Local Area Detection of Incoming War Dial Activity

Dan Powell, Steve Schuster, AT&T Labs, Columbia, Md.
Ed Amoroso, AT&T Labs, Whippany, NJ
http://www.att.com/isc/

Abstract

Cracker attack plans often include attempts to gain access to target local computing and networking resources via war dialed entry around firewall-protected gateways. This paper describes two methods for organizations to reduce this risk in environments where removal of unknown modems is not feasible. In particular, we outline a workstation-based war dial trap scheme as well as a war dial signature-based Private Branch Exchange (PBX) audit processing method.

1 Introduction

A recent article in *Fortune* chronicled the techniques used by hired security experts from the WheelGroup Corporation to demonstrate unauthorized entry into a major U.S. corporation [BE97]. After failing to compromise an otherwise well maintained and firewall protected network perimeter, their next course of action was to war dial the enterprise looking for dial access modems that might provide a means for entry around the corporate firewall. Once a modem was found that was connected to a system without security protections, it proved a minor task to crack entry into the connected computer, and to use this as a point of entry for subsequent Intranet cracking. Unobserved entry was gained which could have resulted in substantial proprietary and competitive information loss.

One issue that influences the introduction of dial access modems into a local environment is the increased maturity of firewall technology in recent years. Often in a management effort to potentially increase worker productivity, filtering of URLs to popular sites is performed by gateway administrators using simple proxy software configuration steps. This turns out to be a double edged sword for most organizations as it increases the chances that employees will use modems to connect to the Internet. Furthermore, as employees have become more mobile and as telecommuting gains in popularity, the need to access resources inside an Intranet from the outside increases as well (see Figure 1).

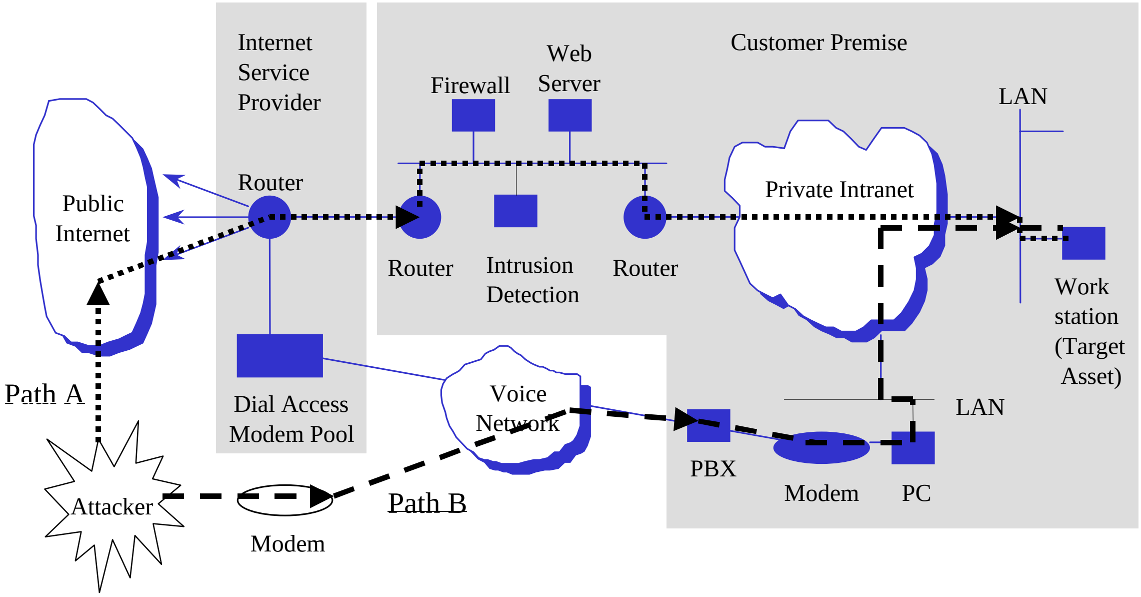


Figure 1. Typical Environment with Internal Dial Access

The biggest problem with attacks that exploit the presence of undocumented modems is that security officers will probably never know that they have occurred. Even in the face of extensive logging and intrusion detection processing at the Internet gateway (as shown in Figure 1) and other Intranet access points, no record of this entry will ever occur unless steps are taken to perform such monitoring.

Intruders take advantage of this vulnerability via a technique known as war dialing. This involves a series of computer-controlled attempts to dial into an enterprise looking for modems. Modems found in the block of specified numbers are noted in a database. Incoming war dial activity can generally be described as a series of short duration calls to a set block of telephone numbers (the numbers called may be sequential in nature or may be randomized in an effort to avoid detection). In addition, this activity may also be identified through the observation of a substantial number of calls destined for unused or unavailable extensions.

This paper describes two methods for detecting incoming war dial activity that may be useful in environments where detection and removal of dial access modems is not feasible. One method uses a workstation-based war dial trap that alarms on incoming war dial access. A second method uses profile-based PBX audit processing to detect incoming war dial access. In both cases, implementation hints of pseudo-C code are provide.

2 Dial Access Modem Risks

The risks inherent in the use of dial-access modems are considerable. In particular, dial-access modems introduce gateways from the outside into an organizational Intranet.—potentially introducing paths for crackers to compromise critical assets. The danger inherent in these modems is compounded by the use of client/server software (PCAnywhere© is an example popular package) that allows potentially unauthenticated access from the public switched telephone network. Furthermore, the attack methodology of the cracker is eased and the time required for the discovery of vulnerable modems is decreased by the use of war-dialer programs (e.g., ToneLoc) that are freely available on the Internet..

The operational cracking scenario for exploiting dial-access modems can be described generally as follows:

Step 1. Cracker identifies target organization and obtains list of candidate phone numbers; this can be done using publicly available directory information, marketing information, business cards, and simple social engineering techniques.

Step 2. Cracker configures war dialer with block of target organization phone numbers and initiates dialing; this is a simple process, but it can result in long-distance billing; crackers would likely combine this step with out-of-band hacking and toll fraud techniques to side-step the billing and to increase anonymity in the case of detection.

Step 3. War dialer returns list of phone numbers with connected modems; recent large-scale experiments, which the authors have been involved with, have resulted in an average 1.4% yield for many tens of thousands of test cases. If this figure is accurate, then an organization with only a hundred phone numbers would be expected to have between one and two connected modems.

Step 4. Cracker dials into select found modems and attempts to gain access; this step may be trivial or difficult, depending on the degree to which security protections are embedded into the server software on the modem-connected system; social engineering may not be useful here as unauthorized dial access modems are unlikely to be associated with a help-desk facility. Furthermore, it is likely that a personal use modem not authorized by local security will be installed with insufficient authentication.

Step 5. Cracker gains access and exploits connection to internal resources; the extent of the damages incurred here are dependent upon the connectivity to other internal resources from the exploited machine and the intent of the cracker who has just gained access.

3 Risk Reduction Approaches

To reduce the risks introduced by the potential presence of undocumented dial-access modems, network security administrators have several options. Among these options are the following:

Find and remove modems. This is an obvious solution that has well-defined goals, that is easy to explain and justify to management, and that is comparable to non-computing scenarios (e.g., finding and removing stolen property, etc.). Unfortunately, however, this approach is generally impossible to implement in most complex Intranet environments. The biggest problem is that it is simply too easy to establish connectivity—whether temporary or permanent—to the Internet. Furthermore, most managers typically side with employees who need to gain access for business reasons, even if it does not comply with generally recognized security practices. This does not suggest that initiatives be avoided that try to find and remove modems; it merely acknowledges that this will never result in a total solution to the problem.

Define strict policy with punishment. This brute force approach to the problem provides a non-technical solution that may be the most effective means of preventing undocumented dial access. The problem here is that certain employees will ignore the policy, especially the more adventurous ones for whom the punishment simply increases the thrill of non-compliance. So again, this solution should be included in the overall security plan, but it will not solve the problem totally.

Initiate dynamic functional protections. This type of protection includes some sort of security functionality to deal with dial access. The network manager has several options here including the following:

- *Dial access authentication software.* Many packages exist that are useful for remote access outside an Intranet. A recent article in Mobile Computing (xx) offered a useful taxonomy of these features in several popular products. The problem here is that individual users by definition control the manner in which these products are used. This leads to the risk of unacknowledged need for tight authentication or misconfiguration.

- *Modem pooling*. Putting all of the modems needed by a corporation into a defined and managed pool allows security managers to control and restrict access into and out of the Intranet. But one must recognize that this sort of centralized management may already exist through the LAN gateway; and it may be the sort of centralized management that caused an individual to install dial access in the first place. So, for those requiring unrestricted access into and out of the Intranet, modem pools for dial access will not meet their (perhaps unreasonable) expectations.
- *Intrusion detection*. The use of intrusion detection systems is typically viewed as a high-end solution requiring considerable resource investment. The administrator often must contend with the technical issues that arise in sensing and warning, with processing based on available information, and with incident response after an attack may have occurred. The major contribution in this paper is that two intrusion detection techniques are described that should not require an extensive security investment. The reader is warned that these techniques also do not completely solve the problem of dial access modems, but rather addresses a small (albeit important) piece in a reactive manner.

4 Intrusion Detection Methods

In this section, we introduce the two intrusion detection methods, providing enough detail for interested readers to produce working implementations without a great deal of effort.

4.1 Workstation-Based War Dial Trap

In this first approach, we propose identifying a workstation that can be dedicated to the process of identifying incoming war dial activity. As mentioned earlier, one indication of war dial activity is calls to unused numbers in the target enterprise. It therefore stands to reason that detecting these calls could give an indication of potential war dial activity.

One particularly easy method of detecting these calls is to place a computer that is equipped with a modem on an unused number. The computer's sole function would be to monitor the phone line. The following pseudo-code demonstrates the algorithm:

```
Wardial_analysis:
    configure modem to answer incoming calls
    for each incoming call do
    Answer Call
    Hang up the Call
    Log details to file
    Generate Alarm (if desired)
end do
```

Annotation of Algorithm:

Line (1): The modem is configured to answer incoming calls. There are two approaches, answer automatically after a preset number of rings, or monitor the modem and answer manually. To answer manually, the S0 register is set to 0 (ATS0=0), and the program should monitor the S1 register for rings. As soon as the S1 register detects a ring, answer the call. To have the monitor answer automatically, set the S0 register to a non-zero number. The S0 register contains the number of rings the modem should wait before answering. The following AT command will cause the modem to answer on the second ring: *ATS0=2*

Line (2): Process all incoming calls in a loop. This gives a real-time response to the system.

Line (3): Answer the call. If monitoring the modem manually, answer the call by issuing the ATA command.

Line (4): Tell the modem to hang up by going back on hook. (ATH0)

Line (5): Write the details of the call such as the date and time called to a file.

Line (6): Generate an alarm of some type if desired, for instance page the system administrator.

Line (7): Continue monitoring the phone line.

The algorithm discussed above can be implemented in different ways, including scripts in a communications package such as ProComm Plus, programs written in Perl, Basic, C/C++, or other languages.

There are a few issues that need to be considered when performing this type of war dial detection. First, for security reasons the computer that is being used to perform the detection should not truly provide a gateway into the Intranet. This is most easily accomplished by configuring it to be physically disconnected to the company's Intranet. A drawback to not connecting to the Intranet is that alarming options are limited, for the most part, to local log files and possibly notification via outbound calling from the modem to page the system administrator.

A second issue is where in the telephone number space to place the system to accept incoming calls. War dialers can dial blocks of numbers either sequentially or randomly. To give the earliest notification possible, it would be wise to have the system monitor the earliest available number in the block of numbers, or near a boundary in the number space, such as where the number rolls over to the next hundred. Of course this would only be beneficial for sequential war dialing.

The rudimentary system described above can be enhanced to offer additional intrusion detection functions. Two possible enhancements include adding an event correlation feature, and/or creating a trap or 'honey pot'. The addition of a correlation function would be useful in profiling the activity. For example, an initial call to the system may be a false alarm --

someone simply dialed the wrong number. If, however, the system detects an additional call shortly thereafter, the probability is higher that a cracker is attempting to exploit the modem as a potential gateway into the Intranet. The correlation function would contain logic that would recognize the activity as intrusive behavior with a higher degree of confidence, and issue an appropriate alarm.

The honey pot feature, if implemented, provides a method for monitoring the activity, and potentially helping to identify the intruder. A more complete discussion on implementing a honey pot can be found in [Am96]. A ‘honey pot’ is simply a computer intended to entice a suspected attacker into a spoofed environment that resembles the attacker’s intended target [Am96].

In order for the honey pot to work, the detection system would need to establish a connection instead of hanging up the modem after the call is detected. A relatively straight forward solution to the honey pot would be to use something like Linux as the operating system on the machine. Linux is a freeware Unix-like operating system. The system would be set up with a few security holes, such as a guest account with no password, dial in access, and auditing would be enabled. This configuration would allow the cracker access as well as the system administrator knowledge of the intruder’s activities. The system must be sufficiently contained, an intruder should not be able to do any harm to the Intranet if the honey pot is compromised.

4.2 PBX Call Record Analysis

Phone call accounting systems found on most Private Branch Exchange (PBX) systems capture, record, analyze, and organize information about telephone calls coming into or originating from a corporation (see [PBX97]). This captured data is presented in the form of call records representing originating calling number, number called, time of call, call duration, and other information. This PBX information is traditionally used for tracking and assessing network usage cost and sometimes for detection of toll fraud. In this section, we show how this information can also be used to detect incoming war dial activity.

4.2.1 Call Record Analysis Techniques

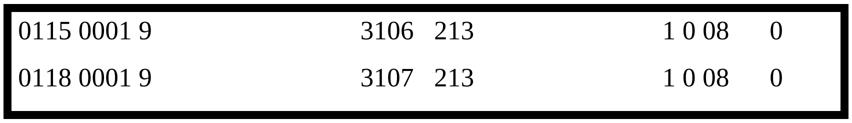
Current call record analysis methods (typically vendor proprietary) that are used for toll fraud detection and exception traffic reporting allow triggering on specific single events such as overseas calls, 900-number usage, and out-of-hours outgoing long distance calls. They make use of high-level call records and ignore more detailed information that is available in the PBX (specifically, call detail records). To detect war dialing activity, however, requires the capability to examine aggregates of calling activity since war dials involve sequences of related incoming phone calls.

As a result, existing vendor proprietary call record oriented analysis methods are insufficient for our needs. Instead, to detect war dial activity, the call record analysis techniques must be augmented by examining the more involved call detail records (CDR) in the PBX and by utilizing custom processing software that we will describe below.

It is worth noting that the resultant incoming war dial activity detection system can provide near real-time alarming from the PBX call detail records. Additionally, it can be run off-line on stored call detail record information to provide further capabilities of current analysis.

4.2.2 Processing PBX Call Detail Records

The diagram in Figure 2 below shows a representation of common CDR file contents.



```
0115 0001 9                  3106   213                  1 0 08     0
0118 0001 9                  3107   213                  1 0 08     0
```

```
0121 0001 9                    3108   213                 1 0 08     0
0124 0001 9                    3109   213                 1 0 08     0
0127 0001 9                    3110   213                 1 0 08     0
0130 0001 9                    3111   213                 1 0 08     0
0914 0001 A 213                3833  3106                  2 0     22  4
0923 0001 A 213         93013697762  3106                  1 0     23  4
```

Figure 2. Sample CDR Contents

An intrusion detection system for detecting incoming war dial activity using CDR data might proceed roughly as described in the following algorithm (written in pseudo-code):

```
CDR_Analysis:
(1) for each generated CDR do
(2)       Parse CDR for relevant information
(3)       If CDR should be logged
(4)            Add CDR information to call history list
(5)            Age calls from call history list
(6)            Analyze for war dialing characteristics
(7)       Else
(8)            NoOP
(9) end do
```

Annotation of Algorithm:

Line (1): The algorithm iterates on incoming CDR; this illustrates the reactive nature of the proposed approach. That is, as calls are incoming, the intrusion detection system collects information and processes this information in real time.

Line (2): Since the CDR record is typically produced for accounting purposes it generally contains information which is not directly relevant to the war dialing detection problem. Each CDR record should be parsed and reformatted into a structure which is more amenable to this type of processing.

Line (3): Not all CDR's generated by a PBX are important or relevant to the particular problem at hand. For this example in particular, the identification of war dialing activity requires an analysis of all incoming calls only so consequently outgoing calls can be ignored. However, as the analysis objective changes and increased functionality is added the CDR's required for analysis will also change.

Line (4): For this algorithm, the call history list is the vehicle by which the aggregate view of calling activity is generated by the analysis function. Call records are added as CDR's are generated by the PBX.

Line (5): Call records which reside on the call history list should be aged and subsequently removed if they are not relevant to the analysis function. In this example, a call record which is more than an hour old and is not part of identified war dialing activity should be removed. This process aids in conserving memory space and decreases the processing time required by the analysis function.

Line (6): The analyze section would change depending upon time of day for the analysis, if the calling number is provided in the CDR, and if CDR's are generated for unassigned numbers, since CDR's are usually generated for accounting purposes only, CDR's are often not generated for incomplete calls. For example, if calling number is available from the CDR it becomes a trivial task to discover that a large number of short-duration calls are originating from a specific number to a block of numbers on this PBX.

Additionally, the characteristics of the analysis must change depending upon the time of day for the analysis - what may be normal call activity during working hours might be unacceptable or uncharacteristic to that of the activity normally observed during non-work hours.

The identification of unauthorized modem connections, on the other hand, would be less concerned with the analysis of call activity over a given time interval but rather with the time of day for each call and the duration of the call. For example, if the characteristics for incoming calls to a corporation, or even a given extension number for that matter, were to change dramatically from calls evenly spread out during work hours to very long duration calls during business hours or non-business hours attention should be drawn to this extension as having a possibility of having a data connection.

Lines (7 and 8): These lines have been added primarily for clarity reasons to indicate that if a CDR does not directly contribute to the analysis function then no additional processing should be accomplished on this call record.

Line (9): This line simply delimits the iterative do loop.

References

[Be97] R. Behar, "Who's Reading Your Email?" *Fortune Magazine*, February, 1997.

[PBX97] <AT&T PBX Reference Guide>

[Am96] E. Amoroso and R. Sharp, PC Week Intranet and Internet Firewall Stragegies, 1996.