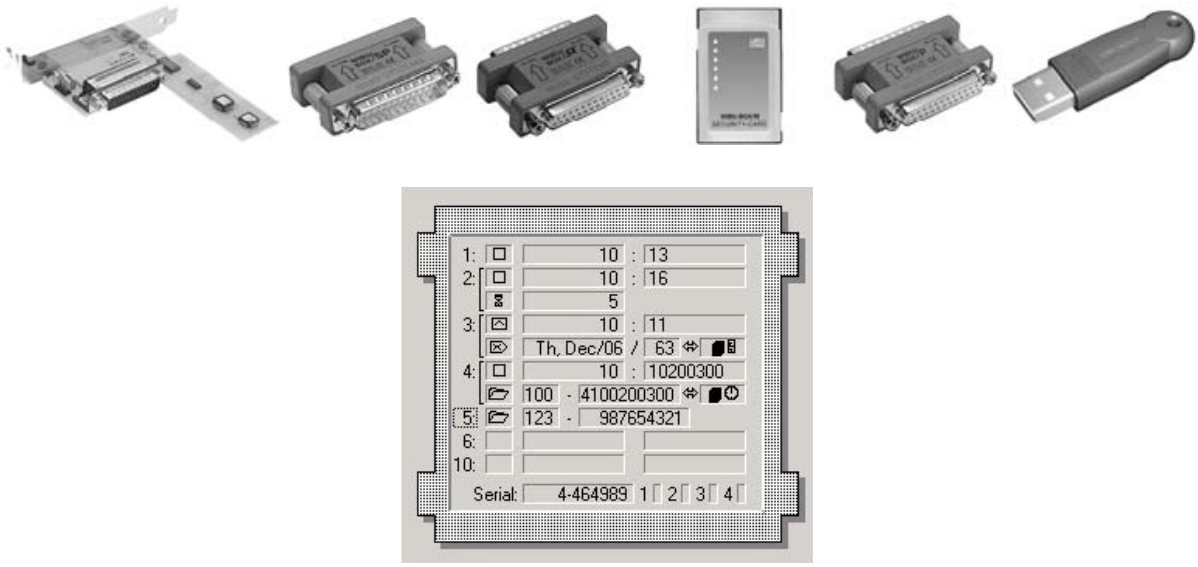

Figure 2: WIBU-BOX – secure protection system

It provides the following licensing features:

- The protected program can use a locally connected WIBU-BOX as well as a WIBU-BOX in the network.
- Pay-Per-Use – ability to count program start (Limit Counter)
- Expiration Dates - makes it possible to realize a time limit for demo
- Maximum number of concurrent users
- Protection of Modular Software
- Huge license management

3. STRUCTURE

The structure of hardware protected Web application is shown on Figure 3. On the client site standard Web browser starts Web application. Signed Java dongle validation applet, embedded in HTML page performs a lookup though Java Native Interface and WIBU-BOX native driver for local or network installed dongle. Once the dongle is found, validation applet checks the stored licenses in the dongle for correctness. If the result of this check is positive it will grant access to the requested content.

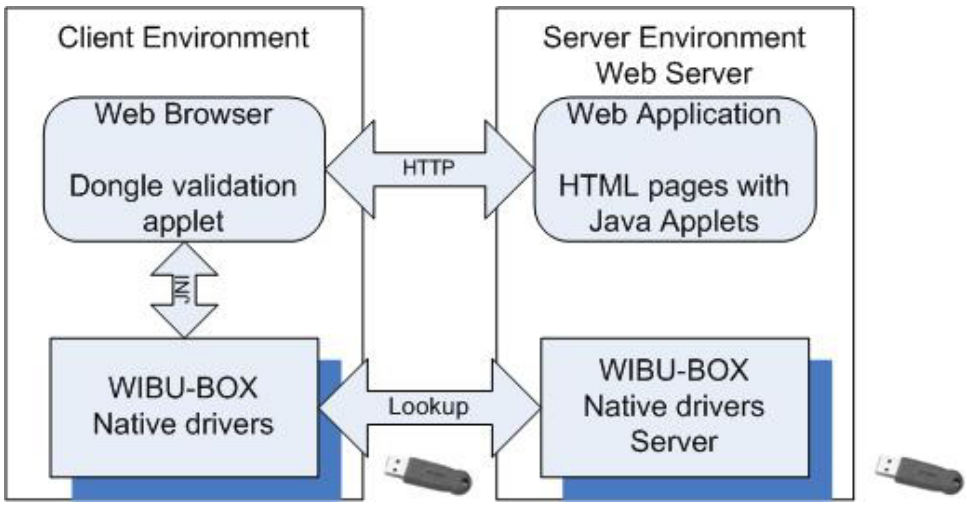

Figure 3: Structure of hardware protected Web application

4. PROTECTION SCENARIOS

Depends on where the dongle is attached, 3 different protection scenarios are recognized:

- Single user protection (Figure 4) – dongle is attached to every single user PC, laptop or Tablet PC. This approach has one big disadvantage – every user must have its own dongle.

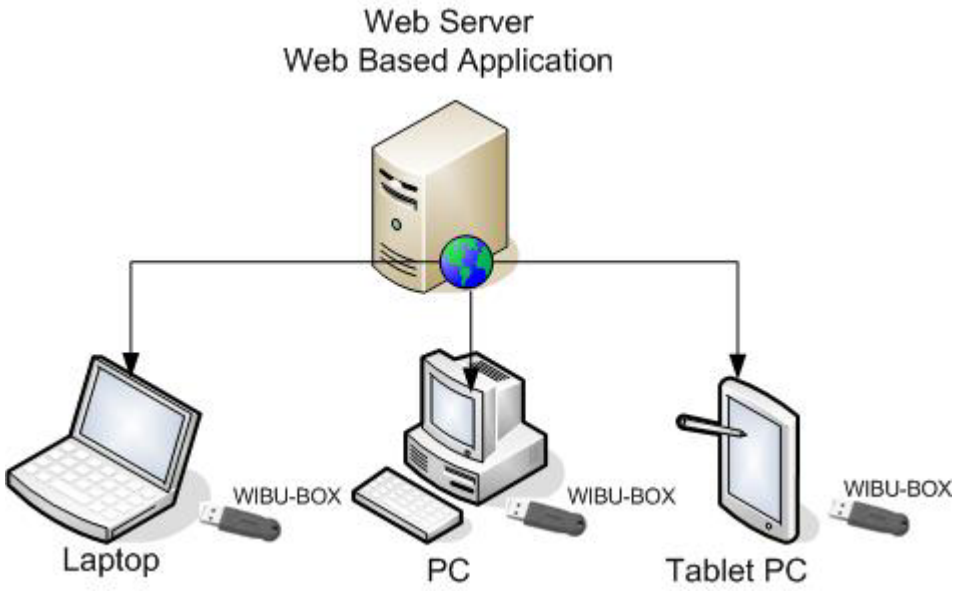

Figure 4: Single user protection

- Multiple user protection with local intranet server (Figure 5) – dongle is attached to local intranet server – useful to protect Web application in small network.

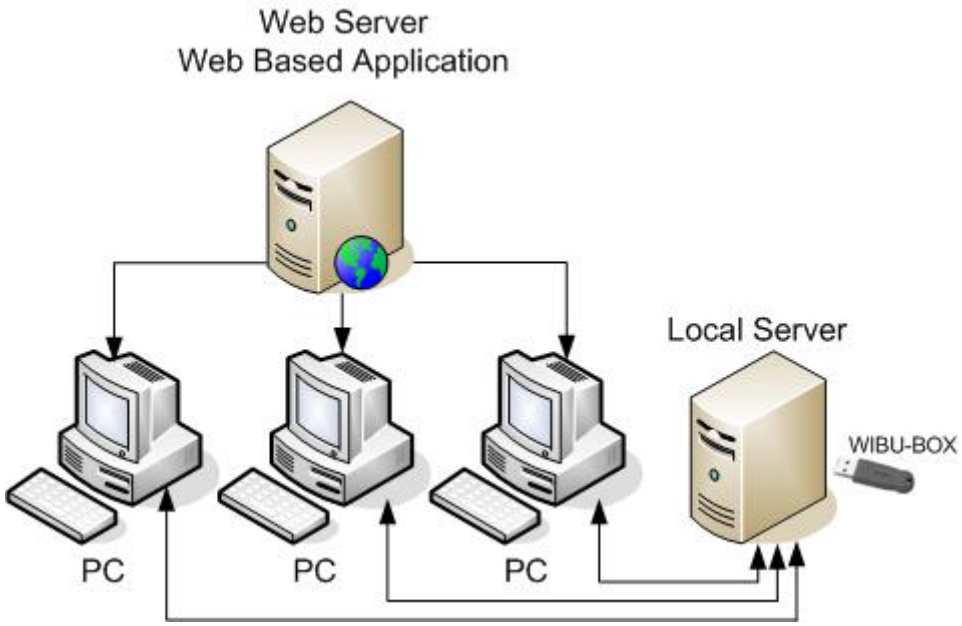

Figure 5: Multiple user protection with local intranet server

- Multiple user protection with application server (Figure 6) – dongle is attached to application server, where the Web application comes from – useful to protect Web application over Internet.

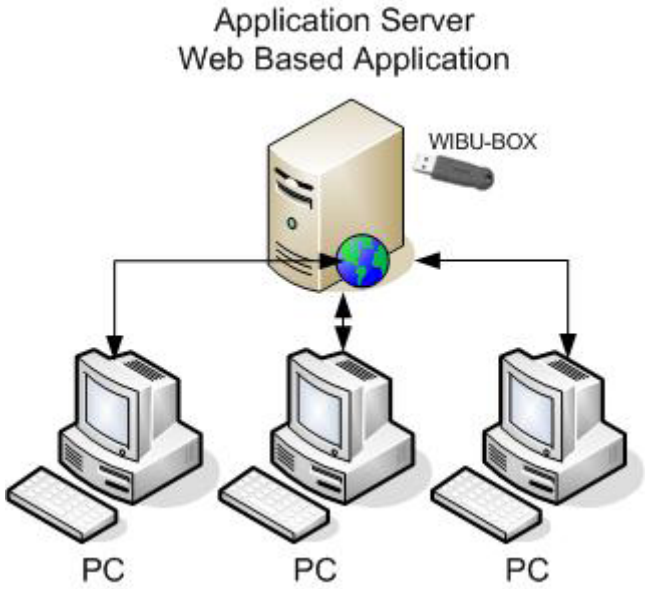

Figure 6: Multiple user protection with application server

5. EXAMPLE

The screen-shots of the Web-based application, which uses this protection system, is shown in Figure 7. The dongle validation applet is implemented as menu applet, which provides application navigation.

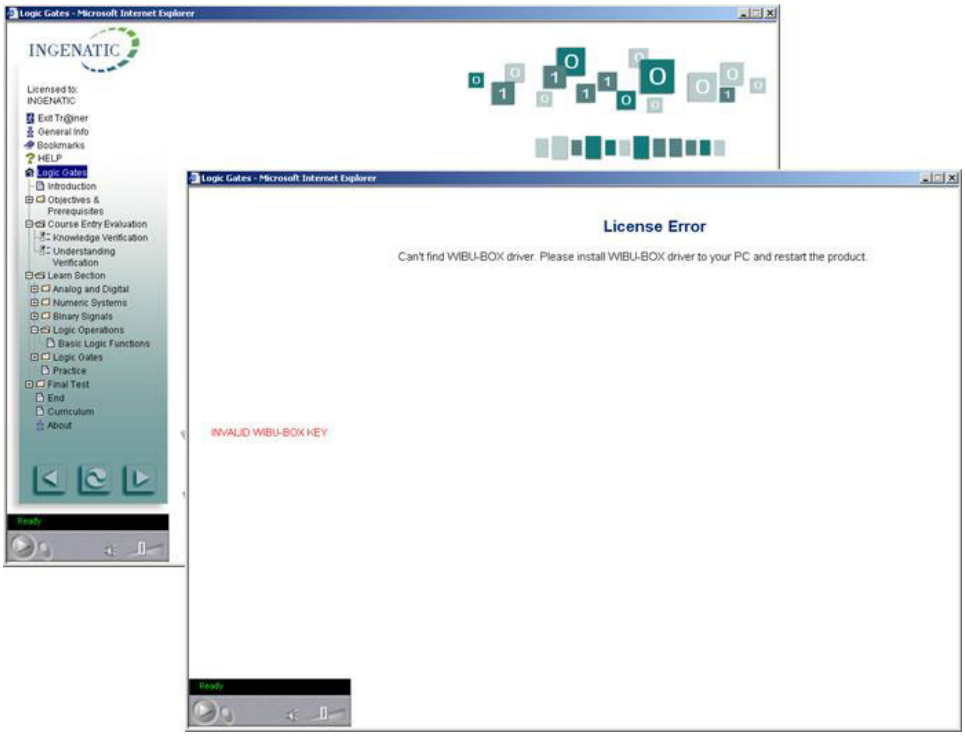

Figure 7: Protection technology in action

6. CONCLUSION

Hardware protection technology for Web based application has been developed, which has the following main features:

- Most reliable and convenient method of protecting software;
- Flexible software protection (time limited evaluation licenses, custom selected features licensing, single user and network licenses);
- Flexible control over the product's features/options;
- Centralized license management;
- Highly effective software evaluation programs possible
- Platform independence
- Advanced encryption algorithm

7. REFERENCES

[1] Java™ 2 Platform, Standard Edition (J2SE™), http://java.sun.com

[2] Secure protection system – WIBU-BOX - http://www.wibu.de

[3] I. Furnadziev, V. Tchoumatchenko, I. Astinov, Licensing Technology for Web Based Applications, Conference ELECTRONICS'2000, Book 1, pp. 11-15, 2000