



RECEIVED

JAN 14 1994

FCC MAIL ROOM

1633 Bayshore Hwy, Suite 120
Burlingame, CA 94010
415/259-1688
800/547-1771
415/259-1690 FAX

DOCKET FILE COPY ORIGINAL

Mr. William F. Caton, Acting Secretary CC Docket No. 93-292
Federal Communications Commission, Common Carrier Bureau
1919 M Street NW,
Washington D.C., 20554

SUBJECT: CPE TOLL FRAUD PREVENTION

Customer Premises Equipment (CPE) Toll Fraud is in most cases avoidable and preventable if "special diligence" is practiced by all businesses involved in the calling process from phone to phone.

Phrack Magazine, Volume Four, Issue Forty Two, file 2b of 14 states: "Why aren't stockholders crying for the heads of system administrators, MIS managers and CIOs? These are the people who have not adequately done their jobs, are they not: If they had expended a bit of time, and a small amount of capital, the tools exist to make their systems impervious to attack. Period."

CURRENT PRACTICES TO CURB CPE TOLL FRAUD ARE:

- 1- PROTECTION: Customer diligence against CPE toll fraud.
- 2- DETECTION: Suspicious calling patterns may be identified.

PROTECTION

THE CPE IS THE STARTING POINT FOR TOLL FRAUD SECURITY PROTECTION.

CPE Switch Manufacturers have been providing, since the invention of the 'Stroger Switch', access control and privileges. The CPE switch is designed to provide or deny calling privileges. If the privileges are constructed according to business objectives, known hacker activity and toll fraud security, the switch will be virtually secure. Hacker technological migration and social engineering skills are the major obstacles to a completely secure environment.

FOUR STEPS TO CPE TOLL FRAUD SECURITY

- 1- Deny access to known hacker penetration points.

Equipment is available to protect against hacker penetration of the CPE through dial-in access and maintenance ports.

- 2- Conduct a Risk Analysis of each CPE to identify its vulnerability to toll fraud.

Risk Analysis is used to identify in the CPE business communication configuration, the vulnerability to toll fraud. This process is based on known hacker activity and corresponding protection techniques.

No. of Copies rec'd
List A B C D E

059



1633 Bayshore Hwy, Suite 120
Burlingame, CA 94010
415/259-1688
800/547-1771
415/259-1690 FAX

3- Reprogram and configure the CPE calling privilege pattern with security in mind.

Reprogramming the CPE provides a "benchmark" calling privilege pattern including security.

4- Monitor and check the CPE communication system for fraud.

Equipment and software programs exist to monitor and check the CPE.

DETECTION

RBOCs, Interconnects, Independents, Carriers and others providing calling service must assist in providing security. Network service providers have monitoring abilities to assist the customer in the fight against toll fraud. Monitoring and checking services are available free, or for a fee, to identify suspicious calling patterns. Timely notification and fraudulent activity shutdown need to be worked out for financial responsibility.

Maintenance Service providers must provide the client with the methodology to control the CPE in regards to security or accept some liability.

TeleDesign MANAGEMENT appreciates the opportunity to share our views on a common industry problem. We have been on the forefront of toll fraud by managing CPE systems with security in mind. We have a successful proven track record with clients, vendors, manufacturers, and long distance carriers.

We would like to testify before the FCC in regards to Toll Fraud.

With over twenty years of fraud detection experience, beginning with coin boxes, now working in the private business sector of the telecommunications industry, we bring a unique perspective to the problem of toll fraud.

Thank you for reading these comments.

Sincerely,



Ed Simonson, Owner, Vice President
TeleDesign MANAGEMENT



Ken Kumasawa, Sales/Marketing
TeleDesign MANAGEMENT

TELGUARD SYSTEMS

Toll fraud is a significant and growing concern within the telecommunications industry—one that could cost your company thousands of dollars.

Criminals seeking unauthorized network entry are targeting companies' Direct Inbound Service Access (DISA), voice mail, automated attendants and remote maintenance/administrative ports. Hackers use personal computers, random-number generators and password-cracking programs to break into even the most sophisticated systems. Once a hacker penetrates a system, thousands of unauthorized calls—primarily to expensive international locations—will be made.

Telecommunications fraud has become a highly profitable criminal activity. AT&T estimates that 1992 losses will be close to 4 billion dollars. The average toll fraud loss (after excluding losses over 1 million dollars) was \$90,000 per incident, as reported to the Tele-Communications Association (TCA) in a recent industry alert. Some industry analysts anticipate a thousand-fold increase in the number of incidents by the end of 1993.

No company is immune, regardless of size. Small companies could be bankrupt by hackers. Recent court cases and current FCC rulings establish the loss as the individual customer's, not the carrier's. Therefore, a company hit by toll fraud is responsible for paying unauthorized long-distance charges.

The TelGuard Solution

Protection and security measures must be installed to discourage unauthorized and fraudulent use of company resources. While no telecommunications system can be made entirely free from the risk of toll fraud, diligent attention to system security can reduce the risk considerably.

To protect against toll fraud, **TeleDesign Management** recommends a four-step program:

1. Stop unauthorized access to systems maintenance/administrative ports with a **Telguard™** or **TelGuard™II** System.
2. Review current configurations with a security check from **TeleDesign Management**.
3. Reprogram your system to eliminate possible security breaches based on **TeleDesign Management's** recommendations.
4. Monitor or have **TeleDesign Management** monitor your system on a weekly or daily basis.

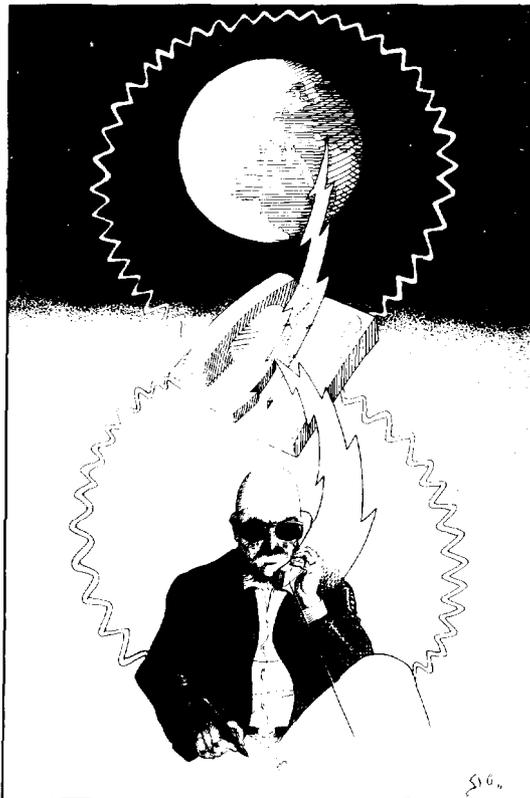
This program offers the best protection available to secure your telecommunications system, and it needs to be done now. Users and attendants alike need to be aware of how to recognize and guard against hacker activity. A single fraud prevention will save your company an amount many times the original investment.

Uncover Security Risks with TelGuard™ Risk Analysis

Corporate America is playing a high-stakes game of chance—and losing billions. Too little attention is given to the security risks inherent in today's highly-sophisticated telecommunications systems. It is mere child's play for hackers and other high-tech thieves to break into these systems, sell access to a company's telephone lines, and rack up thousands of dollars in unauthorized toll charges—all at the company's expense. In fact, before the crime is detected and the hacker shut out, the average company suffers a \$90,000 loss.

A hacker can gain unauthorized access to a company's telecommunications system in a number of ways. A common scenario is for the hacker to find a remote maintenance port, enter the switch and set it up for future illegal use. After waiting a few days until the transaction can no longer be traced, the hacker sets up shop—with little fear of being detected, let alone apprehended or prosecuted.

With today's rapidly-changing technology, every innovation opens the door to a new security risk. No company is immune. According to MCI attorney James Snyder, formerly with the Secret Service, "There are two kinds of [phone] customers: Those who have been victims of toll fraud, and those who will be."* Fortunately, there is a simple, low-cost solution that will uncover your security risks... **TelGuard™ Risk Analysis.**



TelGuard™ Risk Analysis helps protect your telecommunications system from hackers and other high-tech thieves by uncovering inherent security risks.

TelGuard™ Risk Analysis Puts You Back in Control

No manufacturer has developed an impregnable telecommunications system. Whether you have installed sophisticated features like voice mail and SMDR or simply have remote maintenance and administrative ports, your system is at risk. Hackers and other high-tech thieves will attempt entry.

TelGuard™ Risk Analysis will put you back in control. This comprehensive security audit is designed to help you strike a balance between security and ease of use. Weighing the security risks inherent to each, we help you select the combination of features that best fit your needs and ensure the proper safeguards are in place.

Stop Hackers Cold with TelGuard™ Systems

TelGuard™ Systems lock out toll fraud bandits by preventing unauthorized remote access to your telecommunications system's dial-up maintenance and administrative ports. TelGuard™ continues to allow the system to automatically report trouble but blocks incoming calls to the maintenance port, requiring a manual override each time remote access is necessary. TelGuard™ II has an added hang-up and call-back feature which allows authorized users 24-hour remote access but stops hackers cold. Both units are compact, measuring less than seven inches long, seven inches wide and two inches tall, and weighing less than three pounds. They can easily be installed anywhere on site using standard jacks and cables.

For Added Protection, Ask About Our Management Service

For continued protection, TeleDesign Management and our network of qualified telecommunications specialists can provide a complete telecommunications management service. We can educate users and attendants alike in how to recognize and guard against hacker activity, monitor your system on a daily or weekly basis to ensure security is not compromised, or establish a platform for future software enhancements. Ask about our comprehensive telecommunications management service.

Controlled Access Eliminates Worries

Vendors have typically shipped PBX systems in a full-permission environment that allows maximum functionality but provides little security against illegitimate users. **TelGuard™ Risk Analysis** takes the guess work out of systems security.

Here's how **TelGuard™ Risk Analysis** works: First, we conduct a security audit designed to point out inherent risks. Then we assist you in determining the appropriate means of securing your system—recommending ways for you to control access while achieving a balance between functionality and security. Finally, we enter your system remotely, purge existing security breaches and secure the system.

TelGuard™ Risk Analysis makes use of every available feature to prevent toll fraud, using as many as four levels of security. No where else can you find a safer, more secure approach.

TelGuard™ Risk Analysis Means Peace of Mind

You'll get peace of mind knowing all work is performed by TeleDesign Management's security specialists. With over three decades of experience in telecommunications sales, product development, training, software design, technical support, installation and repair, there is no better source for telecommunications security and software support.

Security You Can Count On

No company is immune from toll fraud. Imagine explaining a \$90,000 loss that would have been prevented by a small investment in **TelGuard™ Risk Analysis**. For one low fee, you'll get the most comprehensive, convenient and cost-effective security audit available. Don't wait until your company is hit. Get security you can count on. Get **TelGuard™ Risk Analysis** today.

Don't Delay. Order TelGuard™ Risk Analysis Today.
800/547-1771

TelGuard™ Systems
Marketed by TeleDesign Management, Inc.

1633 Bayshore Highway, Suite 101
Burlingame, CA 94010
TEL 415/259-1688
FAX 415/259-1690



R. E. Bozzomo
Director,
Developmental Relations Group

295 North Maple Avenue
Basking Ridge, NJ 07920

August 13, 1993

Mr. Ed Simonson
TeleDesign Management
Suite 101
11633 Bayshore Highway
Burlingame, CA 94010

Dear Mr. Simonson,

Thank you for participating in the compatibility test of the TeleDesign Management Risk Analysis, which was remotely conducted on July 12, 1993 from Burlingame, CA on the Definity G1 at AT&T's Holmdel test facility. This test is part of the overall test program for assessing security audit services for NetPROTECT^(SM) Service.

Our test report, Attachment A, shows the Risk Analysis complied with the requirements of Advanced and Premium NetPROTECT service tariffs and may be listed as an acceptable security audit service.

Attachment B is a model press release which, I believe, will strengthen the market appeal of your product. Please send John Mikulak an advance copy of your press release prior to publication.

Please contact John Mikulak on (908) 221-6077 if you should have any questions.

Sincerely,

A handwritten signature in cursive script that reads "Robert E. Bozzomo".

Robert E. Bozzomo

cc: J. Mikulak



AT&T Bell Laboratories

**subject: TeleDesign Management Risk Analysis NetPROTECTSM
Service Compliance Test
Work Project No. 596160-1000
File Case 61108**

date: July 29, 1993

**from: J. H. Hobson
Org. 1F5A51000
HO 3K513
(908) 949-4441
honet5!hobson**

Test Report

The compliance testing of the TeleDesign Management Risk Analysis Security Audit Service was conducted on July 12, 1993. This test is part of the overall test program for assessing NetPROTECTSM service conformance of security audit services.

The TeleDesign Management Risk Analysis is a security audit service that measures the relative security of a telephone system and recommends ways of increasing the security. The evaluation of this security audit service is listed here:

1. Covered PBXes. TeleDesign Management is able to audit the following PBX systems:
 1. AT&T Definity Series.
 2. Fujitsu.
 3. Mitel.
 4. Northern Telecom.
 5. Rolm.
 6. Toshiba.
 7. Tadiran.
2. Passwords. A check is made to determine in all passwords have been changed from their factory default values.
3. Administration, Maintenance, and Test ports. Ports are checked for access protection.
4. Trunk to trunk transfers. Trunk to trunk call transfers are verified to be blockable.
5. DISA. A check is made whether DISA is active and the barrier codes are checked.
6. Trunk verification codes and trunk access codes. A check is made on all trunks for active trunk access and trunk verification codes.
7. Station Message Detail Recording (SMDR). A check is made to determine if SMDR is activated.
8. Unusual maintenance and administration activity. A check of the system logs is made for any unusual administration activities.

AT&T - PROPRIETARY (RESTRICTED)
Solely for authorized persons having a need to know
pursuant to Company Instructions.



AT&T Bell Laboratories

**subject: TeleDesign Management Risk Analysis NetPROTECTSM
Service Compliance Test
Work Project No. 598160-1000
File Case 61108**

date: July 29, 1993

**from: J. H. Hobson
Org. 1F5A51000
HO 3K513
(908) 949-4441
honet5|hobson**

Test Report

The compliance testing of the TeleDesign Management Risk Analysis Security Audit Service was conducted on July 12, 1993. This test is part of the overall test program for assessing NetPROTECTSM service conformance of security audit services.

The TeleDesign Management Risk Analysis is a security audit service that measures the relative security of a telephone system and recommends ways of increasing the security.

The TeleDesign Management Risk Analysis meets the expressed requirements of Advanced and Premium NetPROTECT service tariff and may be listed as an acceptable security audit service.

John H. Hobson
J. H. Hobson

HO-1F5A51000-JHH-jhh

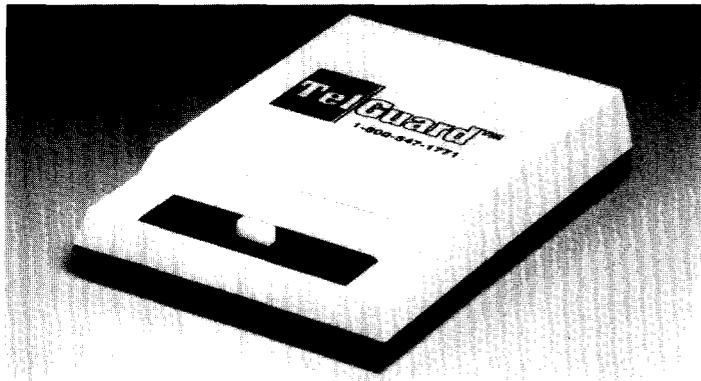
Stop Hackers Cold with TelGuard™

A modern-day techno-nightmare is costing corporate America billions. Bright, well-educated, computer wiz-kids are using personal computers with random-number generators and password-cracking programs to infiltrate even the most sophisticated telecommunications systems.

Once a hacker gains remote access to a company's PBX maintenance/administrative port, it may be sold to crime rings throughout the country. Drug dealers, and the unsuspecting immigrants who are sold illegal call access at public telephone booths, then make thousands of unauthorized calls—most of them to costly international destinations.

Before the crime is detected and the hacker shut out, the average company suffers a \$90,000 hit. Worse yet, despite the fact the calls are unauthorized, the courts have ruled that the corporate victim must foot the bill. And no company is immune. According to MCI attorney James Snyder, formerly with the Secret Service, "There are two kinds of [phone] customers: Those who have been victims of toll fraud, and those who will be." But there is a simple low-cost solution that will stop hackers cold...TelGuard.™*

- Locks Out Toll-Fraud Bandits
- You Control Access with Touch of Button
- Easy to Install Anywhere on Site
- Could Save You Thousands



TelGuard™ protects the dedicated maintenance line of your PBX or Voice Mail/Auto Attendant from unauthorized remote access.

TelGuard™ Locks Out Toll-Fraud Bandits Without Fail

TelGuard™ provides absolute protection from unauthorized remote access to your dial-up maintenance/administrative port, because it requires a manual override. Protection devices that allow software access can be compromised. Not TelGuard.™

Our foolproof design means you control entry to your maintenance/administrative port at all times. TelGuard™ continues to allow your system to automatically report trouble but blocks incoming access to your switch. No one can enter unless you decide to unlock the door each and every time maintenance is required. With TelGuard™ in place, your maintenance line simply cannot be hacked from a remote location.

For Added Protection, Ask About Our Security Review

*For protection from other security breaches such as Voice Mail, DISA and dial access codes, **TeleDesign Management** and our network of qualified telecommunications specialists can provide a complete security review of your existing PBX, Voice Mail and Auto Attendant software. We can also reprogram the system and provide daily and weekly monitoring as needed. Ask how we can help you ensure the proper safeguards are in place.*

TelGuard™ Model #1100

Product Description: Security device for PBX or Voice Mail/Auto Attendant maintenance port to protect from unauthorized access.

Power: 15-35 VDC (Not less than 30 MA)

Manual Override

LED Indicates Open/Secure

Dimensions: 4.24" x 5.65" x 1.25"

Shipping Weight: 1 pound

Patent Pending

Control Access with a Touch of the Button

TelGuard™ couldn't be easier to use. Its simple on/off switch gives you control of maintenance port access at the touch of a button.

Here's how TelGuard™ works: Either you call to gain remote access to the switch or the switch sends out a trouble report and the maintenance provider calls. Once the caller is identified and maintenance/administrative port access is authorized, the attendant pushes the button on the TelGuard™ unit. The red light comes on and the switch is open for maintenance. When the maintenance provider has logged on and is in the switch, the attendant pushes the button again and the system is secured without disrupting the call in progress. TelGuard™ is always in the secure position if there is a power failure or the warning light is out.

If a hacker tries to access your maintenance/administrative port, a "ring no answer" is heard instead of the usual sign-on tone. The hacker can't identify or access the maintenance/administrative port and hangs up. Your telecommunications system is secure.

TelGuard™ is Easy to Install Anywhere on Site

TelGuard™ works on all maintenance/administrative ports including AT&T Definity, Rolm, and Northern Telcom SL1, and installation couldn't be easier. TelGuard™ uses standard phone jacks and cables and can be wall or desk mounted anywhere on site. The compact unit measures less than six inches long, five inches wide and two inches high. You select the best location after weighing the security issues of your building. Common locations for TelGuard™ installation include the telecommunications director's office, PBX attendant's desk or equipment room.

Low-Cost Hacker Protection Could Save You Thousands

No company is immune from toll fraud. Imagine your company is hit next. Then imagine explaining a \$90,000 loss that might have been prevented with a small investment in TelGuard.™ Don't wait until your company is hit. Get TelGuard™ today.

**Don't Delay. Order Your
TelGuard™ System Today.
800/547-1771**

The logo for TelGuard Systems features the word "TelGuard" in a bold, sans-serif font with a grid pattern behind the letters, followed by "Systems" in a similar font. Below the logo, it says "Marketed by TeleDesign Management".

1633 Bayshore Highway, Suite 101
Burlingame, CA 94010
TEL 415/259-1688
FAX 415/259-1690



AT&T Bell Laboratories

subject: **TeleDesign Management TelGuard I NetPROTECTSM
Service Compliance Test
Work Project No. 598160-1000
File Case 61108**

date: **April 9, 1993**

from: **J. H. Hobson
Org. 1F5A51000
HO 3K513
(908) 949-4441
honets!hobson**

Test Report

The compliance testing of the TeleDesign Management TelGuard I was conducted on February 16, 1993 and March 23, 1993. This test is part of the overall test program for assessing NetPROTECTSM service conformance of customer PBX adjunct equipment.

The TelGuard I is an ingress barrier device that requires human intervention to operate. The evaluation of this unit is listed here:

1. Protected port type: RMAT, test, and any analogue voice grade telephone circuit.
2. Ingress access operation: Push button.
3. Unpowered state: Ingress and egress are secure.
4. Power-up state: Secured.
5. Protected port egress state: Unblocked when powered.
6. Protected port ingress access status indicator: Lit red LED when the ingress port is in the unsecure state.
7. Protected port ingress access unsecure timeout: None, however if a call is in progress to the protected port and the button is push to leave the unsecure state then the current connection will be maintained until the call is terminated and the ingress port is blocked.

The TelGuard I meets the expressed requirements of NetPROTECT service tariff and may be listed as acceptable for protecting customer telephone systems.

HO-1F5A51000-JHH-jhh

J. H. Hobson

AT&T - PROPRIETARY (RESTRICTED)
Solely for authorized persons having a need to know
pursuant to Company Instructions.

Stop Hackers Cold with TelGuard™ II and retain round-the-clock remote maintenance access

A modern-day techno-nightmare is costing corporate America billions. Bright, well-educated, computer wiz-kids are using personal computers with random-number generators and password-cracking programs to infiltrate even the most sophisticated telecommunications systems.

Once a hacker gains remote access to a company's PBX maintenance/administrative port, it may be sold to crime rings throughout the country. Drug dealers, and the unsuspecting immigrants who are sold illegal call access at public telephone booths, then make thousands of unauthorized calls—most of them to costly international destinations.

Before the crime is detected and the hacker shut out, the average company suffers a \$90,000 hit. Worse yet, despite the fact the calls are unauthorized, the courts have ruled that the corporate victim must foot the bill. And no company is immune. According to MCI attorney James Snyder, formerly with the Secret Service, "There are two kinds of [phone] customers: Those who have been victims of toll fraud, and those who will be." But there is a simple low-cost solution that will give you round-the-clock remote maintenance access and stop hackers cold...TelGuard™ II.*

- Locks Out Toll-Fraud Bandits
- 24-Hour Remote Access for Authorized Users
- Easy to Install Anywhere on Site
- Could Save You Thousands



TelGuard™ II protects the dedicated maintenance line of your PBX or Voice Mail/Auto Attendant from unauthorized remote access.

TelGuard™ II Locks Out Toll-Fraud Bandits While Preserving Remote Maintenance Access

TelGuard™ II provides absolute protection from unauthorized remote access to your dial-up maintenance/administrative port. Yet, its unique hang-up and call-back feature means you continue to enjoy the benefits of your remote access capability 24 hours a day. Protection devices that allow software access can be compromised. Not TelGuard™ II.

Our foolproof design means you control entry to your maintenance/administrative port at all times. TelGuard™ II continues to allow your system to automatically report trouble but blocks incoming access to your switch. You give out the "keys" to up to 40 dedicated call-back lines that allow remote maintenance access to authorized users. No one else can enter the system unless you unlock the door manually. With TelGuard™ II in place, your maintenance line simply cannot be hacked from a remote location.

For Added Protection, Ask About Our Security Review

For protection from other security breaches such as Voice Mail, DISA and dial access codes, **TeleDesign Management** and our network of qualified telecommunications specialists can provide a complete security review of your existing PBX, Voice Mail and Auto Attendant software. We can also reprogram the system and provide daily and weekly monitoring as needed. Ask how we can help you ensure the proper safeguards are in place.

TelGuard™ II Model #2200

Product Description: Security device for PBX or Voice Mail/Auto Attendant maintenance port to protect from unauthorized access.

Power: 120 VAC 60 Hz, 24 VDC 350 M

Local Only Programmable Dial Back/Manual Override

LED Indicates Open/Secure

Power Indicates On/Off

Status Indicates Programming Activity

Dimensions: 7.0" x 6.3" x 1.6"

Shipping Weight: 3 pounds

Patent Pending

24-Hour Remote Access for Authorized Users —Simple as Dialing the Phone

TelGuard™ II couldn't be easier to use. Up to 40 dedicated call-back lines allow authorized users to access your remote maintenance/administrative port. And setting up a secure call-back is as easy as dialing the telephone.

Here's how **TelGuard™ II** works: The authorized user calls and enters a unique call-back code. The system hangs up and calls the authorized user back. The switch is then open for maintenance. If an unauthorized user attempts to access the maintenance/administrative port and enter a call-back code, **TelGuard™ II** hangs up. The system is not programmed to call the unauthorized user back. The hacker is locked out.

When an authorized system provider requires access to your maintenance/administrative port, an attendant must perform a manual override once the caller is identified and maintenance/administrative port access is authorized. In such cases, the attendant pushes the button on the **TelGuard™ II** unit to allow access and the red light comes on. When the maintenance provider has logged on and is in the switch, the attendant pushes the button again and the system is secured without disrupting the call in progress. The unit is always in the secure position if there is a power failure or the warning light is out.

TelGuard™ II is Easy to Install Anywhere on Site

TelGuard™ II works on all maintenance/administrative ports including AT&T Definity, Rolm, and Northern Telecom SL1, and installation couldn't be easier. **TelGuard™ II** uses standard phone jacks and cables, and can be wall or desk mounted anywhere on site. The compact unit measures less than seven inches long, seven inches wide and two inches high. You select the best location after weighing the security issues of your building.

Low-Cost Hacker Protection Could Save You Thousands

No company is immune from toll fraud. Imagine your company is hit next. Then imagine explaining a \$90,000 loss that might have been prevented with a small investment in **TelGuard™ II**. Don't wait until your company is hit. Get **TelGuard™ II** today.

**Don't Delay. Order Your
TelGuard™ II System Today.
800/547-1771**

TelGuard™ Systems
Marketed by TeleDesign Management

1633 Bayshore Highway, Suite 101
Burlingame, CA 94010
TEL 415/259-1688
FAX 415/259-1690



AT&T Bell Laboratories

subject: TeleDesign Management TelGuard II NetPROTECTSM
Service Compliance Test
Work Project No. 598160-1000
File Case 61108

date: April 9, 1993

from: J. H. Hobson
Org. 1F5A51000
HO 3K513
(908) 949-4441
honet5!hobson

Test Report

The compliance testing of the TeleDesign Management TelGuard II was conducted on February 18, 1993 and March 23, 1993. This test is part of the overall test program for assessing NetPROTECTSM service conformance of customer PBX adjunct equipment.

The TelGuard II is a callback barrier device. The evaluation of this unit is listed here:

1. Protected port type: RMAT, test, and any analogue voice grade telephone circuit.
2. Identification process: Digit, Digit, #.
3. Password: None.
4. Identification, Password, and phone number storage: Non-volatile memory.
5. Maximum attempts: Unlimited, a person can key in any sequence indefinitely, the process terminates only when digit, digit, # are keyed in and the two digits point to a valid telephone number entry in the list. At that time the unit hangs up the original call and calls the specific phone number in the list on a second line.
6. Failed Access Action: None.
7. Unpowered state: Ingress and egress are secure.
8. Power-up state: Secured.
9. Protected port egress state: Unblocked when powered.
10. Protected port ingress access status indicator: Lit red LED when the ingress port is in the unsecure state. Lit green LED if the unit has called an authorized remote user.
11. Protected port ingress access unsecure timeout: Settable in one minute increments from one minute to 99 minutes. If set to zero the time out is unlimited. However, if a call is in progress to the protected port and the button is push to leave the unsecure state then the current connection will be maintained until the call is terminated and the ingress port is blocked.

AT&T - PROPRIETARY (RESTRICTED)
Solely for authorized persons having a need to know
pursuant to Company Instructions.

The TelGuard II meets the expressed requirements of NetPROTECT service tariff and may be listed as acceptable for protecting customer telephone systems.

HO-1F5A51000-JHH-jhh

J. H. Hobson

Telecom Reseller

A PUBLICATION FOR END USERS OF THE SECONDARY MARKET

VOL. 6 NO. 4

APRIL/MAY 1993

At the February meeting of the National Association of Telecommunications Dealers (NATD), Ed Simonson, vice president, sales of TeleDesign Management, Inc., addressed the mutual concerns and responsibilities of vendors and users in protecting telecommunications systems from toll fraud. Below are excerpts from that speech.

"The definition of toll fraud is the illegal use by a third party of another person's communications system. Until recently, what concerned us was internal abuse, or theft, of services. While the abuse of long distance service by employees is costly, such casual toll fraud has gone the way of the Edsel and the regulated airline industry. Most fraud thefts today can actually threaten to put small companies out of business.

"We need to remember that hackers violate corporate security and steal corporate assets. They open up a gateway into the direct line of credit their victim has with the long-distance carrier and use it as if it was their own. We have found that if they hit you, it can cost you about \$100 per hour per trunk. So you could easily get hit for many thousands of dollars over a weekend. It would be difficult for a telecom manager to walk into the CEO's office and say, 'We just had a \$90,000 preventable toll fraud loss.'

DAILING THROUGH THE NETWORK

"A hacker's goal is to gain entry to the PBX via remote access, dial access codes, voice mail, automated attendant or the



Ed Simonson, Vice President, Sales of TeleDesign Management, Inc.

remote maintenance port. In *Hacker Crack Down of 1990*, Bruce Schneier writes, 'if these miscreants have the kind of electronic sophistication to be able to trail their tracks through the network to a mind-boggling untraceable source while still managing to conceal what they're doing from someone.'

'Hackers usually have remote access to any internal destination but they do offer a way out of the switchboard. The remote service port provides hackers with limitless access to all system features. Once entry is gained, hackers take over the management of the system, bypassing restrictions on when calls are made. Who is going to make them and what they are going to be made.

"When a company has a 'plain vanilla' PBX system, there are untold numbers of telecrooks who can crack the system. There are even publications on hacking. John Williams of Almagordo, New Mexico got some pretty good press in the August 1992 issue of *Forbes'* special issue, 'Crime on the Line'. John makes \$200,000 a year selling items that cost from \$29 to \$39, such as a Robo-phone and Auto-dialer that make repetitive dialing automatic. There's also a document called *The 2600* published by Goldstein in Washington, DC. This hacker quarterly has been published since 1984 and offers such articles as 'Revelations Letter,' 'Defeating *69,' 'Hacking American Express' and 'Defeating Callback Verification.'

"Telecommunications technology is changing rapidly and every innovation creates new opportunities for fraudsters. As Alfred Sykes, Chairman of the FCC, said recently, 'Without active work by all participants, toll fraud will get worse as it migrates from one technology to another. No telecommunication system is entirely safe from the risk of toll fraud. While diligent attention to security reduces risk, users must constantly make a trade-off between functionality and security.'

HACKER PROTECTION: A FOUR-STEP PROCESS

"Protection from toll fraud is a four-step process. The first step is to install a protection device to stop unauthorized access to the system's maintenance port.

The second step is to conduct a risk analysis of the current configuration of the system. The existing software may allow the hacker to get in and out without doing anything special. The system may have been shipped with all permissions marked 'YES' or it may have been opened up for maintenance somewhere and then not properly closed. The third step is to re-program the system. This is a complex process because of the amount of inter-related software, but it is vital to system security. The fourth step is to make sure you have someone monitoring and checking the system on a daily or weekly basis to ensure that the changes you make do not aid the hacker.

"Remember, hacker detection is quite a different thing from hacker protection. Don't rely on one type of device to do the work of the other. Today, most SMDR and CDR programs have some means of telling you who is doing what to a system. You can monitor a system with the appropriate program or you can go in physically and look at the system yourself.

"There are many protection products on the market today. AT&T Services and AT&T Long Distance have developed programs through Bell Labs to screen potential vendors to see whether their products do what they are supposed to do to prevent toll fraud. For those who subscribe to AT&T NetProtect, the NetProtect tariff includes instructions on what the client must do to be eligible for this service. I urge that you keep a close eye on the market place and make decisions on what products to employ only after you have done your homework thoroughly.

WHAT TO WATCH FOR

"There are several things to watch for when evaluating different systems. Although I point to AT&T systems in my examples, what I say is true for all systems currently in use.

"MAINTENANCE PORTS: Make sure that maintenance port protection is installed and that the hacker can't get at this port in any way.

"PASSWORDS and LOG-INS: Never use any default password in any of your systems. Use of computer-generated password-breaking programs is well-known in the hacker underground. I personally listened to a recording of a hacker who walked through a 32-digit pass code with a 20-second delay before the last eight digits. It was apparent he had purchased the security device they were using prior to the break-in.

"PREFIX CODES: Check to make sure that your maintenance port has a different central office prefix from the DID, the personal lines. Hackers are using remote automatic dialers. You make their lives easier if you've got a series of numbers where the prefixes can be matched up. So check to see if the remote access feature has been activated and make sure it has a different prefix.

"DISA: Hackers will attempt to find or create DISA in any system that they enter. In the Definity, when you command 'Display Remote Access,' the screen remains blank. If hackers are going in, they can display the remote access. And if it's not there, they know how to fill it out. Then, they set up their trunks and go away so they can come back at their leisure. The remote access should be changed on at least a monthly basis and probably more often if there was a password on it.

"VOICE MAIL/AUTOMATED ATTENDANT: These are the hackers' first choice for break-ins. Voice mail stations should be restricted from transferring to outside trunks. Set up a class of service and a class of restrictions for voice mail to make life difficult for hackers. Add as many layers as possible to your security codes. An article in *The 2600* advises hackers, 'If you can't get into a particular system, just wait. Come back to that one when you've got more time.'

"ACTIVITY: Watch on a continuous basis whether there is unexplained remote maintenance activity. If you are a vendor, urge your customer to watch the maintenance track because that will give an accurate report of anyone going in and doing something they should not be doing.

"TRUNKS: In our investigations, we look for free trunks that are connected to an answering service. Hackers will do the same. They will call a trunk, and when the service hangs up, the system returns a dial tone and the fraud is on the way. So watch your trunk access codes. Watch all the calling permissions and build them so it makes things tough for hackers to get through.

"TAKING CONTROL: Expanded use of features, such as least-cost routing, can improve switching and contribute to cost savings. However, these features also make things easier for the hacker. Remember, every system is going to be the victim of an attempted hacking and no manufacturer of communications systems has yet developed or installed a system that is impregnable. You must control the outcome of these attempts.

"In summary, you must select and implement only the combination of features and vendors which best fits your needs: voice mail, SMDR, voice recognition, port security, etc. A constant tradeoff must be made between security, flexibility and convenience. Hackers live in a rapidly changing world and working together, we must keep a step ahead of them."

For further information, regarding TelGuard and TelGuard II security devices or TelGuard Risk Analysis, call TeleDesign Management, Inc. at 1-800-547-1771.

Reprinted with permission of Telecom Reseller.

December 17, 1993

STANDARD PRODUCT REVIEW WHITE PAPER
of
TeleDesign Management Inc.
TelGuard™ & TelGuard™ II

A. PURPOSE:

This white paper is a review two telecommunications guard products, TeleDesign Management Inc. TelGuard™ and TelGuard™ II.

B. PRODUCT DESCRIPTION:

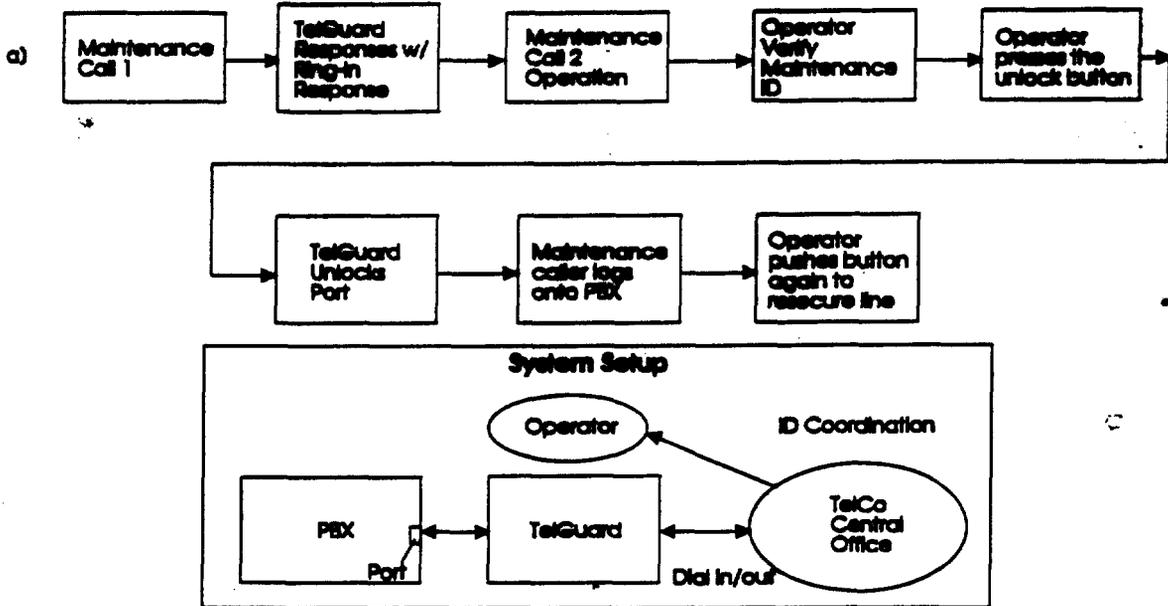
1. Product Function. The two products are add-on units that prevent unauthorized access to commercially available private branch exchanges (PBXs) and voice mail systems (VMS). Several incidents of hackers, using sophisticated computer hardware and software, have broken into computer systems and corporate phone switches. Using the administrative and maintenance port, they have created their own accounts, read through data files, stolen passwords, and, in the case of phone switches, reprogrammed them for free long distance service. TelGuard™ and TelGuard™ II provide a physical security barrier against these attacks.
2. Product Operation (see the Figure). The TelGuard™ utilizes a man-in-the-loop concept. When a maintenance technician dials in, the unit traps the ring signal resulting in a ring-no answer condition. A hacker's autodialer would ignore this signal and move on to the next number. The maintenance technician however knows to call the PBX operator who verifies the caller identification and pushes a button on the unit which "unlocks" the port by allowing the ring signal through to be answered by the system. When the technician logs onto the system, the operator pushes the button again to reactivate the ring signal trap. The TelGuard™ defaults to lock mode during power outages. In a distress mode, the TelGuard™ allows the PBX to dial out to the maintenance technician when a trouble report is generated. In this case the TelGuard™ detects the off-hook condition of the PBX and connects the PBX to the central office (CO) line.

The TelGuard™ II operates in the same fashion but, has an additional feature that allows access 24 hours a day. The using organization can issue up to 40 access codes to authorized users. When an authorized maintenance technician calls and enters his unique access code the unit hangs up. The TelGuard™ verifies the code and calls, on a second line, the telephone number assigned to that access code. Once the remote site answers the call back, a script is run to change the remote modem to the "originate caller" mode. The TelGuard™ II then opens the port to the PBX, waits for an off-hook indicator, and connects the PBX line to the CO line. The call back features and telephone numbers are hard coded into the unit and cannot be remotely altered. Programming can be done by the user or by the installer and can only occur with the unit disconnected from the PBX and attaching a dual-tone multi-frequency (DTMF) phone into the PBX jack of the unit.

For the TelGuard™ II, If a hacker randomly dials the number and enters an access code, the unit again hangs up. The unit will compare the access code to the authorized list. If it finds a match, it will dial

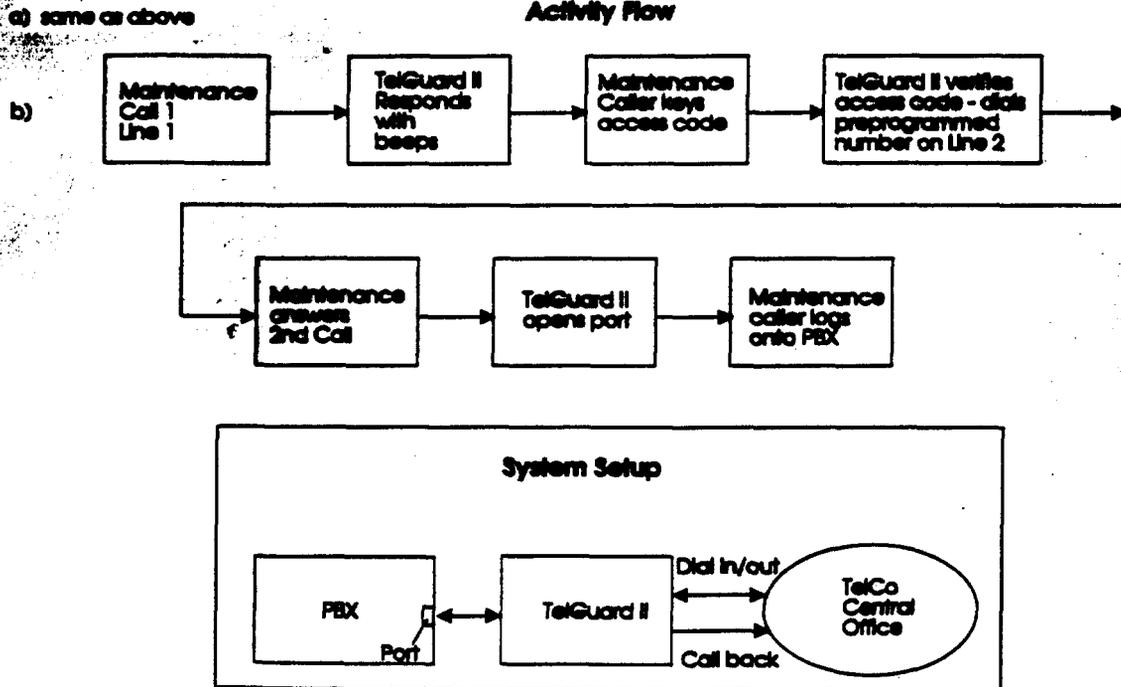
TelGuard™

Activity Flow



TelGuard™ II

Activity Flow



the corresponding authorized user number and not the hacker. Using the second line for call back circumvents published methods for breaking.

C. PRODUCT DETAILS:

TelGuard™ and TelGuard™ II are commercially available from TeleDesign Management, Incorporated. TeleDesign Management is a privately held California corporation that has been in business since January 1993. The principal owners are Stan Distel, President & CEO, Ed Simonson, VP-Marketing and Sales, and Don Costa, VP-Operations. All three are retired Pacific Bell and AT&T employees with a total of 80+ years experience in telecommunications.

TelGuard™ measures 5.65 inches long by 4.24 inches wide by 1.25 inches high, weighs 1 pound, and can be wall or desk mounted at the customers' convenience. TelGuard™ requires 15 to 35 Vdc, 30+ milliamperes of power to operate.

TelGuard™ II, the larger of the two, measures 7 inches long by 6.3 inches wide by 1.6 inches high, weighs 3 pounds and can be wall or desk mounted at the customers convenience. TelGuard™ II uses a 120 Vac 60 Hz transformer that generates the required 24Vdc 340 milliamperes power. Both products were developed under internal funding. They are designed for all AT&T Definity, Rolm, and Northern Telecom SL100 PBXs. Both use standard phone jacks and cables.

D. PRODUCT STATUS:

Both TelGuard™ and TelGuard™ II are available today from TeleGuard Management, Inc. The only known government installations are in Veterans Administrative offices located in California.

E. FUNDING STATUS:

There has been no cost to the government to date for development of these products. The only anticipated costs are for acquisition of either product should a government facility decide to purchase them and potential labor costs associated with operating the unit. Purchase prices are \$1,000 for the TelGuard™ and \$2,000 for the TelGuard™ II.

F. DOCUMENTATION STATUS:

Operating instructions and the FCC Approval Report which contains the product specifications and schematics are available from TeleDesign Management for TelGuard™. An Owners Manual and the FCC Approval Report are available for TelGuard™ II. No technical documentation was provided for this analysis. Sales brochures, the AT&T Bell Laboratories Compliance Report, and several articles on the threat were received. TeleDesign Management has agreed to submit all design documentation, reports, analyses and sample units to the government if there is a decision to submit the products to NSA for a security product profile analysis.

G. TECHNICAL ANALYSIS:

1. **Architectural Compliance:** The products can provide a first line defense against hacker penetration to administrative and maintenance ports of PBX and Voice Mail systems. They are End System (ES) support devices. They are not distributed information processing devices. They are not intended to support information processing among multilevel users or systems. They do provide a degree of ES protection from hostile Communication Networks (CN). The units are designed to prevent toll fraud and denial of service due to unauthorized access and reprogramming of the ES. Either type of unit can only protect the port to which it is connected and works only when the port (or its modem) is active or connected to a CN. They do not fit into the DoD Goal Security Architecture (DGSA), but may have a role as transitional products.
2. **Engineering and Design:** The units can protect most dial-in modem interfaces from remote hostile attacks. They provide a mechanical barrier between a local modem (i.e., PBX) and a telephone line that is disabled only by trusted human intervention, and in the case of TelGuard™ II by a call back feature to a predetermined, hard coded phone number. Call back is done on a separate phone line which foils any attempt to defeat the system. cursory examination (telephone conversations with the manufacturer and review of the sales literature) found no apparent technical weaknesses.

H. REQUIREMENTS ANALYSIS:

We were not able to identify any formal statements of requirements (e.i., Require Operational Capability (ROC)) for access port protection. The threat is well documented in hacker bulletin boards, hacker publication such as 2600, and in trade and newspaper accounts of penetrations to the INTERNET and other information systems. There is an operational requirement for such a protection device at sites that have a remote access capability, whether it be on a PBX or other computer based communications device.

Either product provides I/O port protection in the form of denial of access to unauthorized users. Denial of access to the I/O port helps to ensure that unauthorized users can't penetrate the system and establish bogus accounts or reprogram it for their benefit.

The products cannot protect against an aggressive attack against voice mail, or direct inward service access (the ability to dial into your office, key in an access code and dial out long distance, if that service is available). It cannot protect against poor programming by the PBX installer. Nor can it protect against trojan horses or malicious code that existed in the software prior to installation or that was planted during maintenance by a disgruntled employee.

TeleDesign Management provided an AT&T Bell Laboratories Proprietary Compliance Report which concluded both products met the "expressed requirements of NetPROTECT™ service tariff and can be listed as acceptable for protecting consumer telephone systems."

Unauthorized access by a hacker can result in thousands of dollars of long distance phone calls, or toll fraud for which, the courts have ruled, the company is liable. For a thorough discussion of the threat and status of current Network Security activities, see attached reports 1 and 2. These products can prevent such access.

I. ACCREDITATION:

No product certification is anticipated. If a PBX system that uses one of these products is to undergo certification, the unit will be subjected to the same level of scrutiny as the PBX.

J. ISSUES:

No technical issues were found during our review. There are operational issues which should be considered.

1. Budget and Manpower Downsizing. All services and agencies are experiencing shrinking budgets and are being forced to reduce the size of their forces. This reduces the availability of hands on operators for PBXs and other equipments.

2. Evolution of Remote Network Management Systems. Due to a number of factors, one of which is discussed above, the government is migrating away from full-time, on-site staffing of telephone switches and towards remote operations and maintenance. This "lights out operation" philosophy increases the need for products like the TelGuard™ II.

K. ASSESSMENT:

Lengthy discussions with the designer of the products, Don Costa, VP Services, TeleDesign Management, Inc., (415)-259-1688, revealed they are low cost, reliable products to deter high level PBX hackers. Both the TelGuard™ and TelGuard™ II protect active administrative and maintenance ports of Voice Mail Systems, PBXs and telephone switches. They also provide protection to any other type of active modem or modem-like system. One TelGuard™ unit can only protect one port. Sites that implement policies mandating that administrative and maintenance ports remain inactive, with strictly controlled and monitored exceptions, will receive little or no additional protection from these products. Discussions with MILDEP representatives have not revealed any such DoD operating policy.

L. RECOMMENDATIONS:

It is recommended that:

1. An additional effort be undertaken to educate DoD users on the potential INFOSEC problem of hacker ingress to government owned information processing systems and PBXs, and to help them document their requirements to counter the threat.
2. A vulnerability analysis of all government PBX switches with respect to remote access be initiated.
3. An industry search of technologies and products that are designed to protect dial-in access be initiated.

4. Products such as, TelGuard™ and Telguard™ II, be considered for use in government facilities where remote, online programming access to a computer or phone system is required.

5. A security profile evaluation of TelGuard™ and TelGuard™ II be performed.