Global Information Assurance Certification Paper

GIAC Security Certification (GSEC) Certification
Version v.1.4b

Title: How to Secure an ISDN Backup Solution

Author: Shawn Hendrickson
Date: Jun 25, 2003

Table of Contents

Introduction

In the world of networking, a primary link failure is enviable. Whether it's a cable cut, hardware failure, or COAM (Customer Owned and Maintained) equipment failure, the results are the same. These failures cost companies millions of dollars a year in lost revenue. Having a back up solution in today's world is imperative. In the last couple decades, people, businesses, and organizations have increasingly sought ways to be more efficient by incorporating solutions that save their companies revenue when a single outage occurs. Because personal computers, servers, and mainframes have allowed people to be much more productive on a global scale, digitized data has become a precious commodity. Therefore, the integrity of this commodity is crucial for businesses to be successful.

This document explains the details companies will need to investigate for a secure ISDN (Integrated Service Digital Network) backup solution when a primary link fails under normal circumstances or through malicious attack. Many organizations make the mistake of placing limited to no security on their backup solutions. This oversight can potentially be harmful if not fatal. The more correctly configured layers of security placed within the infrastructure, the safer your data will be long term. This paper will show companies the necessary precautions needed to safeguard their data. To start, we'll talk about the history of ISDN, why it is still used globally, and how it works. Then, we will discuss different security setups, which companies can employ using routers. We then dive into some of the basic attacks that can be used against ISDN circuits. Finally, the paper will speak of different safeguard measures that can be employed to ensure safe data transmissions until primary services can be restored. For some of the below examples, Cisco command line will be provided where appropriate.

ISDN History - Why It is still Used and How It Works

History

ISDN was developed back in the 1960's. Originally many thought it would replace the POTS (Plain Old Telephone System) analog lines coming into people's homes[1]. The digital low-cost high-bandwidth solution was perfect, in theory, to change how the world used data. In short, because standards were not agreed upon in the beginning, the ISDN solution had an extremely slow start. Eventually, broadband services such as DSL and cable modems provided higher throughput at lower cost. ISDN does still have its place in the data world. Its advantages are seen in backup circuits, versatility (voice, data, and video), as

[1] Becker, Ralph. "ISDN History". April 30, 2003. URL: http://www.ralphb.net/ISDN/history.html

well as with its global reach throughout the world. In areas where broadband is not available, ISDN might be the preferred option. Remember, it was meant to replace POTS lines using the same Telecom infrastructure.

Operations

There are two types to ISDN links – PRI (Primary Rate Interface) and BRI (Basic Rate Interface). In each type, they contain a "D" channel and multiple "B" channels. The difference between a PRI and BRI is the amount of "B" channels and cable media. The PRI contains either 23 or 30 "B" channels depending on the media delivery standard (T1 or E1). Each channel (ch) is 64 Kbits. Most of North America multiplexes into a T1, which is 24 channels (24 ch X 64 Kbits per ch = 1.54 MB per sec transfer). On the other hand, the European standard is an E1 containing 30 channels (30 ch X 64 Kbits per ch = 1.984 Mb per sec transfer). Both standards utilize one of the 64 Kbit channels for its "D". Conversely, the BRI always uses three 64 Kbit channels for a total of 192 Kbits per second. Although the quoted bandwidth for the PRI and BRI are accurate, it is not the throughput a user would expect. Only the "B" channels carry data, while the D channel handles signaling, framing, and call setup (16kbits for BRI). The "D" channel sets up an end to end connection, similar to how a normal call from a POTS line works. They access the same switching network within the Telco or ROBC (Regional Operating Bell Companies). In fact, the number ISDN devices used to call and be called looks like a regular 10 digit phone number. The numbering system is the same because the service uses the same POTS switching architecture as stated above. This is the reason why ISDN has such a large reach around the globe. Here is how it works[2]:

1. Caller sends a SETUP to the Switch.
2. If the SETUP is OK, the switch sends a CALL PROCeeding to the Caller, and then a SETUP to the Receiver.
3. The Receiver gets the SETUP. If it is OK, then it rings the router/phone and sends an ALERTING message to the Switch.
4. The Switch forwards the ALERTING message to the Caller.
5. When the receiver answers the call, is sends a CONNECT message to the Switch
6. The Switch forwards the CONNECT message to the Caller.
7. The Caller sends a CONNECT ACKnowledge message to the Switch
8. The Switch forwards the CONNECT ACK message to the Receiver.

[2] Becker, Ralph. "Layer 3 – Network Layer". February 13, 2003. URL: http://www.ralphb.net/ISDN/proto_l3.html

9. Done. The connection is now up at layer 3 of the OSI model. PPP then authenticates.

ISDN can terminate between many devices. For the scope of this paper, we are only going to use ISDN as a back-up solution to connect two or more routers. Therefore, security between routers and networks is what will be discussed. Because security is best when applied in layers, this paper encourages a business to take multiple actions to protect and safeguard its data. There is no all-in-one solution to thwart attackers.

Router to Router Authentication

As soon as the network layer connection is up as shown in step 9, an authentication process starts. During the ISDN setup call from one router to another, each must authenticate after the Link Control Protocol (LCP) is complete. Before the authentication can happen[3], the link must be physically active. The Telecom Information Element (TIE) from the Telco exchanges information with the ISDN devise to allow the called parties know who is calling. ISDN then uses another set of protocols to help verify who is on the other side – PAP or CHAP. Password Authentication Protocol (PAP) exchanges passwords in clear text and is not the preferred method. It does not provide protection from playback using a protocol analyzer or repeated trial-and-error attacks. Even though the authentication is quicker than CHAP, its benefit does not outweigh its short comings. Challenge Handshake Authentication Protocol (CHAP) on the other hand was intended to provide a more secure connection. CHAP uses an MD5 hash with a challenge. The variable length unpredictable challenge limits the time of exposure to any single attack. CHAP[4] works by using the dialer Remote-name, hostname password and random challenge to create the MD5 hash. Please note that both routers must have the same password. In figure one, router "766-1" establishes a call to router "3640-1" – see below diagram. Router "3640-1" then sends a challenge to router "766-1". The receiving router "766-1" will then take the challenge and make a MD5 hash based on the routers name and host name password for router "766-1". Router "766-1" forwards the hash to Router "3640-1", which runs the same hash bases upon contents in its own configurations file. If the checksum match, router "3640-1" will authenticate. One of the great things about this design is that the actual passwords of the

[3] Allied Telesyn. "Cost Effective Integrated Security over ISDN Networks". May 1999. URL: http://www.alliedtelesyn.co.nz/documentation/appnotes/pdf/2006.pdf

[4] Reference Document. "Configuring BRI Backup Interface with Dialer Profiles" February 12, 2003. URL: http://www.cisco.com/en/US/customer/tech/tk801/tk379/technologies_configuration_example09186a008010456b.shtml

routers are never sent over the connections. Therefore, an attacker would have a more difficult time getting access by using a Brute-Force type attack. This whole process is commonly called a 3-way-handshake[5]. The outcome of matching hashes is that the call can proceed and user data can be transferred using PPP (Point to Point Protocol) to communicate at layer three. One thing to note with ISDN is that once the connection is up, anything can cross if proper security is not in place. This significance will be discussed later in the paper. On a different note, if the check sums of the hash do not match, the layer three connection is dropped within 20 seconds.

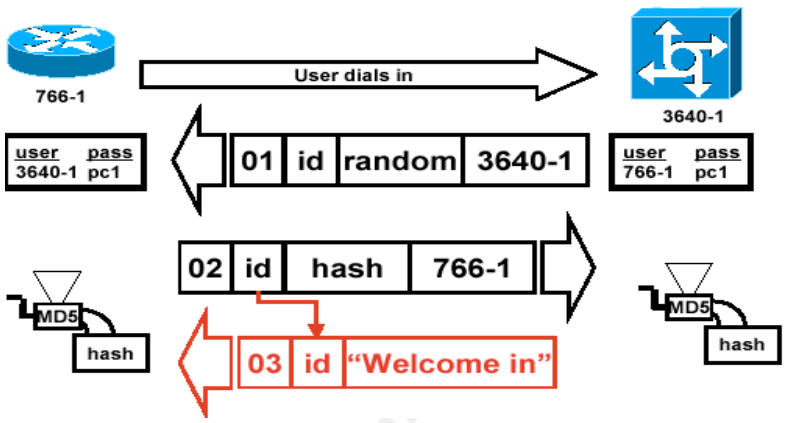

Figure 1

Methods of CHAP

A Network Engineer, can use several different methods to authenticate using:

- CHAP Call In
- CHAP Two Way
- CHAP Callback.

CHAP Call In

The call in feature works when router Left calls router Right as shown in figure 2. Chap is done only in one direction from left to right. Therefore, the configuration will be a slightly different. This is not the preferred method but is still better than PAP.

One-way PPP CHAP Authentication[6]

---

[5] Becker, Ralph. "Layer 3 – Network Layer". February 13, 2003. URL: http://www.ralphb.net/ISDN/proto_l3.html

[6] Reference Document. "Understanding and Configuring PPP CHAP Authentication". April 22, 2003. URL: http://www.cisco.com/en/US/tech/tk713/tk507/technologies_tech_note09186a00800b4131.shtml

Left(config)#	Right(config)#
hostname left username right password sameone encapsulation ppp ppp authentication CHAP callin	hostname right username left password sameone encapsulation ppp ppp authentication CHAP

Figure 2

CHAP Two Way

For the CHAP two way authentications, the algorithm is performed both ways. In figure 3 you can see the configuration is the same for both routers. This type of CHAP is deployed with fixed devised. In this case, two routers are used.

Two-Way PPP CHAP Authentication[7]

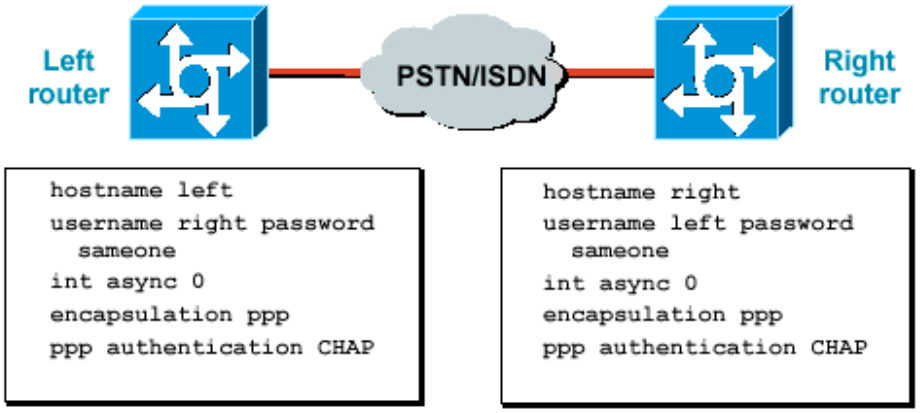

Figure 3

Lastly, the callback feature[8] shown in figure 4, allows Authentication to happen both ways but is initiated by the router "right" after a call from router "Left". If router "Left" calls router "Right", the call in disconnected. Router "Right" would then callback router "Left". This way, router "Left" knows who is on the other side because of a predetermined set of numbers in its configuration. This type of authentication is commonly seen with mobile users and it serves two purposes.

---

[7] Reference Document. "Understanding and Configuring PPP CHAP Authentication". April 22, 2003. URL: http://www.cisco.com/en/US/tech/tk713/tk507/technologies_tech_note09186a00800b4131.shtml

[8] Reference Document. "Configuring ISDN Caller ID Callback". URL: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca6e8.html

It provides a layer of security as well as allows the telephone charges to go to the company versus the user(s).

CHAP Callback

Callback PPP CHAP Authentication[9]

Left(config)#	Right(config)#
hostname left username right password sameone encapsulation ppp ppp authentication CHAP	hostname right username left password sameone encapsulation ppp ppp authentication CHAP isdn caller 15105551000 dialer enable-timeout 2

Figure 4

ISDN is one of the more complicated protocols to configure/setup within a router. Depending on the equipment you use and how the router needs to be set up, there are several areas that need to be covered. Below we will discuss a few of the security related items such as dialer string, username with password, static route, and interesting traffic. A sample Cisco configuration example is listed in Appendix B. The complete configurations for each of these methods are out of the scope of the paper, so I have not included them. Some of the security related steps are shown in the paragraphs below.

Dialer String

The dialer string uses a number that looks like a phone number. In itself, it does not protect against a war dialer, but some protection is offered. The Telco switch and end router have to communicate at layer two. Although no data is passing over the "B" channel, information such as the TEI is being sent by the local Telco switch through the "D" channel. The Telco then knows who it is speaking with on the other end. This offers only a minor road block for a possible attacker via your local phone company.

Usernames and Password

The username and password are used during PAP and CHAP authentications, which is yet another barrier for would be attackers. We have already stated that CHAP is much more secure than PAP. On commercial grade routers, like Cisco's 2500 series and up, the user name and password are typically contained within the same string at the top of the router's running configuration. Other devices may differ.

[9] Reference Document. "Configuring ISDN Caller ID Callback". URL: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca6e8.html

Static Routes

Static route routes serve a couple of different purposes for routers, but we are going to focus on the security aspect. One benefit of a static route or a floating static route in the case of an ISDN backup link is that the router is saying only this network(s) is/are available from the site router. Nothing can be dynamically learned or routed. Every little roadblock provides another barrier. An attacker with physical access to your site could still spoof an address and have complete access to the network.

Access Lists (ACL)

Access Lists for interesting traffic also provides an additional assurance. Because ISDN will pass any traffic after it is up, ACLs are used to block what will allow an ISDN connection to come up. Interesting traffic is valuable to guard against anyone or anything bringing up the link. It is always advisable to restrict ICMP to only between router interfaces. This way if someone tries to map out your network using ping and trace commands, they would not able to establish a connection. This is not full proof. If an attacker sends a legitimate piece of data through to a device on the spoke site or hub end (depending on where you are coming from), the link will come up and ICMP would then be allowed. Again, once the connection is up and authenticated, interesting traffic no longer applies.

Types of Attacks on ISDN

Because most organizations realize that good security practices are done in layers, attackers use a combination of hacking techniques to exploit vulnerabilities. Below are a few of the more common types of attacks, which ISDN and most other media are subject[10]:

Physical Attacks[11]

This type of attack is usually conducted from within the company or from a physical device that connects to the organization. If a vendor, someone visiting, or a person pretending to know someone in the company somehow gets physical access, they potentially have full access to your network. Escorts should always be used in these circumstances to avoid situations that could allow data to be stolen, lost, or altered. Someone with malicious intent only needs a single network connection to do harm. If an attacker is able to get access to a network

[10] Peikari, C & Fogie, S. "Network Attacks". May 15, 2003. URL: http://www.informit.com/isapi/guide~security/seq_id~19/guide/content.asp

[11] Peikari, C & Fogie, S. "Network Attacks". May 15, 2003. URL: http://www.informit.com/isapi/guide~security/seq_id~19/guide/content.asp

device, they could potentially hold your company hostage. As you can see, physical security is critical to protect your company's data. Education is also essential to promote a physically secure organization. Businesses that have to protect their data need to have an education and awareness program to train employees. Employees have to realize that they are shareholders within their respective companies. They directly contribute to the success or failure of their business. By taking certain precautions, shareholders can ultimately detour most would be aggressors. If steps are not taken, your company has a high risk of being infiltrated via a physical attack.

Remember, your telecom links can be compromised without physical security as well. This is particular concerning if you as a business do not own the building and have to share the Telecom closest with other entities in the building. Anyone with access to the Telecom closest may be able to access your network. In many cases, it is extremely easy to fail a WAN communications link with physical access. Do you think that if an attacker knew by taking down your primary link that they would have full access to your network, they would do it? Of course they would! The shared Telco closets need to have limited access allowed to avoid this kind of incident. This leads us to understand why securing our backup solutions are so important. It does take long for a technically savvy hacker to crack basic security. If an aggressor can plan the outage, they have plenty of time to prepare.

It is everyone's responsibility to ask questions if they see someone or something out of place. Not all attackers are people off the streets. Surveys have shown that many of the exploits companies witness are carried out by internal employee. Ask questions if someone looks out of place. In a like manner, always require escorts to be with people that may be visiting. No visitors should ever be allowed physical access to the network in any capacity. Additionally, set policies that allow members of your establishment to know what is expected of them and enforce those expectations. Again, it is everyone's responsibility to maintain physical security as well as enforce other security policies.

Social Engineering[12]

This is a technique used to obtain key information without the other person knowing the attacker's intent. This information may seem useless by itself, but all together it becomes extremely valuable to the hacker to gain access at your network. Many times, information from several people is used to find weaknesses within the security plans. Some Social Engineering ploys come in the form of lost passwords, virtual probes, social spying, and dumpster diving. For our paper, an attacker could call a help desk and obtain key information. For example, they could state that they are from the telephone company and need to

[12] Peikari, C & Fogie, S. "Network Attacks". May 15, 2003. URL: http://www.informit.com/isapi/guide~security/seq_id~19/guide/content.asp

get access to the Telco closet. From there, a number of probing questions could then get asked without anyone getting suspicious.

In larger companies information can be easier to obtain. Because there are many departments all specializing in various functions, no one group understands the attacker's intent. If someone was able to get a directory and call several different departments within a business, they could extract valuable information that would not seem useful to any one individual at the company. Given that in smaller businesses most people typically know each other and perform multiple jobs, it's harder to take advantage of them. As you can see, education is the key to a successful security program. Employees have to understand that they have to question why information is needed. They have to ask their own probing questions to ensure attackers do not gain the information they are seeking. If something does not seem right or out of order, question it. Your instincts are probably right.

Spoofing and Session Hijacking[13]

Spoofing is nothing more than assuming the identity of another computer or using a valid IP or MAC address to make it appear as though you are on a known trusted network. In our case, the attacker could cause the primary link to fail and then spoof an IP address to gain access. Once an attacker has access to your network via your telecom link or a switch communication port from within your business, they can sniff the traffic. After finding a valid layer 3 IP address and mask, the perpetrator can start crafting packets and hijack sessions. In a like manner, if the cracker had access to a switch on-site, he/she could spoof a layer 2 MAC address as well. As you can see, the attacks often come in combinations.

An assailant can then blend in by indicating that they are a part of a valid network via spoofing. This can be done extremely easily if there is no security in place to prevent hacking. Once the attacker simulates or becomes apart of a valid network address range, they can begin to hijack a session to get critical data using a Man-in-the-Middle attack. With the Man-in-the-Middle attack[14], an attacker will determine the IP address of his target and victim. With the source and destination IP addresses, the hacker can sniff the traffic between the devices. They will look for confidential information to come through via applications like telnet, rlogin, ftp, mail applications, and web. An aggressor can do this within minutes given the right circumstances. Therefore, back-up links

---

[13] Peikari, C & Fogie, S. "Network Attacks". May 15, 2003. URL: http://www.informit.com/isapi/guide~security/seq_id~19/guide/content.asp

[14] Bhansali, Bhavin Bharat. "Man-in-the-Middle Attack". February 16, 2001. URL: http://www.giac.org/practical/gsec/Bhavin_Bhansali_GSEC.pdf

should always be as secure as your primary. Networks are only as strong as their least secured links.

Denial of Service via a SYN flood[15]

Regardless of whether the primary link goes down or not, a Denial of Service attack can be done on the local Telco infrastructure to gain access to your network[16]. By compromising the Telco's data, they may be able to indirectly gain access to your network. Although there are not a lot of known ISDN attacks, the media is extremely vulnerable to attacks via the public network.

A hacker can also use a SYN flood to take advantage of your network. While your system(s) wait for an acknowledgement, more SYN requests are made by the assailant. If your systems do not ever receive the final ack, they keep that session open. The attacker will keep sending these TCP SYN requests until the system's resources are exhausted. The server may even crash. This is one technique hackers use to perform a Denial of Service attack.

Different ISDN configurations

A security conscious company may want to utilize one of the following backup configurations for layered security. Depending on how critical security is to that organization, different methods could be implemented. Some security is definitely better than none. In addition to the models, it would be a good idea not to let router "B" have direct internet access. Everything should go through router "C" and use a HTTP proxy located within the DMZ.

We have already discussed the first and most basic security setup using PPP and CHAP. Remember; PAP should not be used. The below option is already available within most commercial grade routers.

[15] Peikari, C & Fogie, S. "Network Attacks". May 15, 2003. URL: http://www.informit.com/isapi/guide~security/seq_id~19/guide/content.asp

[16] Lorenz, G; Moore, T; Manes, J.; Hale, S & Shenoi. "Securing SS7 Telecommunication Networks". Proceeding of the 2001 IEEE Workshop on Information Assurance and Security, Jun 5-6, 2001. URL: http://www.c7.com/ss7/whitepapers/ss7-security/c7-security/securing_ss7.pdf

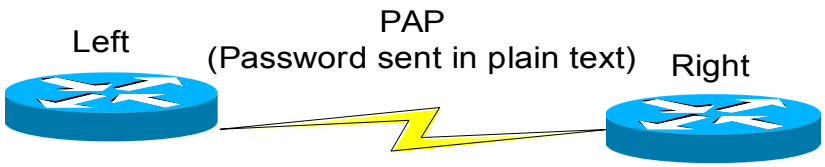

Figure 5

The second setup is not complicated but requires the use of three routers and ACLs (Access-lists). Remember, security is best done in layers. Therefore, if someone is able to breach the CHAP security and gain access, they would then have to be allowed through the routers interface. The use of Access Control Lists (ACLs) provides an additional layer of security to safeguard the network and its data. While the reason for the secondary site is important and is needed for circuit integrity and route diversity, it is out of the scope of this paper. For this configuration, Router B or the FSO (Field Sales Office) loses its primary link and immediately comes up on ISDN backup via router C. Depending on the traffic patterns, router C or B will initiate the call based upon the interesting traffic setups. The routers will use CHAP to authenticate the call in either direction. Once the call is established, the layer 3 PPP allows all traffic to flow. Therefore, ACL are used to block unwanted traffic in the form of "Interesting Traffic" as well as traffic coming through S1/1 on router B after the connection is up. The same list should be applied to both locations. If the ACL of the "Interesting Traffic" was comprised by a good packet, serial 1/1 ACL's would catch the bad traffic after the link is up. You should always try to block data via ACLs as the data comes into the router. A simple ACL configuration that could be used for "Router B" is shown underneath figure 6.

A – Primary
B – FSO
C – Secondary site

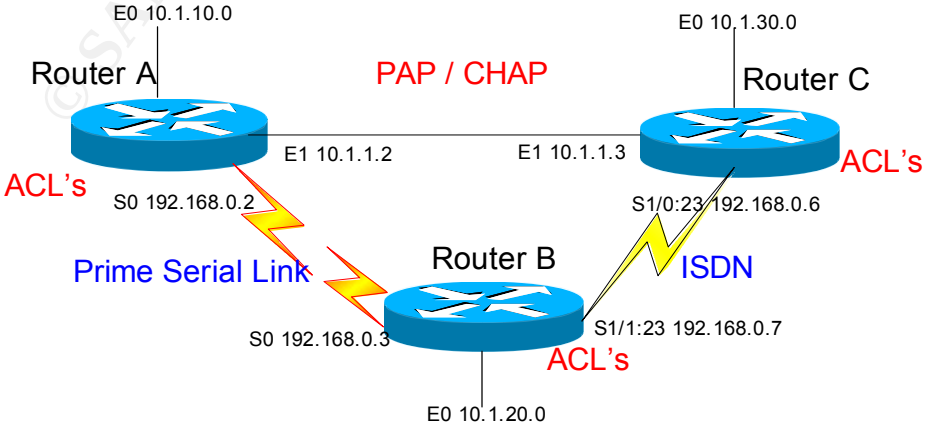

Figure 6

```
Router B(config)# ip access-list extended 100
Router B(config)# deny ip any 0.0.0.255 255.255.255.0
Router B(config)# deny   eigrp any any
Router B(config)# permit permit ip 10.1.10.0 0.0.0.255 any
Router B(config)# permit permit ip 10.1.30.0 0.0.0.255 any
Router B(config)# permit icmp host 192.168.0.2 host 192.168.0.3
Router B(config)# permit icmp host 192.168.0.6 host 192.168.0.7
Router B(config)# deny   icmp any any
Router B(config)# permit ip any any
```

The third configuration requires four routers and utilizes a VPN tunnel and IPSEC. On routers A, B, and C there would be crypto statements similar to the ones shown below[17]. This paper will use IPSEC because it is the industry standard. For the purposes of this document, only the tunnel and crypto statements are shown for the ISDN circuit. Routers A, B, and C would all need a VPN card[18], which will allow the tunnels to be built. Again, the best way to implement security is in layers as seen in this model. First, the routers must know who they are communicating with through CHAP. The router will also use ACLs to prevent unwanted users, and finally the data is protected using a 3DES algorithm via the IPSec tunnels. The 3DES algorithm is currently the industry standard. There are actually two types of Triple Des[19]. The first uses a 3-key cipher, while the other only uses a 2-key cipher. The 3-Key 3Des uses a 168 bit key length, while it counterpart only has a 112-bit key that is said not to be breakable within a lifetime –given the current technology. However, there are new rumors that under certain conditions, the 3DES standard encryption algorithm can be cracked[20]. Cryptographers are still looking into the subject. The exact 3DES operations are out of the scope of the paper.

---

[17] Reference Document. "Configuring ISDN Caller ID Callback". URL: http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/products_feature_guide09186a00800ed371.html

[18] Reference Document. "VPN modules for the 1700, 2600, 3600, and 3700 Series Router". URL: http://www.cisco.com/en/US/products/hw/routers/ps274/products_data_sheet09186a0080088750.html

[19] Reference Document. "Chapter 2: Symmetic Cryptography". ASP Encrypt, URL: http://www.aspencrypt.com/crypto101_symmetric.html

[20] JustinT. "Triple-Des Security Rumor". Security Forums, Apr 25, 2003. URL: http://www.helpforums.co.uk/forum/viewtopic.php?t=5578

A – Primary
B – FSO
B-FW FSO Firewall
C – Secondary

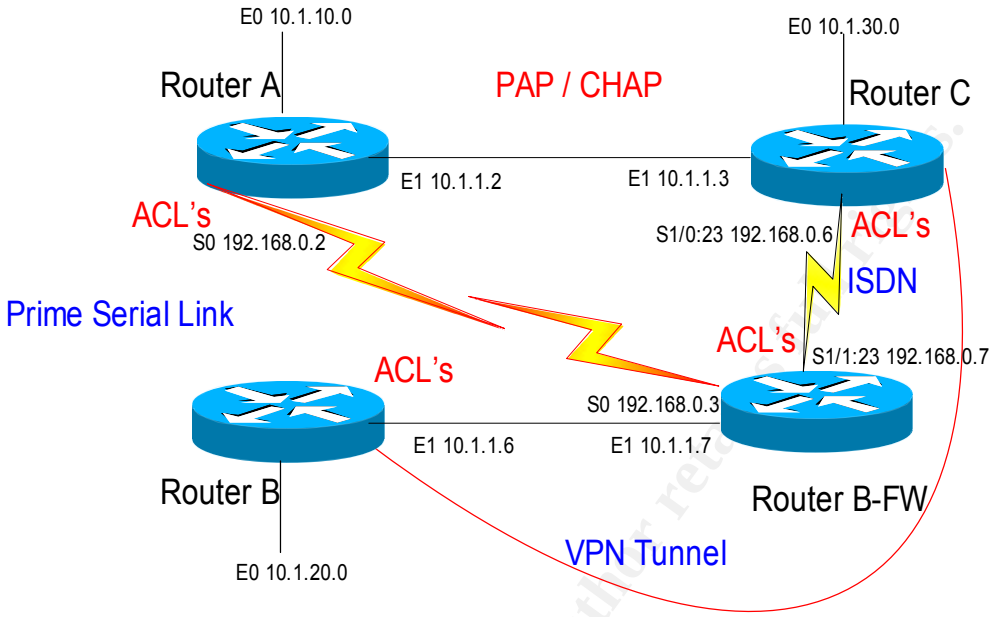

Figure 7

Router B

```
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
 lifetime 120
crypto isakmp key ffffff7483&#*$ghfjeur address 192.168.0.7
!
!
crypto ipsec transform-set encr esp-3des esp-md5-hmac
 mode transport
!
crypto map encr 10 ipsec-isakmp
 set peer 192.168.0.7
 set transform-set encr
 match address fso

ip access-list extended routerC
 permit gre host 192.168.0.6 host 192.168.0.7
```

Router C

```
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
 lifetime 120
crypto isakmp key ffffff7483&#*$ghfjeur address 192.168.0.6

!
!
crypto ipsec transform-set encr esp-3des esp-md5-hmac
 mode transport
crypto ipsec transform-set encrypt esp-3des
 mode transport
crypto mib ipsec flowmib history tunnel size 200
crypto mib ipsec flowmib history failure size 200
!
crypto map encr 10 ipsec-isakmp
 set peer 192.168.0.6
 set transform-set encr
 match address routerB

permit gre host 192.168.0.7 host 192.168.0.6
```

Conclusion

We talked about how ISDN works, why it is still used, and a brief narrative of its history. The paper then covered the basic security inherent to routers. Afterward, we informed of some generic attacks that could be used against ISDN. Finally, we went through staggered security models to show how to provide security in layers.

In short, circuit failures are a part of networking and Wide Area Networks. We discussed that failing to adequately secure a backup circuit could result in a security breach. The security of the network is only as sound as its weakest circuit. It only takes a few minutes to gain full access to a network under the right circumstances. Since the majority of companies now store all their critical data on servers contained on networks, they are at risk of losing essential information if they are not properly secured. Ultimately, losing this vital information could potentially cause a company to go out of business.

Appendix A[21]

SS7 Attack Taxonomy

	INTERCEPTION	INTERRUPTION	MODIFICATION	FABRICATION
SSP - Service Control Points	Eavesdropping (Software) * SS7 Packet Sniffing * SS7 Authentication Attack * Stealth Conference Calls	Denial of Service (Software) * SS7 Authentication Attack * Routing DB Attack * MTP Link Management Attack	Physical Modification * Hardware Configuration ISDN End User * ISUP Msg. Modification * SS7 Authentication Attack	Spoofing (Software) * SS7 Authentication Attack * ISUP, ANI Spoof Eavesdropping (Software) * SSP Impersonation * ISUP Msg. Generation
STP - Signal Transfer Points	Eavesdropping (Software) * SS7 Packet Sniffing * SCCP / Global Title Translation Attack	Denial of Service (Software) * OSS Component Destruction * Virus, Worm, Trojan Horse * Routing DB Deletion * LNP DB Attack * SCCP Msg. Alteration * MTP Link Management Attack	Toll Fraud (Software) * OSS Attack Eavesdropping * Routing DB Attack * SCCP Msg. Rerouting Attack	Eavesdropping (Software) * STP Impersonation * SCCP Msg. Generation
SCP - Service Control Points	Eavesdropping (Software) * SS7 Packet Sniffing * Voice Mail Snooping * Unauthorized SCP Browsing * TCAP Modification * Stealth Conference Calls	Denial of Service (Software) * Call Forwarding DB Deletion * Number Translation Deletion * Call Forwarding DB Deletion * Speed Dialing DB Deletion * Voice Mail DB Deletion * LNP DB Attack * TCAP Msg. Alteration * MTP Link Management Attack	Toll Fraud (Software) * LIDB (Billing) Alteration * CMSDB (Toll Free) Alteration * Credit Insertion * Advanced Service Fraud * TCAP Msg. Modification Eavesdropping * Speed Dialing DB Attack * Number Translation DB Attack	Eavesdropping (Software) * Call Forwarding DB Insertion * SCP Impersonation * SCCP,TCAP Msg. Generation * TCAP DB Query Fabrication

[21] Lorenz, G; Moore, T; Manes, J.; Hale, S & Shenoi. "Securing SS7 Telecommunication Networks". Proceeding of the 2001 IEEE Workshop on Information Assurance and Security, Jun 5-6, 2001. URL: http://www.c7.com/ss7/whitepapers/ss7-security/c7-security/securing_ss7.pdf

Appendix B

Sample Cisco ISDN Configuration

Item	Configuration	How it is Used
User name password	username right password 7 995623450D5A011115	The username and password is used for authentication during PAP and CHAP. It will hang up within 20 seconds of the connection if the hashes do not match. Remember that the passwords on each side must match.
Bri / Pri (Physical interface)	interface BRI0/0 description *** ISDN BU *** bandwidth 128 encapsulation ppp no keepalive dialer pool-member 1 isdn switch-type basic-ni isdn not-end-to-end 56 ppp authentication chap ppp multilink	This is a basic physical interface configuration. The physical interface is always talking to the Telco switch. It should show an active layer 1, while passing TEIs. The Basic-net3 switch types may show deactivated.
Dialer (Logical interface)	interface Dialer0 description *** ISDN BU to Right *** ip address 10.10.10.9 255.255.255.252 encapsulation ppp load-interval 30 dialer pool 1 dialer remote-name right dialer idle-timeout 180 (sec) dialer string 19785551111 dialer load-threshold 80 outbound dialer-group 1 no fair-queue ppp authentication chap ppp multilink	This is a basic logical interface configuration. It maps to a physical interface and uses its dialer string to place a call. When the load reaches 80, another “B” channel is brought up. The PPP multilink allow the channels to load balance.
Dialer Pool	Both are members of pool 1	This is used to map the logical interface to one or more physical interfaces.
Dialer String / SPID	dialer string 19785551111	This is actually contained in the Dialer interface setup. The number looks like a standard telephone number. SPID used with BRI only. They are telephone numbers assigned to each "B" channel. SPID are mostly seen in the US.
Static route	IP route 0.0.0.0 0.0.0.0 10.10.10.10 200	Provides an alternate route when the primary path / protocol is down. This says to route everything with a Administrative Distance of 200 to the next hop router 10.10.10.10. Your normal protocol should have a AD of less than 200.
Dialer Group	Dialer -group 1	The dialer group is listed in the Dialer Interface configuration and points to a dialer list
Dialer List	dialer-list 1 protocol ip list 100	The dialer-list points to an Access list. In this example, it uses the IP stack and points to ACL 100.

Access List	access-list 100 deny ip any 0.0.0.255 255.255.255.0 access-list 100 deny eigrp any any access-list 100 permit icmp host 10.10.10.10 host 10.10.10.9 access-list 100 deny icmp any any access-list 100 permit ip any any	This ACL determines “Interesting Traffic”. “Interesting Traffic” will allow the link to come up only when a valid packet is sent. Once the link is up, all other traffic is allowed unless filtered with another ACL.

References

Allied Telesyn. "Cost Effective Integrated Security over ISDN Networks". May 1999. URL: http://www.alliedtelesyn.co.nz/documentation/appnotes/pdf/2006.pdf

Bhansali, Bhavin Bharat. "Man-in-the-Middle Attack". February 16, 2001. URL: http://www.giac.org/practical/gsec/Bhavin_Bhansali_GSEC.pdf

Becker, Ralph. "ISDN History". April 30, 2003. URL: http://www.ralphb.net/ISDN/history.html

Becker, Ralph. "Layer 3 – Network Layer". February 13, 2003. URL: http://www.ralphb.net/ISDN/proto_l3.html

Castelino, Kenneth. "3DES and Encryption". URL: http://kingkong.me.berkeley.edu/~kenneth/courses/sims250/des.html

Hines, E & Gamble, J. "Non Blind IP Spoofing and Session Hijacking: A Diary From the Garden of Good and Evil." February 25, 2002. URL: http://www.fatelabs.com/library/non-blind-hijacking.pdf

JustinT. "Triple-Des Security Rumor". Security Forums, Apr 25, 2003. URL: http://www.helpforums.co.uk/forum/viewtopic.php?t=5578

Lorenz, G; Moore, T; Manes, J.; Hale, S & Shenoi. "Securing SS7 Telecommunication Networks". Proceeding of the 2001 IEEE Workshop on Information Assurance and Security, Jun 5-6, 2001. URL: http://www.c7.com/ss7/whitepapers/ss7-security/c7-security/securing_ss7.pdf

Peikari, C & Fogie, S. "Network Attacks". May 15, 2003. URL: http://www.informit.com/isapi/guide~security/seq_id~19/guide/content.asp

Reference Document. "Configuring BRI Backup Interface with Dialer Profiles" February 12, 2003. URL: http://www.cisco.com/en/US/customer/tech/tk801/tk379/technologies_configuration_example09186a008010456b.shtml

Reference Document. "Understanding and Configuring PPP CHAP Authentication". April 22, 2003. URL: http://www.cisco.com/en/US/tech/tk713/tk507/technologies_tech_note09186a00800b4131.shtml

Reference Document. "Configuring ISDN Caller ID Callback". URL: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca6e8.html

Reference Document. “Configuring ISDN Caller ID Callback”. URL: http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/products_feature_guide09186a00800ed371.html

Reference Document. “VPN modules for the 1700, 2600, 3600, and 3700 Series Router”. URL: http://www.cisco.com/en/US/products/hw/routers/ps274/products_data_sheet09186a0080088750.html

Reference Document. “Chapter 2: Symmetic Cryptography”. ASP Encrypt, URL: http://www.aspencrypt.com/crypto101_symmetric.html

Tanase, Matthew. “IP Spoofing: An Introduction.” March 11, 2003. URL http://www.securityfocus.com/infocus/1674