Global Information Assurance Certification Paper

Chen Chee Hing
GSEC Practical Assignment
Version 1.4b

A Telecommunications Access Control Policy

Abstract

There are telecommunications management and control systems available now which can provide network management visibility and control of a voice network (telecom infrastructure) , similar to the management and control capabilities we have enjoyed with our data networks. This paper explores the development of a generic telecommunications access control policy which could be used as a starting point for further development and implementation on a commercial telecom management & control system.

Introduction

Most companies tend to focus their information security resources mainly on their data networks and servers and do not pay much attention to their PBX (Private Branch Exchange) systems or telecom infrastructure. This approach is reinforced by the media publicity given to internet hacking incidents or denial-of-service attacks, computer viruses and all the dismaying results of software vulnerabilities. Toll fraud or PBX fraud has been around for so many years that it sounds positively dull compared to news of the rampant progress of the latest worm.

A possible risk response for a company to adopt would be to accept low-level telecom fraud losses rather than spending significant time and money on better security for the telecom infrastructure. Unfortunately, incidents of high-volume organized toll fraud are becoming more common [1] [10]. And toll fraud, whether low-level or high volume, is not the whole story: attacks on the telecom infrastructure could also result in the loss of confidential information, damage to public image, serious disruption to business or legal liabilities. If you have a call center, the integrity and availability of your telecom infrastructure is critical.

An article in the magazine Communications Convergence suggested that "….if you wish to do real damage to a business or institution, telecom infrastructure is probably a better target than the corporate LAN or website…" [2].

The invisible network

Most companies are not really aware of what is going on inside their telecom infrastructure and are not able to monitor voice traffic or apply proper access control, unlike their data networks which are probably monitored with network management systems, controlled with firewalls and routers (with access control lists) and maybe have intrusion detection systems installed.

For most companies, the telecom infrastructure might as well be invisible from a network management point of view and management control would be via the monthly or weekly call accounting reports, incidents or complaints reported by users, and the occasional call-traffic study for capacity planning purposes.

Improving security & avoiding fraud

Apart from the largely reactive form of control, a company should also take proactive steps (which do not involve major expenses) , including the following:

- Improving the physical security of equipment, wiring closets & the cabling plant;

- Auditing and fixing vulnerabilities in :-
  - operating procedures;
  - password management;
  - PBXs;
  - supporting systems (voicemail, call accounting, interactive voice response etc.);
- Improving user education (against social engineering).

The above essential steps have been covered by others including the well-known NIST paper [3], previous GSEC papers [4] [5] and industry articles [2].

Watching the voice network

There is another possible proactive step, namely the active management and control of a telecom infrastructure. There are now commercial products available which can be described as "…a dynamic telemanagement system that includes security and toll-fraud features….that watches traffic in real time and alarms you if it detects evidence of fraud or anomalous behaviour" [2].

For convenience I will use the acronym TMCS to refer generally to these telemanagement and control systems. There are two types of TMCS : both types operate in real time (or near real time).

The first type is normally called a telecommunications firewall and like a data (Internet) firewall it is connected between the public network and the internal

network, in this case between the public switched telephone network (PSTN) and the PBX. The telecom firewall is able to examine, identify and monitor all telecom traffic passing through it and also to exert control over the traffic (dynamically blocking calls). It can distinguish between voice, data & fax traffic. It could also analyze traffic to look for suspicious traffic patterns, which is analogous to an Intrusion Detection System's capabilities.

The second type is a passive system which analyze the output of the Call Detail Record (CDR) port of the PBX. The CDR port of a PBX sends out a data stream of details (in alphanumeric) of all calls going through the PBX, including incoming calls, outgoing calls and internal calls [6]. This type of TMCS is not able to exert any automated control over the telecom traffic and it lacks information about the type of traffic (voice, data, fax) carried by the calls being analyzed. However it would be a cheaper alternative compared to a telecom firewall and would be able to provide alerts (especially on toll fraud) for human intervention.

An example of the first type of TMCS is SecureLogix Corp. 's TeleWALL® telecommunications firewall [7]. The overall online product literature is scanty but TeleWALL® appears to be a fairly comprehensive product., being a combination of hardware and software components. The hardware is necessary for the interfaces to the telephone company (telco)'s public switched telephone network (PSTN) and the PBX, and includes voice trunk /lines cards and CDR buffers.

TeleWALL® is also able to recognize video & STU-III[1] traffic. One customer, the U.S. Air Force, appears to be quite pleased with its TeleWALL® firewalls installed as part of its Information Warfare Battlelab [8].

An example of the second type of TMCS is Soft-ex's SwitchMinder [9] [10] which is a software product making use of a standard PC/server's asynchronous serial port to obtain data from a PBX's CDR port. SwitchMinder focuses mainly on detecting toll fraud and providing alerts in near real time. It also monitors calls to the PBX maintenance port (which is a popular choice of entry for attackers [2] [4]).

Approach

Basically a TMCS implements a telecommunications access control policy, similar to the way a data firewall implements a network access control policy. In rest of this paper I will explore and discuss the development of a generic telecom access control policy which could be used as a starting point for the further customisation and translation work needed to implement the policy with an actual commercial product.

The orientation of this paper is towards the PBX rather than the new IP telephony systems from the "non-traditional" manufacturers . PBXs typically

[1] "Secure Telephone Unit, Third Generation". See http://www.tscm.com/STUIIIhandbook.html

have long service life, much longer than the average IT systems, 10 years or more being quite common and therefore will be around for quite some time to come. Modern PBXs do offer IP telephony as an option and the concepts discussed here should be applicable to IP telephony systems as well.

It is assumed here the telecom infrastructure is under the management of the IT department and not the building facility services department (which may not be true for some companies).

While the PBX may be able to implement a few of the requirements of the policy discussed below it is not enough and from a defence-in-depth point of view it is preferable to have a separate independent control system. The PBX is a complex feature-rich system with many potential vulnerabilities [3].

A telecommunications access control policy

This telecom access control policy will specify which types of access attempts or conditions are not permitted or undesirable because they are information security risks or potential toll fraud attempts: such conditions should give rise to alarms and alerts to the responsible staff through the most effective means (SNMP alarms, pager message, email, cellphone SMS etc.) who should then investigate the cause and follow the company's incident handling procedures if the need arises.

Modem control

The unauthorized installation or use of modems within a company's network could be a serious information security problem (similar to unauthorized wireless LAN access points).

Unauthorized modems (attached to networked servers or PCs) or unauthorized terminal servers/ remote access servers (with dial-in modems), could be used by attackers as potential routes into a company's network, bypassing the external perimeter defenses like building security systems, firewalls, routers, intrusion detection systems etc. Typically, if dial-in access is possible, the authentication control will not be strong (password authentication at best).

Employees have also been known to dial out to Internet Service Providers (ISPs) from their office PCs, bypassing the company's official connections to the Internet, bypassing proxy servers and firewalls and any internet access logging, URL filtering or content control (including virus checking). Apart from the legal implications if the employee indulged in dubious activities, the access to the ISP opens up another potential route for attackers out in the Internet into a company's network, if they manage to compromise the offending employee's PC (which is connected to the company's LAN). Usually the telephone numbers of the various ISPs' access points in an area, territory

or state would be known and these telephone numbers could be used to detect or control access.

If a company bans direct CO lines (i.e. telephone lines which goes direct to the desk from the CO, bypassing the PBX), installs digital telephone extensions by default (which could be an expensive proposition in a lot of countries), make Basic Rate ISDN lines & analogue extensions a scarce and closely controlled facility, and perform regular war dialing checks of its own PBX, then it would seem to have the risks of unauthorized modems under control.

However there is still the issue of the office fax machines which are typically Group 3 machines which require analogue telephone lines (it is trivial to unplug a fax machine and plug in a PC /modem instead). And Group 4 fax machines require Basic Rate ISDN lines which could also be misused.

Most offices would have some vacant desks or vacant offices with telephone extensions. Unless a company is able to (or willing to) diligently track and disable (or downgrade to the most restrictive class of service) every extensions not in current use and re-activate them when required, there is bound to be a few unused active extensions lying around. This might even be true of telephones lines inside the corporate data center.

In certain environments (e.g. a research & development setup) another possible concern is the potential transmission of company's confidential data, intellectual property etc. by employees, contractors, or "visitors" (legitimate or otherwise) from inside the company's network to an outside 3rd party. An unauthorized modem connection could be one of the methods used for the transmission.

At this point we can now specify some of the statements of our access control policy (for now I will just number them in the order of discussion and re-arrange them at the end).

1. *A denied call shall be logged as an exception (including date & time and captured telephone numbers) and the persons responsible for the security of the telecom infrastructure alerted.*

2. *Fax transmissions on outgoing calls placed from telephone extensions/ lines authorized for fax machines shall be permitted.*

3. *Fax transmissions on incoming calls to telephone extensions/ lines authorized for fax machines shall be permitted.*

4. *Data transmissions on outgoing calls placed from telephone extensions/ lines not authorized for modems shall not be permitted.*

5. *Data transmissions on incoming calls to telephone extensions/ lines not authorized for modems shall not be permitted.*

6. *Outgoing calls to Internet Service Providers shall not be permitted.*

7. *Data transmissions on outgoing calls placed from telephone extensions/ lines authorized for fax machines shall not be permitted.*

8. *Data transmissions on incoming calls to telephone extensions/ lines authorized for fax machines shall not be permitted.*

It would be necessary to do an initial inventory of all authorized modems and fax machines and maintain the lists after that. The fact that our TMCS needs to be updated each time a modem or fax machine is added to the network could be viewed in a positive light: it serves as an additional check that the connection was indeed authorized.

Authorized dial-out modems

Some companies may have authorized modems which are used for connecting (dialing out) to external business partners or service providers like banks (e.g. financial transactions, credit card approvals). We will cover the correct use of these modems with another policy statement.

9. *Data transmissions on outgoing calls placed from telephone extensions/ lines authorized for dial-out modems shall be permitted.*

However these modems lines could also be potentially abused to make non-business data calls (voice calls will be discussed later). We could add another statement to restrict outgoing data calls to authorized destination telephone numbers only (assuming the list of destination telephone numbers is not huge or very dynamic).

10. *Data transmissions on outgoing calls placed to unregistered telephone numbers shall not be permitted.*

Remote Access Servers

It is common for employees to be given the facility to remotely access their company's networks while away from the office, often nowadays via the Internet using VPN technology and VPN gateways. The "traditional" method of Remote Access Servers (RAS) with dial-in ports accessible over the PSTN is still used, often ironically enough by IT support staff either as an alternate access or because it can be a faster access method (during "peak" Internet hours).

Although it is often recommended that remote access servers be connected to telephone lines with a range of numbers separate from the company's main telephone numbers ranges, that is really security by obscurity. Good security practice would in any case recommend at least the use of two-factor

authentication. It would not be an issue for our TMCS if our RAS were to make use of direct CO telephone lines (not connected to the PBX) as long our TMCS is also connected between the PSTN and the RAS.

11. *Data transmissions on incoming calls to telephone extensions/ lines authorized for dial-in modems shall be permitted.*

To increase security we could specify that all calls to our RAS longer than X hours in duration shall be logged.

12. *Incoming calls to telephone extensions/ lines (authorized for modems) longer in duration than X hours shall be logged as an exception.*

However if a risk analysis recommends it, we could also decide that long duration calls shall be terminated as well.

War dialing

War dialing is a basic & popular technique used by attackers to search for active modems on a target's network, typically by scanning the entire known ranges of the target's telephone numbers.

It is also possible that a employee might "war dial" the telephone numbers of an external parties from his work place, which could have legal implications for the employee's company.

It is not clear if any of the commercial TMCS products have the ability to detect war dialing but it would be one feature to look out for.

Deny list of telephone numbers

For various reasons a company might have a list of external telephone numbers, telephone prefixes, telephone area codes or telephone country codes, that it would like to deny for incoming or outgoing calls. The list could include Internet Service Providers (ISPs) discussed earlier, suspected attackers (or war dialers), competitors, known sources of harassing or nuisance calls, premium rate services (e.g. "1-900", sex chat lines etc.), those countries the company currently have no business dealings with or have toll fraud experiences with and so on.

We could re-write our statement no. 6 to make it more general and specify a new statement for incoming calls.

6. *Outgoing calls to telephone numbers (or prefixes) on the deny list shall not be permitted.*

13. *Incoming calls from telephone numbers (or prefixes) on the deny list shall not be permitted.*

Note that we are denying all types of calls here, regardless of whether it is data, fax or voice.

The exception logs of our TMCS would be a useful source of potential telephone numbers to put on the deny list (after due investigations).

Voice calls

Of course the main purpose of a PBX is to switch voice calls between the PSTN and internal extensions. However there are some instances where we would need to deny voice calls to avoid fraud.

14. *Voice transmissions for outgoing calls from telephone extensions/ lines shall be permitted except where they are denied by other specific statements.*

15. *Voice transmissions for incoming calls to telephone extensions/ lines shall be permitted except where they are denied by other specific statements.*

Toll fraud

There are many ways toll fraud could be committed by employees, contractors, visitors, cleaning staff, external attackers etc. and for some methods we could block it before it happens and for other methods we could discover it as it happens. Statement no. 6 on denying calls would help to block some avenues of toll fraud. Telcos usually have fraud management systems in place which can detect fraud activities [11] and the telcos may alert their customers but this is usually after the event. Some of the toll fraud issues are discussed below.

Voice calls over modem & fax lines

Telephone extensions or lines assigned to authorized dial-in modems should be disabled for outgoing calls unless you are making use of the call back feature. But dial-in lines could still be abused by means of collect calls placed via operators and we could also have dial-out modems.

16. *Voice transmissions on incoming calls to telephone extensions/ lines authorized for modems shall not be permitted.*

17. *Voice transmissions on outgoing calls placed from telephone extensions/ lines authorized for modems shall not be permitted.*

Fax machines are usually shared devices and placed in common areas and quite often the telephone extensions assigned to fax machines are enabled for long distance calls without the need for account codes (or authorization

codes). If this is the case, it is trivial to use a fax line to make voice calls when no one else is around (some models of fax machines even have a telephone handset). However enabling account codes could present another problem: fax machines are not designed to hide your PBX account code when you key it in and your account code could be displayed on screen (& upon "redial").

We could re-write our statements no. 7 & no. 8 to make them more general.

7. *Non-fax transmissions on outgoing calls placed from telephone extensions/ lines authorized for fax machines shall not be permitted.*

8. *Non-fax transmissions on incoming calls to telephone extensions/ lines authorized for fax machines shall not be permitted.*

DISA & voice mail

The Dial In System Access (DISA) feature of a PBX is often used to allow employees to make long distance calls from the company's PBX while outside the office [2]. Some voice mail systems may have a menu option for access to the PBX dial tone, similar to DISA. Authentication is via an account or authorization code, which is essentially a PIN and weak codes could be compromised e.g. quite often the default voice mail code is the telephone extension number which the user never bothered to change.

Detecting fraud

The commercial TMCS products generally perform call pattern analysis from CDR data [12] [13] looking for toll fraud warning signals such as :

- Excessive calls over a period (presumably compared with a baseline or historical statistics).
- Unusual increases in calls after office hours, during weekends or holidays.
- Calls to unusual destinations (especially overseas calls)
- Unusual amount of calls to voice mail or DISA (if the feature is used)
- Unusual amount of call forwarding [2] (if used) to mobile phones, long distance or overseas numbers.

If we can live with denying calls to certain destinations (e.g. foreign countries) after hour office hours (e.g 6:00 pm – 8:00 am), during weekends and holidays, our policy could say:

18. *Outgoing calls made after-hours to telephone numbers (or prefixes) in the after-hours list shall not be permitted.*

Emergency calls

It is important for the building security staff or the health, safety & environment (HSE) staff of a company to be quickly informed of any calls made by

employees to any of the emergency services (e.g. “911” in the U.S., “999” in other countries).

The TMCS would be able to detect such calls, the source telephone numbers and generate alerts.

19. Outgoing calls to emergency services numbers shall be logged and the persons on the emergency list shall be alerted (of the source).

Putting it together

Re-arranging and re-numbering the various policy statements, we arrive at the following policy.

General

1) A denied call shall be logged as an exception (including date & time and captured telephone numbers) and the persons responsible for the security of the telecom infrastructure alerted.

Outgoing calls

1) Outgoing calls to telephone numbers (or prefixes) on the deny list shall not be permitted.

2) Outgoing calls made after-hours to telephone numbers (or prefixes) in the after-hours list shall not be permitted.

3) Data transmissions on outgoing calls placed to unregistered telephone numbers shall not be permitted.

4) Data transmissions on outgoing calls placed from telephone extensions/ lines not authorized for modems shall not be permitted.

5) Data transmissions on outgoing calls placed from telephone extensions/ lines authorized for fax machines shall not be permitted.

6) Voice transmissions on outgoing calls placed from telephone extensions/ lines authorized for modems shall not be permitted.

7) Voice transmissions for outgoing calls from telephone extensions/ lines shall be permitted except where they are denied by other specific statements.

8) Data transmissions on outgoing calls placed from telephone extensions/ lines authorized for dial-out modems shall be permitted.

9) Fax transmissions on outgoing calls placed from telephone extensions/ lines authorized for fax machines shall be permitted.

10) Outgoing calls to emergency services numbers shall be logged and the persons on the emergency list shall be alerted (of the source).

Incoming calls

1) Incoming calls from telephone numbers (or prefixes) on the deny list shall not be permitted.

2) Data transmissions on incoming calls to telephone extensions/ lines not authorized for modems shall not be permitted.

3) Data transmissions on incoming calls to telephone extensions/ lines authorized for fax machines shall not be permitted.
4) Incoming calls to telephone extensions/ lines (authorized for modems) longer in duration than X hours shall be logged as an exception.

5) Voice transmissions on incoming calls to telephone extensions/ lines authorized for modems shall not be permitted.

6) Voice transmissions for incoming calls to telephone extensions/ lines shall be permitted except where they are denied by other specific statements.

7) Data transmissions on incoming calls to telephone extensions/ lines authorized for dial-in modems shall be permitted.

8) Fax transmissions on incoming calls to telephone extensions/ lines authorized for fax machines shall be permitted.

References

[1] Hodgson, Jeffrey, "Telephone Fraud: Proactive Solutions to a Costly Menance".
http://www.beckcomputers.com/NewBot/art3.html

[2] Jainschigg, John, "Securing your switch", Communications Convergence magazine, April 2002 issue.
http://www.cconvergence.com/shared/article/showArticle.jhtml?articleId=8701258

[3] NIST, "PBX Vulnerability Analysis", Special Publication 800-24
http://csrc.nist.gov/publications/nistpubs/800-24/sp800-24pbx.pdf

[4] Herrera, Chris, "Often Overlooked: PBX and Voice Security in a Networked World"
http://www.sans.org/rr/catindex.php?cat_id=58

[5] Klein, Alan, "Security Analysis: Traditional Telephony and IP Telephony"
http://www.sans.org/rr/catindex.php?cat_id=58

[6] Bezar, David D., "LAN Times: Guide to Telephony"
McGraw-Hill, 1995, ISBN 0-07-882126-6

[7] SecureLogix Corporation, "TeleWALL® Telecommunications Firewall 4.0"
http://applications.securelogix.com/telewall.htm

[8] U.S. Air Force, "Battlelab success stories: TeleWall"
http://www.au.af.mil/au/awc/awcgate/batlabs/batlabsuccess1.htm

[9] Soft-ex, "SwitchMinder"
http://www.soft-ex.net/html/tollfraudbody.htm

[10] Stewart, Simon (Soft-ex), "The common sense guide to PBX Fraud"
http://www.soft-ex.net/html/pdfs_docs/Soft-ex_CommonSense_Guide_To_PBX_Fraud.pdf

[11] SOTAS, "Fraud Management solution"
http://www.sotas.com/solutions-fraud.html

[12] Soft-ex, "SwitchMinder product description"
http://www.soft-ex.net/html/pdfs_docs/Soft-ex_SwitchMinder_Factsheet.pdf

[13] Omnitronix Inc., "Toll Fraud Detection"
http://www.omnitronix.com/wtpaper/tollfraud.htm