Modem Port Watch Dog

Product Overview

16. February 2001

GreenHouse
Software & Consulting

Karl-Heinz Weber
Heinrichstraße 12
D-45711 Datteln/Horneburg
Germany

What is Modem Port Watch Dog?

Modem Port Watch Dog (MPWD) is an authentication and session control tool. It secures dial-up ports as well as TCP/IP TELNET ports, and enforces a Challenge/Response handshake to authenticate a user. Challenge/Response is the strongest authentication method currently available.

In addition to this main feature, MPWD is able to trace all terminal I/O data, take action when a session is inactive, and clean-up a session.

The standard authentication mechanism on Tandem systems, supported by either GUARDIAN or SAFEGUARD, is based on static Passwords.

What is Wrong with Passwords?

How can we tell that a user is who they claim to be? Traditionally, this is done with Passwords. One problem with Passwords, even when they are encrypted on the host, is that they are vulnerable during entry. They are very easy to intercept via wiretaps, Trojan horses on the host system, or monitoring on the host system.

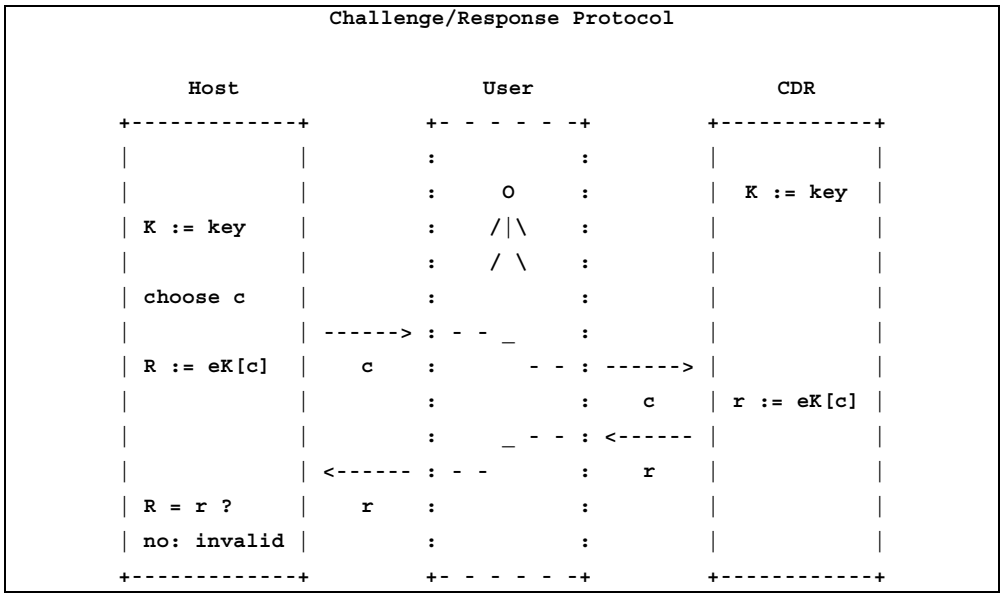
Other problems with Passwords include people writing them down, giving them to their friends or strangers, never changing them, picking ones that are easy to remember or as short as possible, etc. Sometimes vendors supply Passwords with the system which then become instantly available on hundreds of computerized bulletin boards. Quite often initial Passwords supplied with user accounts are merely the name of the user. These issues have resulted in solutions such as Password generators, system-selected Passwords, forced Password changes, Password history files, minimum-length Passwords, etc.

Fundamentally, these solutions can only help slightly. Users always try to make their Passwords as simple as possible and change them as infrequently as possible. Criminals know this and are very proficient at searching through common names, dates, easy keyboard patterns, single characters, and dictionaries while breaking into systems. (There are only about 1000 words in common English; with a thousand guesses, you are very likely to find a password.)

What Can We Do?

Luckily, a solution exists which solves these problems and even eliminates the need for users to have Passwords: Challenge/Response authentication. All Challenge/Response systems are based on the principle: "if you are who you say you are, you should have a challenge/response device and be able to correctly encrypt a random number that I send to you."

The basic protocol is:



Where:

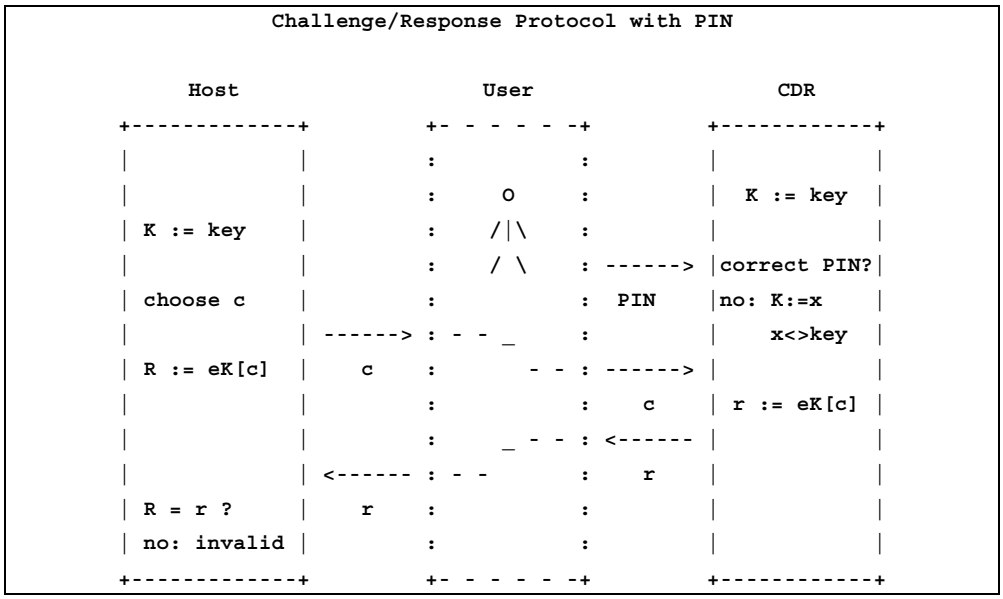
- CRD = Challenge Response Device
- K = key for this user
- c = challenge value
- eK[c] = encryption under K of c
- r = response value

When you use Challenge/Response authentication, recording a session does not benefit a criminal because the challenge is randomly chosen each time. Even the user doesn't know what the proper Response is to a particular challenge. It's like having a new password each time you log on and not knowing what the next one will be.

The problem with this simplistic system is that a criminal can still steal a Challenge Response Device and pretend to be the rightful owner.

This is solved by having a secret PIN (Personal Identification Number) to activate the Challenge/Response device.

The protocol becomes:



Now, even if someone steals the Challenge/Response Device, they cannot activate it without the PIN. Even if they guess PINs, the Challenge Response Device doesn't indicate whether they have entered a correct or incorrect PIN.

This is the level of security that we need. The three basic ways of identifying someone are by:

1. What they are.
2. What they have.
3. What they know.

Good security practice dictates that a user should have at least two of these three. Having the Challenge/Response Device and knowing its PIN are numbers 2 and 3.

Atalla's Challenge Response Device

The Atalla Challenge/Response Device (ACR) (or compatible device) is a small hand-held device which contains the functions necessary to generate responses to challenges posed by a host computer during session establishment (logon). The Challenge/Response algorithm used is based on the Federal Data Encryption Standard (DES) and includes some Atalla proprietary functions. Since these proprietary functions cannot be divulged, they are provided in object form only.

ACR Devices are capable of storing only one key and one PIN. A duress function is implemented in MPWD. Of course, if an ACR is stolen, the owner should still inform the appropriate authorities immediately.

The MPWD Solution

MPWD supports the Challenge/Response Authentication mechanism, using the Atalla Challenge/Response or compatible Devices.

MPWD has the following benefits:

- Display of customized early banner text before the authentication hand shake takes place.
- Minimum terminal I/O during the authentication process (hackers do not know to which system they are talking).
- Eight digit (decimal) Challenge and 8 digit (decimal or hexadecimal) Response.
- Display of customized late banner text.
- Support for generic users (no system known ID or password required) including complete password management.
- Passwords can be phrases up to 256 bytes long.
- Users do not need to be system users, but can be application users.
- Mapping of application users to GUARDIAN users.
- Active/Freeze status for user records.
- Specification of number of parallel sessions per user.
- Restricting a user to one device (X.25 DTE address, IP address, terminal name) at a time.
- Device control (IP address, DTE address, terminal name).
- Authentication parameters configurable based on user, or the device/port used.
- Failed logon timeout or freeze penalty, based on the user or the device logged on from.
- Session inactivity time-out.
- Session tracing (input, input/output).
- Configurable number of authentications a user might do before being automatically frozen (1 to 9).
- Unlimited number of authentication time windows, based on day of week.
- Configurable resources start when authentication is successful.
- Duress function with display of customized text.
- Multiple User-to-Resource relationships.
- Display of user available resources in one screen, selectable with a keypress.
- Log of all authentication attempts (session start and end).
- Event log.
- EMS event generation.

MPWD's Development and Run Time Environment

- MPWD is developed on a Himalaya Type System K122 and S7000, running D45 and G06.06.
- It runs on GUARDIAN Dxx or better only, and supports all GUARDIAN Dxx features, like HighRequesters, or starting a resource in HighPIN.
- It does NOT need SAFEGUARD.
- It needs to be licensed, because it runs PRIV code.

Requirements

To make use of all of MPWD's features, the user has to possess an Atalla Challenge/Response device. This device is about US$ 70 per unit. The algorithm to check the validity of a Challenge/Response number pair is done within the MPWD software. An Atalla security processor (e.g. A7000) is NOT required.

MPWD Subsystems

MPWD comes with the following subsystems:

- Challenge/Response device initialization program (INITACR).
  The supported devices are Atalla Challenge/Response Devices, or compatible devices.
- Test program to test Challenge/Response Devices (CRDCOM).
- PATHWAY application to maintain the MPWD database (PATHMAKER generated).

Example MPWD Session

When MPWD is controlling the authentication of a session, it displays an 'early banner' and prompts the user for an ID:

```
YOU ARE ENTERING A CONTROLLED SYSTEM. UNLAWFUL ENTRY INTO THIS
SYSTEM
BY INDIVIDUALS, NOT SPECIFICALLY AUTHORIZED, IS A CRIMINAL
OFFENSE.
VIOLATORS WILL BE PROSCECUTED.

ID
```

The user has to enter their ID as stored in USData. The ID is a case sensitive string up to 32 bytes long.

After the ID is entered, MPWD displays the Challenge to the user. This is an eight digit decimal number, displayed in the 12-34-5678 format:

```
ID Weber_Carl
-> 94-73-3896
```

Then the user is prompted for the Response:

```
<-
```

A valid Response can only be calculated with the user's Atalla Challenge/Response Device.

```
ID Weber_Carl
-> 94-73-3896
<- 663cfc03
```

A correct Response to the Challenge starts the resource defined for the user on the host. The resource can be any program, like a PATHWAY application, or TACL. A TACL is started as already logged on with the GUARDIAN-ID that is defined for the logical user:

Before the resource is started, the user is prompted to accept the second (late) Banner text displayed.

```
ID Weber_Carl
-> 94-73-3896
<- 663cfc03

MPWD (120) - T7172G06.AAX - (01Sep2000)   System \BEECH
Copyright (c) GreenHouse Software & Consulting 1994-2000

*************************************************************************
*                                                                       *
* This is a private system operated for GreenHouse Software & Consulting *
* business. Authorization from GreenHouse Management is required to use  *
* this system.  Use by unauthorized persons is prohibited.              *
*                                                                       *
*************************************************************************

Do you want to continue (y/N)?y
 *** WARNING - all INPUT is logged
Last MPWD logon:   04Sep2000, 13:04'32
Starting Resource: $SYSTEM.SYSTEM.TACLH
System ID:         GHS.CARL

TACL (T9205D46 - 30JUL1999), Operating System G06, Release G06.06
COPYRIGHT COMPAQ COMPUTER CORPORATION 1985,1987-1999
CPU 1, process has no backup
September 11, 2000 11:39:25
(Invoking $SYSTEM.SYSTEM.TACLLOCL)
(Invoking $GHS1.SECOM.TACLCSTM)
$GHS1 SECOM 1>
```

In addition to starting a resource, MPWD can display a menu of resources the user can choose from by pressing a function key:

```
                    Main Menu for Carl Weber
                   =========================


  F1   SECOM                              SF1   High PIN TACL 2
  F2   APPL1MGMT                          SF2   SECOM Management
  F3   APPL2MGMT                          SF3   SUPER.SUPER High PIN TACL
  F4   BTX-MGMT                           SF4   Start GENERIC1 program
  F5   KEYMANAGEMENT                      SF5   WWW-SECOM Management
  F6   KEYMANAGEMENT2
  F7   Low-PIN-TACL
  F8   High-PIN-TACL
  F9   \SEQUOIA.TACL
  F10  \BEECH.TACL
  F11  \GINKO.TACL
  F12  \GINKO.PATHCOM-$GHS
  F13  ACI Managemkent
  F14  Manage Users in $ACI
  F15  Run Update
  F16  Execute NETBATCH

Your Choice (Fn, SFn, E[XIT]):
```

Example Duress Session

A special resource is called DURESS. This name directs the system to display a customized message, and to abort the session. The implementation works as follows:

The user under duress enters a specific ID for authentication. The system reacts by displaying the DURESS file, followed by a session abort, rather than establishing a valid session.

```
ID Carl_Weber
-> 09-47-6313
<- 2a51377d
      ****************************************************************
      *                                                              *
      *   Your access rights have been withdrawn.  Please contact    *
      *   operations at 02363-72566.                                 *
      *   GreenHouse Software & Consulting          (12Mai95, CW)    *
      *                                                              *
      ****************************************************************
```

At session end, or if the session aborts (for example due to a modem error), MPWD abends and closes the connection to the controlled port.

Feature List

Challenge/Response (CR) authentication	√
TimeToken (TT) authentication	√
System Password (PW) authentication	√
Generic Password (GP) authentication, supporting complete password management with functions including: - minimum length (0 .. 256 bytes) - history stack (0 .. 9,999) - may and must change period (0 .. 9,999 days) - expiration grace (0 .. 9,999 days) - enforced password change at first logon time - password length up to 256 bytes (pass phrases) - support for embedded blanks - encoded storage of passwords in ISO 10118-2 Hash Format	√
Authentication time window	√
Maximum Authentication counter	√
Grace logon, allows an automatic logon of subsequent windows within a defined time	√
Failed Logon Penalty - for a user or for a device - time out or FREEZE	√
Inactivity time-out	√
Session clean-up	√
Session input log (Log)	√
Session input/output trace (Trace)	√
Message generation to EMS system	√
MPWD event logging	√
Free configurable early BANNER	√
Free configurable late BANNER	√
DURESS function and alarming	√
Device control (terminal name, X.25 number, IP address)	√
Restricting user to the initial device	√
Limitation of number of parallel user sessions	√
TCP/IP TELNET support	√

X.25 support	√
Async. support (incl. modem)	√
GUARDIAN D40 or better	√

Delivery

- MPWD program
- DDL Source
- All Challenge/Response maintenance programs
- Documentation
- Pre-defined ENFORM queries to list the LOG and TRACE files

Escrow Agent

*Green*House Software and Consulting is willing to put all sources into escrow.

Availability

A fully functional version of MPWD is available for a 2 month trial period for free.

To make use of all functions of MPWD, at least one Atalla Challenge/Response Device is required. It can be ordered along with the test copy for $75 US per unit.

MPWD is designed, produced, and maintained by
Safe and Secure
*Green*H*ouse* Software and Consulting
Heinrichstraße 12
D-45711 Datteln/Horneburg
Germany
Phone: +49 (0)2363 72566
Mobile +49(0)172 23 18248
FAX +49 (0)2363 66106
E-Mail Info@GreenHouse.de
Home Page http://www.GreenHouse.de
PGP fingerprint 3A 32 D9 0A D1 25 54 18
11 50 24 84 66 29 2D D2

In North America contact: Computer Security Products at: Info@TandemSecurity.com

Year 2000 compliance:

MPWD is Year 2000 compliant.