```
% = % = % = % = % = % = % = %
=                           =
%   P h r a c k   X V I I   %
=                           =
% = % = % = % = % = % = % = %
```

Phrack Seventeen
07 April 1988

File 1 of 12 : Phrack XVII Introduction

It's been a long time, but we're back. After two successful releases under the new editorship, Taran King told us that with his vacation from school, he'd be able to put Phrack Seventeen together. His plans soon changed, and Seventeen was now our responsibility again. Procrastination set in, and some difficulty was encountered in compiling the files, but we finally did it and here it is.

There's a lot of good material in this issue, and we're lucky enough to have PWN contributions from several sources, making it a true group effort. Since The Mad Chemist and Sir Francis Drake, as well as myself, are moving on to other things, the editorship of Phrack Inc. may be changing with the release of Phrack Eighteen. Regardless of what direction the publication takes, I know that I will have no part in the creation of the next issue, so I'd like to mention at this time that my involvement with the magazine, first as a contributor and later as a contributing editor, has been fun. Phrack will go on, I'm sure, for another seventeen issues at least, and will continue to be a primary monument to the vitality of the hacker culture.

-- Shooting Shark
Contributing Editor

Phrack XVII Table of Contents

```
% = % = % = % = % = % = % = %
=                           =
%   P h r a c k   X V I I   %
=                           =
% = % = % = % = % = % = % = %
```

Phrack Seventeen
07 April 1988

File 2 of 12 : Dun & Bradstreet Report on AT&T

AT&T Credit File, taken from Dun & Bradstreet by Elric of Imrryr

DUN'S FINANCIAL RECORDS
COPYRIGHT (C) 1987
DUN & BRADSTREET CREDIT SERVICE

Name & Address:
AMERICAN TELEPHONE AND TELEGRAPH
550 Madison Ave
NEW YORK, NY 10022

Trade-Style Name:
AT & T

Telephone: 212-605-5300

DUNS Number: 00-698-0080

Line of Business: TELECOMMUNICATIONS SVCS TELE

Primary SIC Code: 4811
Secondary SIC Codes: 4821 3661 3357 3573 5999

Year Started: 1885		(12/31/86)	COMBINATION FISCAL
Employees Total:	317,000	Sales:	34,087,000,000
Employees Here:	1,800	Net Worth:	14,462,000,000

This is a PUBLIC company

12/31/86 COMBINATION FISCAL
(Figures are in THOUSANDS)

FINANCIALS	COMPANY	% CHANGE	COMPANY %	INDST NORM %
Cash.	2,602,000	17.5	6.7	9.0
Accounts Receivable	7,820,000	(13.1)	20.1	5.7
Notes Receivable.	----	----	----	0.2
Inventory	3,519,000	(26.1)	9.1	1.3
Other Current Assets.	1,631,000	72.0	4.2	5.8
Total Current Assets.	15,572,000	(8.0)	40.0	22.0
Fixed Assets.	21,078,000	(4.7)	54.2	35.6
Other Non-current Assets. . .	2,233,000	55.9	5.7	42.4
Total Assets.	38,883,000	(3.9)	100.0	100.0
Accounts Payable.	4,625,000	(6.4)	11.9	4.2
Bank Loans.	----	----	----	0.2
Notes Payable	----	----	----	1.0
Other Current Liabilities . .	6,592,000	0.8	17.0	6.2
Total Current Liabilities . .	11,217,000	(2.4)	28.8	11.6

Other Long Term Liab.	13,204,000	38.2	34.0	46.8
Deferred Credits.	----	----	----	6.4
Net Worth	14,462,000	(1.2)	37.2	35.2
Total Liabilities & Worth. .	38,883,000	(3.9)	100.0	100.0
Net Sales	34,087,000	(2.4)	100.0	100.0
Gross Profit.	15,838,000	----	46.5	40.1
Net Profit After Tax.	139,000	(91.1)	0.4	15.3
Dividends/Withdrawals	1,371,000	(0.9)	4.0	7.7
Working Capital	4,355,000	(19.8)	----	----

RATIOS	COMPANY	% CHANGE	---INDUSTRY QUARTILES--- UPPER	MEDIAN	LOWER
(SOLVENCY)					
Quick Ratio	0.9	(10.0)	2.9	1.2	0.6
Current Ratio	1.4	(6.7)	4.9	2.2	1.0
Curr Liab to Net Worth (%). .	77.6	(1.1)	13.2	26.4	38.1
Curr Liab to Inventory (%). .	318.8	32.1	244.8	475.8	675.0
Total Liab to Net Worth (%) .	168.9	(4.3)	127.4	180.2	297.2
Fix Assets to Net Worth (%) .	145.7	(3.6)	144.9	215.0	263.0
(EFFICIENCY)					
Coll Period (days).	83.7	(11.1)	31.9	46.7	61.6
Sales to Inventory.	9.7	32.9	56.2	33.8	20.0
Assets to Sales (%)	114.1	(1.6)	210.5	266.1	373.4
Sales to Net Working Cap. . .	7.8	21.9	6.3	2.3	1.1
Acct Pay to Sales (%)	13.6	(4.2)	4.9	8.7	13.8
(PROFITABILITY)					
Return on Sales (%)	0.4	(91.1)	20.1	14.6	11.3
Return on Assets (%).	0.4	(89.5)	7.2	5.7	3.7
Return on Net Worth (%) . . .	1.0	(90.6)	19.0	15.9	12.8

Industry norms based on 469 firms,

with assets over $5 million.

12/31/85 COMBINATION FISCAL
(Figures are in THOUSANDS)

FINANCIALS	COMPANY	% CHANGE	COMPANY %	INDST NORM %
Cash.	2,213,700	3.4	5.5	7.5
Accounts Receivable	8,996,100	(4.0)	22.2	5.6
Notes Receivable.	----	----	----	0.4
Inventory	4,759,300	(0.6)	11.8	1.2
Other Current Assets.	948,500	(8.2)	2.3	5.1
Total Current Assets.	16,917,600	(2.4)	41.8	19.8
Fixed Assets.	22,112,900	5.2	54.7	39.2
Other Non-current Assets. . .	1,432,000	(3.2)	3.5	41.0
Total Assets.	40,462,500	1.6	100.0	100.0
Accounts Payable.	4,942,800	(11.4)	12.2	4.9
Bank Loans.	----	----	----	0.3
Notes Payable	2,100	----	----	0.8
Other Current Liabilities . .	6,542,600	15.5	16.2	5.9
Total Current Liabilities . .	11,487,500	2.2	28.4	11.9
Other Long Term Liab.	9,553,200	2.7	23.6	46.8
Deferred Credits.	4,788,500	18.9	11.8	6.8
Net Worth	14,633,300	(4.1)	36.2	34.5

Total Liabilities & Worth. .	40,462,500	1.6	100.0	100.0
Net Sales	34,909,500	5.2	100.0	100.0
Gross Profit.	----	----	----	33.7
Net Profit After Tax.	1,556,800	13.6	4.5	14.0
Dividends/Withdrawals	1,382,900	3.7	4.0	13.0
Working Capital	5,430,100	(10.8)	----	----

RATIOS		%	---INDUSTRY QUARTILES---		
	COMPANY	CHANGE	UPPER	MEDIAN	LOWER
(SOLVENCY)					
Quick Ratio	1.0	----	2.5	1.1	0.6
Current Ratio	1.5	----	3.8	1.9	0.9
Curr Liab to Net Worth (%). .	78.5	6.5	15.8	29.4	43.9
Curr Liab to Inventory (%). .	241.4	2.8	285.7	485.5	790.6
Total Liab to Net Worth (%) .	176.5	9.6	134.4	190.1	320.9
Fix Assets to Net Worth (%) .	151.1	9.7	148.4	219.0	289.5
(EFFICIENCY)					
Coll Period (days).	94.1	(8.7)	31.5	47.2	63.8
Sales to Inventory.	7.3	5.8	52.3	31.4	18.0
Assets to Sales (%)	115.9	(3.4)	217.1	277.8	356.8
Sales to Net Working Cap. . .	6.4	16.4	6.0	2.7	1.6
Acct Pay to Sales (%)	14.2	(15.5)	6.1	10.4	15.7
(PROFITABILITY)					
Return on Sales (%)	4.5	9.8	19.0	13.6	9.5
Return on Assets (%).	3.8	11.8	6.9	5.3	3.4
Return on Net Worth (%) . . .	10.6	17.8	19.7	15.8	12.7

Industry norms based on 605 firms,
with assets over $5 million.

12/31/84 COMBINATION FISCAL
(Figures are in THOUSANDS)

FINANCIALS	COMPANY	COMPANY %	INDST NORM %
Cash.	2,139,900	5.4	6.6
Accounts Receivable	9,370,800	23.5	6.3
Notes Receivable.	----	----	0.4
Inventory	4,789,200	12.0	1.2
Other Current Assets.	1,033,100	2.6	4.1
Total Current Assets.	17,333,000	43.5	18.6
Fixed Assets.	21,015,000	52.8	45.0
Other Non-current Assets. . .	1,478,600	3.7	36.4
Total Assets.	39,826,600	100.0	100.0
Accounts Payable.	5,580,300	14.0	5.2
Bank Loans.	----	----	0.2
Notes Payable	----	----	1.0
Other Current Liabilities . .	5,663,300	14.2	5.5
Total Current Liabilities . .	11,243,600	28.2	11.9
Other Long Term Liab.	9,300,200	23.4	47.8
Deferred Credits.	4,026,000	10.1	6.5
Net Worth	15,256,800	38.3	33.8
Total Liabilities & Worth. .	39,826,600	100.0	100.0

Net Sales	33,187,500	100.0	100.0
Gross Profit	16,436,200	49.5	28.1
Net Profit After Tax	1,369,900	4.1	14.1
Dividends/Withdrawals	1,333,800	4.0	7.3
Working Capital	6,089,400	----	----

RATIOS	COMPANY	---INDUSTRY QUARTILES--- UPPER	MEDIAN	LOWER
(SOLVENCY)				
Quick Ratio	1.0	2.3	1.0	0.6
Current Ratio	1.5	3.4	1.6	0.9
Curr Liab to Net Worth (%)	73.7	17.7	30.6	43.5
Curr Liab to Inventory (%)	234.8	312.5	491.6	754.3
Total Liab to Net Worth (%)	161.0	139.2	193.7	314.9
Fix Assets to Net Worth (%)	137.7	161.5	228.9	295.3
(EFFICIENCY)				
Coll Period (days)	103.1	34.3	51.6	67.8
Sales to Inventory	6.9	52.1	32.6	20.1
Assets to Sales (%)	120.0	216.7	268.2	353.0
Sales to Net Working Cap	5.5	7.2	3.1	1.7
Acct Pay to Sales (%)	16.8	6.2	10.9	15.4
(PROFITABILITY)				
Return on Sales (%)	4.1	18.5	13.1	9.8
Return on Assets (%)	3.4	7.0	5.3	3.3
Return on Net Worth (%)	9.0	19.7	15.7	12.6

Industry norms based on 504 firms,
with assets over $5 million.

END OF DOCUMENT

Name & Address:
AMERICAN TELEPHONE AND
550 Madison Ave
NEW YORK, NY 10022

Trade-Style Name:
At & T

Telephone: 212-605-5300

DUNS Number: 00-698-0080

Line of Business: TELECOMMUNICATIONS SVCS TELE

Primary SIC Code: 4811
Secondary SIC Codes: 4821 3661 3357 3573 5999

Year Started: 1885
Employees Total: 317,000
Employees Here: 1,800

(12/31/86) COMBINATION FISCAL
Sales: 34,087,000,000
Net Worth: 14,462,000,000

This is a PUBLIC company

HISTORY
04/20/87

JAMES E. OLSON, CHB-CEO+
RANDALL L TOBIAS, V CHM+
MORRIS TANENBAUM, V CHM+
ROBERT E. ALLEN, PRES-COO+
CHARLES MARSHALL, V CHM+
S. LAWRENCE PRENDERGAST, V PRES-TREAS

C. PERRY COLWELL, V PRES-
CONTROLLER
DIRECTOR(S): The officers identified by (+) and Howard H. Baker Jr, James H. Evans, Peter F. Haas, Philip M. Hawley, Edward G. Jefferson, Belton K. Johnson, Juanita M. Kreps, Donald S. Perkins, Henry B. Schacht, Michael I. Sovern, Donald F. McHenry, Rawleigh Warner Jr, Joseph D. Williams and Thomas H. Wyman.

Incorporated New York Mar 3 1885.

Authorized capital consists of 1,200,000,000 shares common stock $1 par value and 100,000,000 shares preferred stock $1 par value.

Outstanding Capital Stock at Feb 28 1987: 1,071,904,000 common shares and at Dec 31 1986 preferred stock outstanding consisted of redeemable preferred shares composed of 8,500,000 shares of $3.64 preferred stated value $50; 8,800,000 shares of $3.74 preferred, stated value $50 and 25,500 shares of $77.50 preferred, stated value $1,000.

Business started 1885.

The company's common stock is listed on the New York, Boston, Midwest, Philadelphia and Pacific Coast Stock Exchanges under the symbol "ATT". At Dec 31 1986 there were 2,782,102 common shareholders. At Jan 1 1986 officers and directors as a group owned less than 1% of the outstanding common stock with the remainder owned by the public.

OLSON, born 1925. 1950 Univ of North Dakota, BSC. Also attended Univ of Pennsylvania. 1943-1946 United States Army Air Force. 1960-1970 Northwestern Bell Telephone Co, V Pres-Gen Mgr. 1970-1974 Indiana Bell Telephone Co, Pres. 1974-1977 Illinois Bell Telephone Co, Pres. 1977 to date AT&T, 1979 V Chb-Dir; Jun 1985 President, 1986 CHM.

MARSHALL, born 1929, married. 1951 Univ of Illinois, BS; also attended Bradley Univ; 1953-present AT&T; 1980 Asst Treas, 1976 Vice Pres-Treas; 1985 Exec Vice President, 1986 V-CHM.

TANENBAUM, born 1928 married. 1949 Johns Hopkins Univ, BA chemistry. 1950 Princeton Univ, MA chemistry. 1952 PhD in physical chemistry. 1952 to date AT&T, various positions, 1985 Ex Vice Pres, 1986 V-CHM.

PRENDERGAST, born 1941 married. 1963 Brown Univ, BA. 1969 New York Univ, MBA. 1963-1973 Western Electric Company; 1973 to date AT&T, 1980 Asst Treas, 1984 V Pres-Treas.

COLWELL, born 1927. Attended AT&T Institute of Technology. 1945-1947 U S Army. Employed by AT&T and its subsidiaries since 1948 in various positions. 1984 Vice Pres & Contr, AT&T Technologies Inc (subsidiary); 1985-present V Pres-Contr.

ALLEN born 1935 married. 1957 Wabash College BA. Has held a vareity of executive position with former Bell Operating subsidiaries and AT&T subsidiaries. Appointed to current position in 1986.

TOBIAS born 1943. 1964 Indiana University with a BS in Marketing. Has held a variety of management and executive positions with former Bell Operating subsidiaries and AT&T subsidiaries. Elected to current position in 1986.

OTHER OFFICERS: James R. Billingsley, Sr V Pres Federal Regulation; Michael Brunner, Ex V Pres Federal Systems; Harold Burlingame, Sr V Pres Public Relations and Employee Information; Vittorio Cassoni, Sr V Pres Data Systems Division; Richard Holbrook, Sr V Pres Business Sales; Robert Kavner, Sr V Pres & CFO; Gerald Lowrie, Sr V Pres Public Affairs; John Nemecek, Ex V Pres Components & Electronic Systems; John O'Neill, Ex V Pres National Systems Products; Alfred Partoll, Sr V Pres External Affairs; John Segall, Sr V Pres Corporate Strategy & Development; Alexander Stack, Sr V Pres Communications Systems; Paul Villiere, Ex V Pres Network Systems Marketing and Customer Operations; John Zegler, Sr V Pres and General Counsel; and Lydell Christensen, Corp V Pres and Secretary.

DIRECTORS: MCHENRY, research professor, Georgetown University. BAKER JR, partner, Vinson & Elkins and Baker, Worthington, Crossley, Stansberry & Woolf, attorneys. EVANS, former Chairman, Union Pacific Corporation. HAAS, Chairman, Levi Strauss & Company. HAWLEY, Chairman, Carter Hawley Hale Stores Inc. JEFFERSON, former Chairman, E.I. du Pont de Nemours and Company. JOHNSON, private investor and owner of The Chaparrosa Ranch. KREPS, former United States Secretary of Commerce. PERKINS, former Chairman, Jewel Companies Inc. SCHACHT, Chairman, Cummins Engine Company Inc. SOVERN, President, Columbia University.

WARNER JR, former Chairman, Mobil Corporation. WILLIAMS, Chairman, Warner Lambert Company. WYMAN, former Chairman, CBS Inc.

As a result of an antitrust action entered against American Telephone and Telegraph Company (AT&T) by the Department of Justice, AT&T agreed in Jan 1982 to break up its holdings. In Aug 1982, the U. S. District Court-District of Columbia, entered a consent decree requiring AT&T to divest itself of portions of its operations.

The operations affected consisted of exchange telecommunications, exchange access functions, printed directory services and cellular radio telecommunications services. AT&T retained ownership of AT&T Communications Inc, AT&T Technologies Inc, Bell Telephone Laboratories Incorporated, AT&T Information Systems Inc, AT&T International Inc and those portions of the 22 Bell System Telephone Company subsidiaries which manufactured new customer premises equipment. The consent decree, with modifications, was agreed to by AT&T and the U. S. Department of Justice and approved by the U. S. Supreme Court in Feb 1983. In Dec 1982, AT&T filed a plan of reorganization, outlining the means of compliance with the divestiture order. The plan was approved by the court in Aug 1983

The divestiture completed on Jan 1 1984, was accomplished by the reorganization of the 22 principal AT&T Bell System Telephone Company subsidiaries under 7 new regional holding companies. Each AT&T common shareowner of record as of Dec 10 1983 received 1 share of common stock in each of the newly formed corporations for every 10 common shares of AT&T. AT&T common shareowners retained their AT&T stock ownership.

The company has an ownership interest in certain ventures to include:

(1) Owns 22% of the voting stock of Ing C. Olivetti & C., S.p.A. of Milan, Italy with which the company develops and markets office automation products in Europe.

(2) Owns 50% of a joint venture with the N. V. Philips Company of the Netherlands organized to manufacture and market switching and transmission systems in Europe and elsewhere.

(3) Owns 44% of a joint venture with the Goldstar Group of the Republic of Korea which manufactures switching products and distributes the company's 3B Family of Computers in Korea.

The company also maintain stock interests in other concerns.

In addition to joint venture activities described above, intercompany relations have also included occasional advances from subject.

OPERATION
04/20/87

Through subsidiaries, provides intrastate, interstate and international long distance telecommunications and information transport services, a broad range of voice and data services including, Domestic and Long Distance Service, Wide Area Telecommunications Services (WATS), 800 Service, 900 Dial It Services and a series of low, medium and high speed digital voice and data services known as Accunet Digital Services. Also manufactures telephone communications equipment and apparatus, communications wire and cable, computers for use in communications systems, as well as for general purposes, retails and leases telephone communications equipment and provides research and development in information and telecommunications technology. The company is subject to the jurisdiction of the Federal Communications Commission with respect to interstate and international rates, lines, services and other matters. Terms: Net 30, cash and contract providing for progress payments with final payment upon completion. The company's AT&T Communications Inc subsidiary provides interstate and intrastate long distance communications services for 80 million residential customers and 7 million businesses. Sells to a wide variety of businesses, government agencies, individuals and others. Nonseasonal.

EMPLOYEES: 317,000 including officers. 1,800 employed here.

FACILITIES: Owns premises in multi story steel building in good condition. Premises neat.

LOCATION: Central business section on main street.

BRANCHES: The company's subsidiaries operate 19 major manufacturing plants located throughout the United States containing a total 26.2 million square feet of space of which 1.49 million square feet were in leased premises. There are 7 regional centers and 24 distribution centers. In addition, there are numerous domestic and foreign branch offices.

SUBSIDIARIES: The company had numerous subsidiaries as of Dec 31 1986. Subsidiaries perform the various services and other functions described above. Its unconsolidated finance subsidiary, AT&T Credit Corporation, provides financing to customers through leasing and installment sales programs and purchases from AT&T's subsidiaries the rights to receivables under long-term service agreements. Intercompany relations consists of parent making occasional advances to subsidiaries and service transactions settled on a convenience basis. A list of principal subsidiaries as of Dec 31 1986 is on file at the Millburn, NJ office of Dun & Bradstreet.

08-27(9Z0 /61) 00703 001 678 NH

Chemical Bank, 277 Park Ave; Marine Midland Bank, 140 Broadway; Chase Manhattan Bank, 1 Chase Manhattan Plaza

12/31/86 COMBINATION FISCAL
(Figures are in THOUSANDS)

FINANCIALS	COMPANY	% CHANGE	COMPANY %	INDST NORM %
Total Current Assets.	15,572,000	(8.0)	40.0	22.0
Fixed Assets.	21,078,000	(4.7)	54.2	35.6
Other Non-current Assets. . .	2,233,000	55.9	5.7	42.4
Total Assets.	38,883,000	(3.9)	100.0	100.0
Total Current Liabilities . .	11,217,000	(2.4)	28.8	11.6
Other Long Term Liab.	13,204,000	38.2	34.0	46.8
Net Worth	14,462,000	(1.2)	37.2	35.2
Total Liabilities & Worth. .	38,883,000	(3.9)	100.0	100.0
Net Sales	34,087,000	(2.4)	100.0	100.0
Gross Profit.	15,838,000	----	46.5	40.1

RATIOS	COMPANY	% CHANGE	---INDUSTRY QUARTILES--- UPPER	MEDIAN	LOWER
Quick Ratio	0.9	(10.0)	2.9	1.2	0.6
Current Ratio	1.4	(6.7)	4.9	2.2	1.0
Total Liab to Net Worth (%) .	168.9	(4.3)	127.4	180.2	297.2
Sales to Inventory.	9.7	32.9	56.2	33.8	20.0
Return on Sales (%)	0.4	(91.1)	20.1	14.6	11.3
Return on Assets (%).	0.4	(89.5)	7.2	5.7	3.7
Return on Net Worth (%) . . .	1.0	(90.6)	19.0	15.9	12.8

Industry norms based on 469 firms,
with assets over $5 million.

End_of_File.

```
% = % = % = % = % = % = % = %
=                           =
%   P h r a c k   X V I I   %
=                           =
% = % = % = % = % = % = % = %
```

Phrack Seventeen
07 April 1988

File 3 of 12 : Dun & Bradstreet Report on Pacific Telesis

Pacific Telesis Credit File, taken from Dun & Bradstreet by Elric of Imrryr

Name & Address:
PACIFIC TELESIS GROUP (INC)
140 New Montgomery St
SAN FRANCISCO, CA 94105

Telephone: 415-882-8000

DUNS Number: 10-346-0846

Line of Business: TELECOMMUNICATION SERVICES

Primary SIC Code: 4811
Secondary SIC Codes: 2741 5063 5732 6159

Year Started: 1906		(12/31/86)	COMBINATION FISCAL
Employees Total:	74,937	Sales:	8,977,300,000
Employees Here:	2,000	Net Worth:	7,753,300,000

This is a PUBLIC company

12/31/86 COMBINATION FISCAL
(Figures are in THOUSANDS)

FINANCIALS	COMPANY	% CHANGE	COMPANY %	INDST NORM %
Cash.	200,600	671.5	1.0	9.0
Accounts Receivable	1,390,700	(3.8)	6.8	5.7
Notes Receivable.	----	----	----	0.2
Inventory	116,300	(4.4)	0.6	1.3
Other Current Assets.	448,700	18.6	2.2	5.8
Total Current Assets.	2,156,300	9.3	10.6	22.0
Fixed Assets.	17,244,900	1.6	84.9	35.6
Other Non-current Assets. . .	919,300	53.8	4.5	42.4
Total Assets.	20,320,500	4.0	100.0	100.0
Accounts Payable.	1,760,300	74.1	8.7	4.2
Bank Loans.	21,800	847.8	0.1	0.2
Notes Payable	----	----	----	1.0
Other Current Liabilities . .	623,000	(35.8)	3.1	6.2
Total Current Liabilities . .	2,405,100	21.3	11.8	11.6
Other Long Term Liab.	5,564,600	(7.6)	27.4	46.8
Deferred Credits.	4,597,500	9.0	22.6	6.4
Net Worth	7,753,300	6.0	38.2	35.2

Total Liabilities & Worth. .	20,320,500	4.0	100.0	100.0
Net Sales	8,977,300	5.6	100.0	100.0
Gross Profit.	----	----	----	40.1
Net Profit After Tax.	1,079,400	16.2	12.0	15.3
Dividends/Withdrawals	654,100	10.0	7.3	7.7
Working Capital	248,800	(999.9)	----	----

RATIOS	COMPANY	% CHANGE	---INDUSTRY QUARTILES--- UPPER	MEDIAN	LOWER
(SOLVENCY)					
Quick Ratio	0.7	----	2.9	1.2	0.6
Current Ratio	0.9	(10.0)	4.9	2.2	1.0
Curr Liab to Net Worth (%). .	31.0	14.4	13.2	26.4	38.1
Curr Liab to Inventory (%). .	999.9	26.9	244.8	475.8	675.0
Total Liab to Net Worth (%) .	162.1	(2.9)	127.4	180.2	297.2
Fix Assets to Net Worth (%) .	222.4	(4.1)	144.9	215.0	263.0
(EFFICIENCY)					
Coll Period (days).	56.5	(9.0)	31.9	46.7	61.6
Sales to Inventory.	77.2	10.6	56.2	33.8	20.0
Assets to Sales (%)	226.4	(1.5)	210.5	266.1	373.4
Sales to Net Working Cap. . .	----	----	6.3	2.3	1.1
Acct Pay to Sales (%)	19.6	64.7	4.9	8.7	13.8
(PROFITABILITY)					
Return on Sales (%)	12.0	10.1	20.1	14.6	11.3
Return on Assets (%).	5.3	10.4	7.2	5.7	3.7
Return on Net Worth (%) . . .	13.9	9.4	19.0	15.9	12.8

Industry norms based on 469 firms,

with assets over $5 million.

12/31/85 COMBINATION FISCAL
(Figures are in THOUSANDS)

FINANCIALS	COMPANY	% CHANGE	COMPANY %	INDST NORM %
Cash.	26,000	550.0	0.1	7.5
Accounts Receivable	1,446,200	20.6	7.4	5.6
Notes Receivable.	----	----	----	0.4
Inventory	121,700	----	0.6	1.2
Other Current Assets.	378,300	(8.3)	1.9	5.1
Total Current Assets.	1,972,200	22.1	10.1	19.8
Fixed Assets.	16,968,400	6.1	86.8	39.2
Other Non-current Assets. . .	597,700	29.4	3.1	41.0
Total Assets.	19,538,300	8.1	100.0	100.0
Accounts Payable.	1,011,100	14.6	5.2	4.9
Bank Loans.	2,300	----	----	0.3
Notes Payable	----	----	----	0.8
Other Current Liabilities . .	969,900	18.6	5.0	5.9
Total Current Liabilities . .	1,983,300	(1.0)	10.2	11.9
Other Long Term Liab.	6,021,700	0.8	30.8	46.8
Deferred Credits.	4,216,300	16.6	21.6	6.8
Net Worth	7,317,000	12.9	37.4	34.5
Total Liabilities & Worth. .	19,538,300	8.1	100.0	100.0
Net Sales	8,498,600	8.6	100.0	100.0

Gross Profit.	----	----	----	33.7
Net Profit After Tax.	929,100	12.1	10.9	14.0
Dividends/Withdrawals	594,400	11.9	7.0	13.0
Working Capital	11,100	----	----	----

RATIOS		%	---INDUSTRY QUARTILES---		
	COMPANY	CHANGE	UPPER	MEDIAN	LOWER
(SOLVENCY)					
Quick Ratio	0.7	16.7	2.5	1.1	0.6
Current Ratio	1.0	25.0	3.8	1.9	0.9
Curr Liab to Net Worth (%). .	27.1	(12.3)	15.8	29.4	43.9
Curr Liab to Inventory (%). .	999.9	----	285.7	485.5	790.6
Total Liab to Net Worth (%) .	167.0	(6.7)	134.4	190.1	320.9
Fix Assets to Net Worth (%) .	231.9	(6.0)	148.4	219.0	289.5
(EFFICIENCY)					
Coll Period (days).	62.1	11.1	31.5	47.2	63.8
Sales to Inventory.	69.8	----	52.3	31.4	18.0
Assets to Sales (%)	229.9	(0.5)	217.1	277.8	356.8
Sales to Net Working Cap. . .	----	----	6.0	2.7	1.6
Acct Pay to Sales (%)	11.9	5.3	6.1	10.4	15.7
(PROFITABILITY)					
Return on Sales (%)	10.9	2.8	19.0	13.6	9.5
Return on Assets (%).	4.8	4.3	6.9	5.3	3.4
Return on Net Worth (%) . . .	12.7	(0.8)	19.7	15.8	12.7

Industry norms based on 605 firms,
with assets over $5 million.

12/31/84 COMBINATION FISCAL
(Figures are in THOUSANDS)

FINANCIALS	COMPANY	COMPANY %	INDST NORM %
Cash.	4,000	----	6.6
Accounts Receivable	1,198,800	6.6	6.3
Notes Receivable.	----	----	0.4
Inventory	----	----	1.2
Other Current Assets.	412,400	2.3	4.1
Total Current Assets.	1,615,200	8.9	18.6
Fixed Assets.	15,999,500	88.5	45.0
Other Non-current Assets. . .	461,800	2.6	36.4
Total Assets.	18,076,500	100.0	100.0
Accounts Payable.	882,100	4.9	5.2
Bank Loans.	----	----	0.2
Notes Payable	304,000	1.7	1.0
Other Current Liabilities . .	817,600	4.5	5.5
Total Current Liabilities . .	2,003,700	11.1	11.9
Other Long Term Liab.	5,973,500	33.0	47.8
Deferred Credits.	3,617,000	20.0	6.5
Net Worth	6,482,300	35.9	33.8
Total Liabilities & Worth. .	18,076,500	100.0	100.0
Net Sales	7,824,300	100.0	100.0
Gross Profit.	----	----	28.1
Net Profit After Tax.	828,500	10.6	14.1
Dividends/Withdrawals	531,200	6.8	7.3

Working Capital	388,500	----	----

RATIOS	COMPANY	---INDUSTRY QUARTILES--- UPPER	MEDIAN	LOWER
(SOLVENCY)				
Quick Ratio	0.6	2.3	1.0	0.6
Current Ratio	0.8	3.4	1.6	0.9
Curr Liab to Net Worth (%). .	30.9	17.7	30.6	43.5
Curr Liab to Inventory (%). .	----	312.5	491.6	754.3
Total Liab to Net Worth (%) .	178.9	139.2	193.7	314.9
Fix Assets to Net Worth (%) .	246.8	161.5	228.9	295.3
(EFFICIENCY)				
Coll Period (days).	55.9	34.3	51.6	67.8
Sales to Inventory.	----	52.1	32.6	20.1
Assets to Sales (%)	231.0	216.7	268.2	353.0
Sales to Net Working Cap. . .	----	7.2	3.1	1.7
Acct Pay to Sales (%)	11.3	6.2	10.9	15.4
(PROFITABILITY)				
Return on Sales (%)	10.6	18.5	13.1	9.8
Return on Assets (%).	4.6	7.0	5.3	3.3
Return on Net Worth (%) . . .	12.8	19.7	15.7	12.6

Industry norms based on 504 firms,
with assets over $5 million.

END OF DOCUMENT

Name & Address:

PACIFIC TELESIS GROUP (INC)
140 New Montgomery St
SAN FRANCISCO, CA 94105

Telephone: 415-882-8000

DUNS Number: 10-346-0846

Line of Business: TELECOMMUNICATION SERVICES

Primary SIC Code: 4811
Secondary SIC Codes: 2741 5063 5732 6159

Year Started: 1906		(12/31/86)	COMBINATION FISCAL
Employees Total:	74,937	Sales:	8,977,300,000
Employees Here:	2,000	Net Worth:	7,753,300,000

This is a PUBLIC company

HISTORY
09/01/87

DONALD E GUINN, CHB PRES+
SAM L GINN, V CHB+
ROBERT V R DALENBERG, EX V PRES GEN COUNSEL SEC
ARTHUR C LATNO JR, EX V PRES
FRANK V SPILLER, V PRES COMPTROLLER
THEODORE J SAENGER, V CHB GROUP PRES+
JOHN E HULSE, V CHB CFO+
BENTON W DIAL, EX V PRES-HUM RESOURCES
THOMAS G CROSS, V PRES TREAS

DIRECTOR(S): The officers identified by (+) and Norman Barker Jr, William P Clark, Willaim K Coblentz, Myron Du Bain, Herman E Gallegos James R Harvey, Ivan J Houston, Leslie L Luttgens, E L Mc Neely, S Donley Ritchey, Willaim French Smith & Mary S Metz.

Incorporated Nevada Oct 26 1983. Authorized capital consists of 505,000,000 shares common stock, $.10 par value.

OUTSTANDING CAPITAL STOCK: Consists of following at Dec 31 1986: 215,274,878 common shares at a stated value of $21.5 million plus additional paid in capital of $5,068.5 million.

The stock is publicly traded on the New York, Pacific and Midwest Stock Exchanges. There were 1,170,161 common shareholders at Feb 1 1987. Officers and directors as a group hold less than 1% of stock. No other entity owned more than 5% of the common stock outstanding.

The authorized capital stock was increased to $1,100,000,000 shares in 1987 by Charter Amendment. In addition, the company declared a two-for-one stock split in the form of a 100% stock dividend effective Mar 25 1987.

BACKGROUND: This business was founded in 1906 as a California Corporation. The Pacific Telephone & Telegraph Company formed Dec 31 1906. Majority of the stock was held by American Telephone & Telegraph Co (A T & T), New York, NY, prior to divestiture.

DIVESTITURE: Pursuant to a court oder of the U S District Court for the Distirict of Columbia, A T & T divested itself of the exchange, telecommunications, exchange access and printing directory advertising portions of its 22 wholly-owned subsidiary operating telephone companies, including the Pacific Telephone & Telegraph Company. A T & T retains ownership of the former A T & T long lines interstate organization, as well as those portions of the subsidiaries that provide interchange services and customer premises equipment. To accomplish the divestiture, this regional holding company was formed, which took over the applicable operations and assets of the Pacific Telephone & Telegraph Company and its subsidiary, Bell Telephone Company of Nevada. Stock in the subject was distributed to the shareholders of A T & T, who also retained their existing A T & T Stock. The divestiture was accomplished on Jan 1 1984.

RECENT EVENTS:During Jun 1986, the company completed the acquisition of Communications Industries Inc, Dallas, TX.

In Dec 1986, the company's wholly-owned subsidiary Pac Tel Cellular Inc of Michigan signed an agreement to purhcase five cellular telephone properties for $316 million plus certain contingent payments. These five systems operate under the name of Cellular One. This acquaition is subject to regulatory and court approval and final legal review.

----------OFFICERS----------.

GUINN born 1932 married. 1954 received BSCE from Oregon State University. 1954-60 with The Pacific Telephone & Telegraph Company, San Francisco, CA. 1960-64 with Pacific Northwest Bell Telephone Co, Seattle, WA, as vice president. 1964-70 with A T & T. 1970-76 with Pacific Northwest Bell. 1976-80 with A T & T as vice president-network service. 1980 chairman and chief executive officer of The Pacific Telephone & Telegraph Company. 1984 with Pacific Telesis Group as chairman, president and chief executive officer.

SAENGER born 1928 married. 1951 received BS from the University of California. 1946-47 in the U S Army. 1951-52 secretary and manager for the Oakland Junior Chamber of Commerce. 1950-70 held various positions with The Pacific Telephone & Telegraph Company. 1970-71 traffic operations director for Network Administration in New York, A T & T. 1971 with The Pacific Telephone & Telegraph Company. 1974 vice president. 1977 president. 1984 with Pacific Telesis Group as vice chairman and president, Pacific Bell.

GINN born 1937 married. 1959 graduated from Auburn University. 1969 received MS from Stanford University. 1959-60 in the U S Army Signal Corps as captain. 1960 joined A T & T Long Lines. 1977 vice president-staff for A T & T Long Lines. 1978 joined The Pacific Telephone & Telegraph Company as executive vice president-network. 1983 vice chairman. 1984 with Pacific Telesis Group as vice chairman and group president, PacTel Companies.

HULSE born 1933 married. 1955 received BS from the University of South Dakota. 1956-58 in the U S Army. 1958 joined Northwestern Bell

Telephone Co. 1980 joined The Pacific Telephone & Telegraph Company as executive vice president and chief financial officer. 1983 vice chairman. 1984 with Pacific Telesis Group as vice chairman and chief financial officer.

LATNO born 1929 married. Received BS degree from the University of Santa Clara. 1952 with Pacific Telephone & Telegraph Co. 1972 vice president-regulatory. 1975 executive vice president-external affairs. 1984 with Pacific Telesis Group as executive vice president-external affairs.

DALENBERG born 1930 married. Graduated from the University of Chicago Law School and Graduate School of Business. 1956 admitted to practice at the Illinois Bar and in 1973 the California Bar. 1957-67 private law practice in Chicago, IL. 1967-72 general attorney for Illinois Bell. 1972-75 general attorney for The Pacific Telephone & Telegraph Company. 1975 associate general counsel. 1976 vice president and secretary-general counsel. 1984 with Pacific Telesis Group as executive vice president and general counsel-secretary.

CROSS. Vice President and Treasurer and also Vice President of Pacific Bell.

DIAL born 1929 married. 1951 received BA from Whittier College. 1961 received MS from California State University. 1951-53 in the U S Army. 1954 with The Pacific Telephone & Telegraph Company. 1973 vice president-regional staff and operations service for Southern California. 1976 vice president-customer operations in Los Angeles, CA. 1977 vice president-corporate planning. 1980 vice president-human resources. 1984 with Pacific Telesis Group as executive vice president-human resources.

SPILLER born 1931 married. 1953 received BS from the University of California, San Francisco. 1954-56 in the U S Army as a second lieutenant. 1953 with The Pacific Telephone & Telegraph Company. 1977 assistant comptroller. 1981 assistant vice president-finance management. 1981 vice president and comptroller. 1984 with Pacific Telesis Group as vice president and comptroller.

----------OTHER DIRECTORS----------.

BARKER. Retired chairman of First Interstate Bank Ltd.

CLARK. Of counsel to the law firm of Rogers & Wells.

COBLENTZ. Senior Partner in Coblentz, Cahen, Mc Cabe & Breyer, Attorneys, San Francisco, CA.

DU BAIN. Chairman of SRI International.

GALLEGOS. Management consultant.

HARVEY. Chairman, and chief executive officer of Transamerica Corporation, San Francisco, CA.

HOUSTON. Chairman and chief executive officer of Golden State Mutual Life Insurance Co.

LUTTGENS. Is a community leader.

MC NEELY. Chairman and chief executive officer of Oak Industries, Inc, San Diego, CA.

RITCHEY. Retired Chairman of Lucky Stores Inc.

SMITH. Partner in Gibson, Dunn & Crutcher, Attorneys.

METZ. President of Mills College.

OPERATION
09/01/87

Pacific Telesis Group is a regional holding company whose operations are conducted by subsidiaries.

The company's two major subsidiaries, Pacific Bell and Nevada Bell, provide a wide variety of communications services in California and Nevada, including local exchange and toll service, network access and directory advertising, and provided over 90% of total 1986 revenues.

Other subsidiaries, as noted below, are engaged in directory publishing, cellular mobile communications and services, wholesaling of telecommunications products, integrated systems and other services, retails communications equipment and supplies, financing services for products of affiliated customers, real estate development, and consulting. Specific percentages of these operations are not available but in the aggregate represent approximately 10%.

Terms are net 30 days. Has over 11,000,000 accounts. Sells to the general public and commercial concerns. Territory :Worldwide.

EMPLOYEES: 74,937 including officers. 2,000 employed here. Employees are on a consolidated basis as of Dec 31 1986.

FACILITIES: Owns over 500,000 sq. ft. in 20 story concrete and steel building in good condition. Premises neat.

LOCATION: Central business section on side street.

BRANCHES: The subject maintains minor additional administrative offices in San Francisco, CA, but most operating branches are conducted by the operating subsidiaries, primarily Pacific Bell and Nevada Bell in their respective states.

SUBSIDIARIES: Subsidiaries: The Company has the following principal operating subsidiaries, all wholly-owned either directly or indirectly. The telephone subsidiaries account for over 90% of the operating results.

(1) Pacific Bell (Inc) San Francisco CA. Formed 1906 as a California corporation. Acquired in 1984 as part of the divestiture of AT&T. It is the company's largest subsidiary . It provides telecommunicaton services within its service area in California.

(2) Nevada Bell (Inc) Reno NV. Incorporated in 1913. acquired from Pacific Bell in 1984 by the divestiture of its stock. Provides telecommunications, services in Nevada.

(3) Pac Tel Cellular Inc, TX. Renamed subsidiary formerly known as Comminications Industries Inc. Acquired in 1986. Operates as a marketer of cellular and paging services. This subsidiary, in turn, has several primary subsidiaries as follows:.

(a) Gen Com Incorporated. Provides personal paging services.

(b) Multicom Incorporated. Markets paging services.

(4) Pac Tel Personal Communications. Formed to eventually hold all of the company's cellular and paging operations. It is the parent of the following:.

(c) Pac Tel Cellular supports the company's cellular activities.

(d) Pac Tel Mobile Services-formed to rent and sell cellular CPE and paging equipment and resell cellular services, is now largely inactive.

(5) Pac Tel Corporation, San Francisco CA began operations in Jan 1986 as a direct holding company subsidiary. It owns the stock of the following companies:.

(e) Pac Tel Communications Companies-operates two primary divisions, Pac Tel Info Systems and Pac Tel Spectrum Services.

(f) Pac Tel Finance-provides lease financing services.

(g) Pac Tel Properties-engages in real estate transactions holding real estate valued at approximately $140 million at Dec 31 1986.

(h) Pac Tel Publishing -inactive at present.

(i) Pacific Telesis International-manages and operates telecommunicatin businesses in Great Britain, Japan, South Korea, Spain and Thailand.

(6) Pac Tel Capital Resources, San Francisco, CA -provides funding through the sale of debt securities.

INTERCOMPANY RELATIONS: Includes common management, intercompany services, inventory and equipment transactions, loans and advances. In addition, the debt of Pac Tel Capital Resources is backed by a support agreement from the parent with the debt unconditionally guaranteed for repayment without recourse to the stock or assets of the telephone subsidiaries or any interest therein.

08-27(1Z2 /27) 29709 052678678 H

ANALYST: Dan Quinn

12/31/86 COMBINATION FISCAL
(Figures are in THOUSANDS)

FINANCIALS	COMPANY	% CHANGE	COMPANY %	INDST NORM %
Total Current Assets.	2,156,300	9.3	10.6	22.0
Fixed Assets.	17,244,900	1.6	84.9	35.6
Other Non-current Assets. . .	919,300	53.8	4.5	42.4
Total Assets.	20,320,500	4.0	100.0	100.0
Total Current Liabilities . .	2,405,100	21.3	11.8	11.6
Other Long Term Liab.	5,564,600	(7.6)	27.4	46.8
Net Worth	7,753,300	6.0	38.2	35.2

Total Liabilities & Worth. .	20,320,500	4.0	100.0	100.0
Net Sales	8,977,300	5.6	100.0	100.0
Gross Profit.	----	----	----	40.1

RATIOS	COMPANY	% CHANGE	---INDUSTRY QUARTILES--- UPPER	MEDIAN	LOWER
Quick Ratio	0.7	----	2.9	1.2	0.6
Current Ratio	0.9	(10.0)	4.9	2.2	1.0
Total Liab to Net Worth (%) .	162.1	(2.9)	127.4	180.2	297.2
Sales to Inventory.	77.2	10.6	56.2	33.8	20.0
Return on Sales (%)	12.0	10.1	20.1	14.6	11.3
Return on Assets (%).	5.3	10.4	7.2	5.7	3.7
Return on Net Worth (%) . . .	13.9	9.4	19.0	15.9	12.8

Industry norms based on 469 firms,
with assets over $5 million.

% = % = % = % = % = % = % = %
= =
% P h r a c k X V I I %
= =
% = % = % = % = % = % = % = %

Phrack Seventeen
07 April 1988

File 4 of 12 : Nitrogen-Trioxide Explosives

Working notes on Nitrogen Tri-Iodide (NI-3)

By: Signal Sustain

INTRODUCTION

This particular explosive is a real loser. It is incredibly unstable, dangerous to make, dangerous to work with, and you can't do much with it, either. A string of Black Cats is worth far more. At least you can blow up anthills with those.

NI-3 is basically a compound you can make easily by mixing up iodine crystals and ammonia. The resulting precipitate is very powerful and very unstable. It is semi stable when wet (nothing you want to trust) and absolutely unstable when dry. When dry, anything will set it off, such as vibration, wind, sun, a fly landing on it. It has to be one of the most unstable explosives you can deal with.

But it's easy to make. Anyone can walk into a chem supply house, and get a bottle of iodine, and and a supermarket, and get clear ammonia. Mix them and you're there. (See below for more on this)

So, some of you are going to try it, so I might as well pass on some tips from hard experience. (I learned it was a loser by trying it).

Use Small Batches

First, make one very small batch first. Once you learn how powerful this stuff is, you'll see why. If you're mixing iodine crystals (that's right, crystals, iodine is a metal, a halogen, and its solid form is crystals; the junk they sell as "iodine" in the grocery store is about 3% iodine in a bunch of solvents, and doesn't work for this application), you want maybe 1/4 teaspoonful MAX, even less maybe. 1/4 TSP of this stuff is one hellacious bang; it rattled the windows for a block around when it went off in my back yard.

So go with 1/4 TSP, if I can talk you into it. The reason is the instability of this compound. If you mix up two teaspoonfuls and it goes off in your hand, kiss your hand goodbye right down to the wrist. A bucketful would probably level any house you'll find. But 1/4 teaspoon, you might keep your fingers. Since I know you're not going to mix this stuff up with remote tools, keep the quantities small. This stuff is so unstable it's best to hedge your bets.

Note: When holding NI3, try to hold with remote tools -- forceps? But if you have to pick it up, fold your thumb next to your first finger, and grip around with your fingers only. Do not grip the flask the conventional way, fingers on one side, thumb of the other. This way, if it goes, you may still have an opposing thumb, which is enough to get by with.

The compound is far more stable when wet, but not certain-stable. That's why

companies that make explosives won't use it; even a small chance of it blowing up is too dangerous. (They still lose dynamite plants every now and then, too, which is why they're fully automated). But when this stuff gets dry, look out. Heinlein says "A harsh look will set it off", and he isn't kidding. Wind, vibration, a breath across it, anything will trigger it off. (By the way, Heinlein's process, from SF book "Farnham's Freehold", doesn't work, either -- you can't use iodine liquid for this. You must use iodine crystals.)

Don't Store It

What's so wickedly dangerous is if you try to store the stuff. Say you put it in a cup. After a day, a crust forms around the rim of the liquid, and it dries out. You pick up the cup, kabang!, the crust goes off, and the liquid goes up from the shock. Your fingers sail into your neighbor's lawn. If you make this, take extreme pains to keep it all wet. At least stopper the testtube, so it can't evaporate.

Making It

Still want to make it? Okay. Get some iodine crystals at a chem supply store. If they ask, say you need to purify water for a camping trip, and they'll lecture you on better alternatives (halazone) but you can still get it. Or, tell them you've been elected to play Mr. Wizard, and be honest -- you'll probably get it too. Possession is not illegal.

Get as little as possible. You need little and it's useless once you've tried it once. Aim for 1/4 teaspoonful.

Second, get some CLEAR, NON SUDSY ammonia at the store, like for cleaning purposes (BUT NO SUDS! They screw things up, it doesn't make the NI-3).

Third, pour ammonia in a bowl. Peeew! Nice smell.

Fourth, add 1/4 TSP or less of iodine crystals. Note these crystals, which looks like instant coffee, will attack other metals, so look out for your tableware. Use plastic everything (Bowl, spoon) if you can. These crystals will also leave long-standing iodine stains on hands, and that's damned incriminating if there was just an NI-3 explosion and they're looking for who did it. Rubber gloves, please, dispose after use.

Now the crystals will sort of spread out. Stir a little if need be. Be damned careful not to leave solution on the spoon that might dry. It'll go off if you do, believe me. (Experience).

Let them spread out and fizzz. They will. Then after an hour or so there will be left some reddish-brown glop in the bottom of the clear ammonia. It's sticky like mud, hard to handle.. That's the NI-3.

It is safe right now, as it is wet. (DO NOT LET A RIM FORM ON THE AMMONIA LIQUID!)

Using It

Now let's use up this junk right away and DON'T try to store it.

Go put it outside someplace safe. In my high school, someone once sprinkled tiny, tiny bits (like individual crystals) in a hallway. Works good, it's like setting off a cap under someone's shoe after the stuff dries. You need far less than 1/4 TSP for this, too.

Spread it out in the sun, let it dry. DO NOT DISTURB. If you hear a sudden CRACK!, why, it means the wind just blew enough to set it off, or maybe it just went off by itself. It does that too.

It must be thoroughly dry to reach max instability where a harsh look sets it off. Of course the top crystals dry first, so heads up. Any sharp impact will set it off, wet or dry.

While you're waiting for it to dry, go BURN the plastic cup and spoon you made it with. You'll hear small snapping noises as you do; this is the solution drying and going off in the flames.

After two hours or so, toss rocks at the NI3 from a long ways away, and you'll see it go off. Purplish fumes follow each explosion. It's a sharp CRACK, you can't miss it.

Anyway. Like I say, most people make this because the ingredients are so easily available. They make it, say what the hell do I do now?, and sprinkle tiny crystals in the hallway. Bang bang bang. And they never make it again, because you only get one set of fingers per hand, and most people want to keep them.

Or they put it in door locks (while still in the "sludge" form), and wait for it to try. Next person who sticks a key in there has a big surprise.

(This is also why most high school chem teachers lock up the iodine crystals.)

Getting Rid Of It

If you wash the NI-3 crystals down your kitchen sink, then you have to only wait for them to dry out and go off. They'll stick to the pipe (halogen property, there). I heard a set of pipes pop and crackle for days after this was done. I'd recommend going and throwing the mess into a vacant lots or something, and trying to set it off so no one else does accidentally.

If you do this, good luck, and you've been warned.

-- Signal Sustain

% = % = % = % = % = % = % = %
= =
% P h r a c k X V I I %
= =
% = % = % = % = % = % = % = %

Phrack Seventeen
07 April 1988

File 5 of 12 : How to Hack Cyber Systems

How To Hack A CDC Cyber

By: ** Grey Sorcerer

Index:

I'm going to go ahead and skip all the stuff that's in your CDC reference manuals.. what's a local file and all that. If you're at the point of being ready to hack the system, you know all that; if not, you'll have to get up to speed on it before a lot of this will make sense. Seems to me too many "how to hack" files are just short rewrites of the user manuals (which you should get for any serious penetration attempt anyway, or you'll miss lots of possibilities), without any tips on ways to hack the system.

General hacking tips:

Don't get caught. Use remote dialups if possible and never never use any user number you could be associated with. Also never re-use a user number. Remember your typical Cyber site has a zillion user numbers, and they can't watch every one. Hide in numbers. And anytime things get "hot", lay off for awhile.

Magtapes are great. They hold about 60 Meg, a pile of data, and can hold even more with the new drives. You can hide a lot of stuff here offline, like dumps of the system, etc., to peruse. Buy a few top quality ones.. I like Black Watch tapes my site sells to me the most, and put some innocuous crap on the first few records.. data or a class program or whatever, then get to the good stuff. That way you'll pass a cursory check. Remember a usual site has THOUSANDS of tapes and cannot possibly be scanning every one; they haven't time.

One thing about the Cybers -- they keep this audit trail called a "port log" on all PPU and CPU accesses. Normally, it's not looked at. But just remember that *everything* you do is being recorded if someone has the brains and the determination (which ultimately is from you) to look for it. So don't do something stupid like doing real work on your user number, log off, log right onto another, and dump the system. They WILL know.

Leave No Tracks.

Also remember the first rule of bragging: Your Friends Turn You In.

And the second rule: If everyone learns the trick to increasing priority, you'll all be back on the same level again, won't you? And if you show just two friends, count on this: they'll both show two friends, who will show four...

So enjoy the joke yourself and keep it that way.

Fun With The Card Punch

Yes, incredibly, CDC sites still use punch cards. This is well in keeping with CDC's overall approach to life ("It's the 1960's").

The first thing to do is empty the card punch's punchbin of all the little punchlets, and throw them in someone's hair some rowdy night. I guarantee the little suckers will stay in their hair for six months, they are impossible to get out. Static or something makes them cling like lice. Showers don't even work.

The next thing to do is watch how your local installation handles punch card decks. Generally it works like this. The operators love punchcard jobs because they can give them ultra-low priority, and make the poor saps who use them wait while the ops run their poster-maker or Star Trek job at high priority. So usually you feed in your punchcard deck, go to the printout room, and a year later, out comes your printout.

Also, a lot of people generally get their decks fed in at once at the card reader.

If you can, punch a card that's completely spaghetti -- all holes punched. This has also been known to crash the cardreader PPU and down the system. Ha, ha. It is also almost certain to jam the reader. If you want to watch an operator on his back trying to pick pieces of card out of the reader with tweezers, here's your chance.

Next, the structure of a card deck job gives lots of possibilities for fun. Generally it looks like this:

```
  JOB card:  the job name (first 4 characters)
  User Card:  Some user number and  password -- varies with site
EOR card: 7-8-9 are punched
  Your Batch job (typically, Compile This Fortran Program).  You know, FTN.
  LGO.  (means, run the Compiled Program)
EOR card: 7-8-9 are punched
  The Fortran program source code
EOR card: 7-8-9 are punched
  The Data for your Fortran program
EOF card: 6-7-8-9 are punched.  This indicates:  (end of deck)
```

This is extremely typical for your beginning Fortran class.

In a usual mainframe site, the punchdecks accumulate in a bin at the operator desk. Then, whenever he gets to it, the card reader operator takes about fifty punchdecks, gathers them all together end to end, and runs them through. Then he puts them back in the bin and goes back to his Penthouse.

GETTING A NEW USER NUMBER THE EASY WAY

Try this for laughs: make your Batch job into:

```
  JOB card:  the job name (first 4 characters)
  User Card:  Some user number and  password -- varies with site
  EOR card:  7-8-9 are punched
```

COPYEI INPUT,filename: This copies everything following the EOR mark to the filename in this account.
EOR Card: 7-8-9 are punched.

Then DO NOT put an EOF card at the end of your job.

Big surprise for the job following yours: his entire punch deck, with, of course, his user number and password, will be copied to your account. This is because the last card in YOUR deck is the end-of-record, which indicates the program's data is coming next, and that's the next person's punch deck, all the way up to -his- EOF card. The COPYEI will make sure to skip those pesky record marks, too.

I think you can imagine the rest, it ain't hard.

Hacking With Telex

When CDC added timeshare to the punch-card batch-job designed Cyber machines, they made two types of access to the system: Batch and Telex. Batch is a punch-card deck, typically, and is run whenever the operator feels like it. Inside the system, it is given ultra low priority and is squeezed in whenever. It's a "batch" of things to do, with a start and end.

Telex is another matter. It's the timeshare system, and supports up to, oh, 60 terminals. Depends on the system; the more RAM, the more swapping area (if you're lucky enough to have that), the more terminals can be supported before the whole system becomes slug-like.

Telex is handled as a weird "batch" file where the system doesn't know how much it'll have to do, or where it'll end, but executes commands as you type them in. A real kludge.

Because the people running on a CRT expect some sort of response, they're given higher priority. This leads to "Telex thrashing" on heavily loaded CDC systems; only the Telex users get anywhere, and they sit and fight over the machine's resources.

The poor dorks with the punch card decks never get into the machine, because all the Telex users are getting the priority and the CPU. (So DON'T use punch cards.)

Another good tip: if you are REQUIRED to use punch cards, then go type in your program on a CRT, and drop it to the automatic punch. Sure saves trying to correct those typos on cards..

When you're running under Telex, you're part of one of several "jobs" inside the system. Generally there's "TELEX," something to run the line printer, something to run the card reader, the mag tape drivers (named "MAGNET") and maybe a few others floating around. There's limited space inside a Cyber.. would you believe 128K 60-bit words?.. so there's a limited number of jobs that can fit. CDC put all their effort into "job scheduling" to make the best of what they had.

You can issue a status command to see all jobs running; it's educational.

Anyway, the CDC machines were originally designed to run card jobs with lots of magtape access. You know, like IRS stuff. So they never thought a job could "interrupt," like pressing BREAK on a CRT, because card jobs can't. This gives great possibilities.

Like:

Grabbing a Copy Of The System

For instance. Go into BATCH mode from Telex, and do a Fortran compile. While in that, press BREAK. You'll get a "Continue?" verification prompt. Say no, you'd like to stop.

Now go list your local files. Whups, there's a new BIG one there. In fact, it's a copy of the ENTIRE system you're running on -- PPU code, CPU code, ALL compilers, the whole shebang! Go examine this local file; you'll see the whole bloody works there, mate, ready to play with.

Of course, you're set up to drop this to tape or disk at your leisure, right?

This works because the people at CDC never thought that a Fortran compile could be interrupted, because they always thought it would be running off cards. So they left the System local to the job until the compile was done. Interrupt the compile, it stays local.

Warning: When you do ANYTHING a copy of your current batch process shows up on the operator console. Typically the operators are reading Penthouse and don't care, and anyway the display flickers by so fast it's hard to see. But if you copy the whole system, it takes awhile, and they get a blow-by-blow description of what's being copied. ("Hey, why is this %^&$^ on terminal 29 copying the PPU code?") I got nailed once this way; I played dumb and they let me go. ("I thought it was a data file from my program").

Staying "Rolled In"

When the people at CDC designed the job scheduler, they made several "queues." "Queues" are lines.

There's:

1. Input Queue. Your job hasn't even gotten in yet. It is standing outside, on disk, waiting.
2. Executing Queue. Your job is currently memory resident and is being executed, although other jobs currently in memory are competing for the machine as well. At least you're in memory.
3. Timed/Event Rollout Queue: Your job is waiting for something, usually a magtape. Can also be waiting for a given time. Yes, this means you can put a delayed effect job into the system. Ha, ha. You are on disk at this point.
4. Rollout Queue: Your job is waiting its turn to execute. You're out on disk right now doing nothing.

Anyway, let's say you've got a big Pascal compile. First, ALWAYS RUN FROM TELEX (means, off a CRT). Never use cards. If you use cards you're automatically going to be low man on the priority schedule, because the CPU doesn't *have* to get back to you soon. Who of us has time to waste?

Okay, do the compile. Then do a STATUS on your job from another machine. Typically you'll be left inside the CPU (EXECUTE) for 10 seconds, where you'll share the actual CPU with about 10-16 other jobs. Then you'll be rolled-out (ROLLOUT), at which time you're phucked; you have to wait for your priority to climb back up before it'll execute some more of your job. This can take several minutes on a deeply loaded system.

(All jobs have a given priority level, which usually increments every 10 sec or so, until they start executing).

Okay, do this. Press BREAK, then at the "Continue?" prompt, say yes. What happened? Telex had to "roll your job in" to process the BREAK! So you get another free 10 seconds of CPU -- which can get a lot done.

If you sit and hit BREAK - Y <return> every 10 sec or so during a really big job, you will just fly through it. Of course, everyone else will be sitting and staring at their screen, doing nothing, because you've got the computer.

If you're at a school with a Cyber, this is how to get your homework done at high speed.

Macro Library

If you have a typical CDC site, they won't give you access to the "Macro library." This is a set of CPU calls to do various things -- open files, do directory commands, and whatnot. They will be too terrified of "some hacker." Reality: The dimbulbs in power don't want to give up ANY of their power to ANYONE. You can't really do that much more with the Macro library, which gives assembly language access to the computer, than you can with batch commands.. except what you do leaves lots less tracks. They REALLY have to dig to find out what your program did if you use Macro calls.. they have to go to PPU port logs, which is needle in a haystack sort of stuff, vs. batch file logs, which are real obvious.

Worry not. Find someone at Arizona State or Minnesota U. that's cool, and get them to send you a tape of the libraries. You'll get all the code you can stand to look at. By the way they have a great poster tape... just copy the posters to the line printer. Takes a long time to print them but it's worth it. (They have all the classic ones.. man on the moon, various playmates, Spock, etc. Some are 7 frames wide!).

With the Macro library, you can do many cool things.

The best is a demon scanner. All CDC user numbers have controlled access for other users to individual files -- either private, (no access to anyone else), semiprivate (others can read it but a record is made), or public (anyone can diddle your files, no record). What you want is a program (fairly easy to do in Fortran) that counts through user numbers, doing directory commands. If it finds anything, it checks for non semi-private (so no records are made), then copies it to you.

You'll find the damnedest stuff, I guarantee it. Try to watch some system type signing in and get the digits of his user number, then scan variations beginning with that user #. For instance, if he's a SYS1234, then scan all user #'s beginning with SYS (sysaaaa to sys9999).

Since it's all inside the Fortran program, the only record, other than hard-to-examine PPU logs, is a "Run Fortran Program" ("LGO.") on the batch dayfile. If you're not giving the overworked system people reason to suspect that commonplace, every-day student Fortran compile is anything out of the ordinary, they will never bother to check -- the amount of data in PPU logs is OVERWHELMING.

But you can get great stuff.

There's a whole cool library of Fortran-callable routines to do damned near anything a batch command could do in the Minnesota library. Time to get some Minnesota friends -- like on UseNet. They're real cooperative about sending out tapes, etc.

Generally you'll find old files that some System Type made public one day (so a buddy could copy them) then forgot about. I picked off all sorts of stuff like this. What's great is I just claimed my Fortran programs were hanging into infinite loops -- this explained the multi-second CPU execution times. Since there wasn't any readily available record of what I was up to, they believed it. Besides, how many idiot users really DO hang into loops? Lots. Hide in numbers. I got Chess 4.2 this way -- a championship Chess program -- and lots of other stuff. The whole games library, for instance, which was blocked from access to mere users but not to sysfolk.

Again, they *can* track this down if you make yourself obnoxious (it's going to be pretty obvious what you're doing if there's a CAT: SYSAAAA CAT: SYSAAAB CAT: SYSAAAC .. etc. on your PPU port log) so do this on someone else's user number.

RJE Status Checks

Lots of stupid CDC installations.. well, that doesn't narrow the field much.. have Remote Job Entry stations. Generally at universities they let some poor student run these at low pay.

What's funny is these RJE's can do a status on the jobs in the system, and the system screeches to a halt while the status is performed. It gets top priority.

So, if you want to incite a little rebellion, just sit at your RJE and do status requests over and over. The system will be even slower than usual.

The Worm

Warning: This is pretty drastic. It goes past mere self-defense in getting enough priority to get your homework done, or a little harmless exploration inside your system, to trying to drop the whole shebang.

It works, too.

You can submit batch jobs to the system, just as if you'd run them through the punchcard reader, using the SUBMIT command. You set up a data file, then do SUBMIT datafile. It runs separate from you.

Now, let's say we set up a datafile named WORM. It's a batch file. It looks like this:

```
JOB
USER,blah (whatever -- a user number you want crucified)
GET,WORM; get a copy of WORM
SUBMIT,WORM.; send it to system
SUBMIT,WORM.; send it to system
SUBMIT,WORM.; send it to system
SUBMIT,WORM.; send it to system
SUBMIT,WORM.; send it to system
SUBMIT,WORM.; send it to system
SUBMIT,WORM.; send it to system
SUBMIT,WORM.; send it to system
SUBMIT,WORM.; send it to system
SUBMIT,WORM.; send it to system
SUBMIT,WORM.; send it to system
SUBMIT,WORM.; send it to system
SUBMIT,WORM.; send it to system
SUBMIT,WORM.; send it to system
SUBMIT,WORM.; send it to system
SUBMIT,WORM.; send it to system
  (16 times)
(end of file)
```

Now, you SUBMIT WORM. What happens? Worm makes 16 copies of itself and submits those. Those in turn make 16 copies of themselves (now we're up to 256) and submit those. Next pass is 4096. Then 65536. Then...

Now, if you're really good, you'll put on your "job card" a request for high priority. How? Tell the system you need very little memory and very little CPU time (which is true, Submit takes almost nothing at all). The scheduler "squeezes" in little jobs between all the big ones everyone loves to run, and gives ultra-priority to really tiny jobs.

What happens is the system submits itself to death. Sooner or later the input queue overflows .. there's only so much space .. and the system falls apart.

This is a particularly gruesome thing to do to a system, because if the guy at the console (count on it) tries the usual startup, there will still be copies of WORM in the input queue. First one of those gets loose, the system drops again. With any luck the system will go up and down for several hours before someone with several connected brain cells arrives at the operator

console and coldstarts the system.

If you've got a whole room full of computer twits, all with their hair tied behind them with a rubber band into a ponytail, busily running their Pascal and "C" compiles, you're in for a good time. One second they will all be printing -- the printers will be going weep-weep across the paper. Next second, after you run, they will stop. And they will stay stopped. If you've done it right they can't get even get a status. Ha, ha.

The faster the CPU, the faster it will run itself into the ground.

CDC claims there is a limit on the number of jobs a user number can have in the system. As usual they blew it and this limit doesn't exist. Anyway, it's the input queue overflow that kills things, and you can get to the input queue without the # of jobs validation check.

Bear in mind that *anything* in that batch file is going to get repeated ten zillion times at the operator console as the little jobs fly by by the thousands. So be sure to include some charming messages, like:

```
job,blah
user,blah
* eat me!
get,worm
submit,worm .. etc.
```

There will now be thousands of little "eat me!"'s scrolling across the console as fast as the console PPU can print them.

Generally at this point the operator will have his blood pressure really spraying out his ears.

Rest assured they will move heaven and earth to find you. This includes past dayfiles, user logs, etc. So be clean. Remember, "Revenge is a dish best served cold." If you're mad at them, and they know it, wait a year or so, until they are scratching their heads, wondering who hates them this much.

Also: make sure you don't take down a really important job someone else is doing, okay? Like, no medical databases, and so forth.

Now, for a really deft touch, submit a timed/event job. This "blocks" the job for awhile, until a given time is reached. Then, when you're far, far away, with a great alibi, the job restarts, the system falls apart, and you're clear. If you do the timed/event rollout with a Fortran program macro call, it won't even show up on the log.

(Remember that the System Folk will eventually realize, in their little minds, what you've done. It may take them a year or two though).

CHECKPOINT / RESTART

I've saved the best for last.

CDC's programmers supplied two utilities, called CheckPoint and Restart, primarily because their computers kept crashing before they would finish anything. What Checkpoint does is make a COMPLETE copy of what you're doing - all local files, all of memory, etc. -- into a file, usually on a magtape. Then Restart "restarts" from that point.

So, when you're running a 12 hour computer job, you sprinkle checkpoints throughout, and if the CDC drops, you can restart from your last CKP. It's like a tape backup of a hard disk. This way, you only lose the work done on your data between the last checkpoint and now, rather than the whole 12 hours. Look, this is real important on jobs that take days -- check out your local IRS for details..

Now what's damned funny is if you look closely at the file Checkpoint

generates, you will find a copy of your user validations, which tell everything about you to the system, along with the user files, memory, etc. You'll have to do a little digging in hex to find the numbers, but they'll match up nicely with the display you of your user validations from that batch command.

Now, let's say you CKP,that makes the CKP file. Then run a little FORTRAN program to edit the validations that are inside that CKP-generated file. Then you RESTART from it. Congratulations. You're a self made man. You can do whatever you want to do - set your priority level to top, grab the line printer as your personal printer, kick other jobs off the system (it's more subtle to set their priority to zilch so they never execute), etc. etc. You're the operator.

This is really the time to be a CDC whiz and know all sorts of dark, devious things to do. I'd have a list of user numbers handy that have files you'd like made public access, so you can go in and superzap them (then peruse them later from other signons), and so forth.

There's some gotchas in here.. for instance, CKP must be run as part of a batch file out of Telex. But you can work around them now that you know the people at CDC made RESTART alter your user validations.

It makes sense in a way. If you're trying to restart a job you need the same priority, memory, and access you had when trying to run it before.

Conclusion

There you have it, the secrets of hacking the Cyber.

They've come out of several years at a college with one CDC machine, which I will identify as being somewhere East. They worked when I left; while CDC may have patched some of them, I doubt it. They're not real fast on updates to their operating system.

** Grey Sorcerer

```
% = % = % = % = % = % = % = %
=                           =
%   P h r a c k   X V I I   %
=                           =
% = % = % = % = % = % = % = %
```

Phrack Seventeen
07 April 1988

File 6 of 12 : How to Hack HP2000's

How to Hack an HP 2000

By: ** Grey Sorcerer

Okay, so you've read the HP-2000 basic guides, and know your way around. I will not repeat all that.

There's two or three things I've found that allow you through HP 2000 security.

1. When you log in, a file called HELLO on the user number Z999 is run. A lot of time this file is used to deny you access. Want in? Well, it's just a BASIC program, and an be BREAKed.. but, usually the first thing they do in that program is turn Breaks (interrupts) off by the BRK(0) function. However, if you log in like this:

HELLO-D345,PASS (return) (break)

With the break nearly instantly after the return, a lot of time, you'll abort the HELLO program, and be home free.

2. If you can create a "bad file", which takes some doing, then anytime you try to CSAVE this file (compile and save), the system will quickly fade into a hard crash.

3. How to make a bad file and other goodies:

The most deadly hole in security in the HP2000 is the "two terminal" method. You've got to understand buffers to see how it works. When you OPEN a file, or ASSIGN it (same thing), you get 256 bytes of the file -- the first 256. When you need anymore, you get 256 more. They are brought in off the disk in discrete chunks. They are stored in "buffers."

So. Save a bunch of junk to disk -- programs, data, whatever. Then once your user number is full, delete all of it. The effect is to leave the raw jumbled data on disk.

Pick a time when the system is REAL busy, then:

1. Have terminal #1 running a program that looks for a file to exist (with the ASSIGN) statement as quickly as it can loop. If it finds the file there, it goes to the very end of the file, and starts reading backwards, record by record, looking for data. If it finds data, it lets you know, and stops at an input prompt. It is now running.

2. Have terminal #2 create a really huge data file (OPEN-FILE, 3000) or however it goes.

What happens is terminal #2's command starts zeroing all the sectors of the file, starting at file start. But it only gets so far before someone else needs the processor, and kicks #2 out. The zeroing stops for a sec. Terminal #1 gets in, finds the file there, and reads to the end. What's there? Old trash on disk. (Which can be mighty damned interesting by the way -- did you know HP uses a discrete mark to indicate end-of-buffer? You've just maybe got

yourself a buffer that is as deep as system memory, and if you're clever, you can peek or poke anywhere in memory. If so, keep it, it is pure gold).

But. Back to the action.

3. Terminal #2 completes the OPEN. He now deletes the file. This leaves Terminal #1 with a buffer full of data waiting to be dumped back to disk at that file's old disk location.

4. Terminal #2 now saves a load of program files, as many as are required to fill up the area that was taken up by the deleted big file.

5. You let Terminal #1 past the input prompt, and it writes its buffer to disk. This promptly overlays some program just stored there. Result: "bad program." HPs are designed with a syntax checker and store programs in token; a "bad program" is one that the tokens are screwed up in. Since HP assumes that if a program is THERE, it passed the syntax check, it must be okay... it's in for big problems. For a quick thrill, just CSAVE it.. system tries to semi-compile bad code, and drops.

Really, the classier thing to do with this is to use the "bottomless buffer" to look through your system and change what you don't like.. maybe the password to A000? Write some HP code, look around memory, have a good time. It can be done.

** Grey Sorcerer

```
% = % = % = % = % = % = % = %
=                           =
%   P h r a c k   X V I I   %
=                           =
% = % = % = % = % = % = % = %
```

Phrack Seventeen
07 April 1988

File 7 of 12 : Accessing Government Computers

```
++++++++++++++++++++++++++++++++++++
+   ACCESSING GOVERNMENT COMPUTERS   +
+            (LEGALLY!)              +
+------------------------------------+
+      Written by The Sorceress      +
+    (The Far Side 415/471-1138)     +
++++++++++++++++++++++++++++++++++++
```

Comment: I came across this article in Computer Shopper (Sept. 1987) and it talked about citizens access government computers since we do pay for them with our taxpayers monies. Since then, I have had friends and gone on a few myself and the databases are full of information for accessing. One thing, you usually have to call the sysop for access and give him your real name, address and the like. They call you back and verify your existence. Just a word of warning; crashing a BBS is a crime, so I wouldn't fool with these since they are government based.

National Bureau of Standards -
Microcomputers Electronic Information Exchange.

Sysops: Ted Landberg & Lisa Carnahan
Voice: 301-975-3359
Data: 301-948-5717 300/1200/2400

This BBS is operated by the Institute for Computer Sciences and Technology which is one of four technical organizations within the National Bureau of Standards. This board also contains information on the acquisition, management, security, and use of micro computers.

Census Bureau -
Census Microcomputer and Office Technology Center, Room 1065 FB-3 Washington, D.C. (Suitland, MD)

Sysop: Nevins Frankel
Voice: 301-763-4494
Data: 301-763-4576 300/1200

The purpose of this BBS is to allow users to access the following: Census Microcomputer and office technology information center bulletins and catalogues, software and hardware evaluations, Hardware and software inventories, Census computer club library, Public Domain software, etc.

Census Bureau -
Census Microcomputer and Office Technology Center, Personnel Division, Washington DC.

Voice: 301-763-4494
Data: 301-763-4574 300/1200/2400

The purpose of this board is to display Census Bureau vacancies from entry level to senior management.

Department of Commerce -

Office of the Under Secretary for Economic Affairs, Office of Business Analysis, Economic Bulletin Board.

Sysop: Ken Rogers
Voice: 202-377-0433
Data: 202-377-3870 300/1200

This is another well run BBS with in-depth news about the Department of Commerce Economic Affairs Agencies including current press releases and report summaries.

COE BBS -
Manpower and Force Management Division, Headquarters, U.S. Army Corps of Engineers, 20 Massachusetts Ave. NW, Washington, DC.

Sysop: Rich Courney
Voice: 202-272-1646
Data: 202-272-1514 300/1200/2400

The files database was one of the largest they ever seen. Directory 70 has programs for designing masonry and retaining walls using Lotus's Symphony.

General Services Administration -
Information Resources Service Center.

Data: 202-535-8054 300 bps
Data: 202-535-7661 1200 bps

GSA's Information Resources Service Center provides information on contracts, schedules, policies, and programs. One of the areas that is interesting was the weekly supplement to the consolidated list of debarred, suspended and ineligible contractors.

Budget and Finance Board of the Office of Immigration Naturalization Service.

DO NOT CALL THIS BBS DURING WORKING HOURS.

Sysop: Mike Arnold
Data: 202-787-3460 300/1200/2400

The system is devoted to the exchange of information related to budget and financial management in the federal government. It is a 'working' system for the Immigration and Naturalization Service personnel.

Naval Aviation News Computer Information (NANei) -
Supported by: Naval Aviation News Magazine, Bldg. 159E, Navy Yard Annex, Washington, DC 20374.

Sysop: Commander Howard Wheeler
Voice: 202-475-4407
Data: 202-475-1973 300/1200

Available from 5 pm to 8 am. weekdays 5pm Friday to 8 am Monday

This is a large BBS with lots of Navy related information and programs. NANci is for those interested in stories, facts, and historical information related to Naval Aviation.

Federal National Mortgage Association -

Sysop: Ken Goosens
Data: 202-537-7475
202-537-7945 300/1200

This BBS is in transition. Ken Gossens will be running a new BBS at 703-979-6360. The BBS maybe become a closed board under the new sysop. This BBS has/had one of largest collections of files for downloading.

The World Bank, Information, Technology and Facilities Department, Office System Division, Washington DC.

Sysop: Ashok Daswani
Voice: 202-473-2237
Data: 202-676-0920 300/1200

Basically a software exchange BBS, but has other information about the use of microcomputers and software supported by World Bank. IBM product announcements also kept up to date.

National Oceanic Atmospheric Administration (NOAA), National Meteorological Center.

* You must obtain a password from the SYSOP to log on to this BBS.

Sysop: Vernon Patterson
Voice: 301-763-8071
Data: 301-899-0825 300 bps
301-899-0830 1200 bps

This is one of the most useful databases available on-line. With it you can access meteorological data collected form 6000 locations throughout the world. It can also display crude, but useful graphic maps of the US illustration temperatures, precipitation and forecasts.

National Weather Service, US Dept. of Commerce, East Coast Marine Users BBS

* You must obtain a p/w from the SYSOP to logon this BBS.

Sysop: Ross Laporte
Voice: 301-899-3296
Data: 301-454-8700 300bps

Use this BBS to obtain info about marine weather and nautical info about coastal waterways including topical storm advisories.

NARDAC, Navy Regional Data Automation Center, Norfolk, VA. 23511-6497

Sysop: Jerry Dew
Voice: 804-445-4298
Data: 804-445-1627 300 & 1200 bps

A basic Utilitarian system developed to support the informational needs of NARDAC. The Dept. of Defense mag., CHIPS is available in the files section of this BBS. There are also Navy and IBM related articles to read.

Veterans Administration, Info Technology Bulletin Board.

Data: 202-376-2184 300/1200 bps

The content of this BBS ranges from job opening listings to information computer security.

Dept. of Energy, Office of Civilian Radioactive Waste Management, Infolink.

Sysop: Bruce Birnbaum
Voice: 202-586-9707
Data: 202-586-9359 300/1200 bps

This BBS has press leases, fact sheets, backgrounders, congressional questions, answers, speeches & testimony, from the Office of Civilian Radioactive Waste Management.

I skipped listing a few of the BBSes in this article if the chances were slim to get on or if the BBS got a bad review. Most of the ones listed seemed

to have lot of informative files for downloading and viewing pleasure. This article carried a very strong word of warning about tampering/crashing these since they are run by the govt. and a volunteer Sysop. Since you can get on these legally why not use it?

The Sorceress

% = % = % = % = % = % = % = %
= =
% P h r a c k X V I I %
= =
% = % = % = % = % = % = % = %

Phrack Seventeen
07 April 1988

File 8 of 12 : Dialback Modem Security

In article <906@hoptoad.uucp> gnu@hoptoad.UUCP writes:
>Here are the two messages I have archived on the subject...

>[I believe the definitive article in that discussion was by Lauren Weinstein,
>vortex!lauren; perhaps he has a copy.

What follows is the original article that started the discussion. I do not know whether it qualifies as the "definitive article" as I think I remember Lauren and I both posted further comments.

- Dave

** ARTICLE FOLLOWS **

An increasingly popular technique for protecting dial-in ports from the ravages of hackers and other more sinister system penetrators is dial back operation wherein a legitimate user initiates a call to the system he desires to connect with, types in his user ID and perhaps a password, disconnects and waits for the system to call him back at a prearranged number. It is assumed that a penetrator will not be able to specify the dial back number (which is carefully protected), and so even if he is able to guess a user-name/password pair he cannot penetrate the system because he cannot do anything meaningful except type in a user-name and password when he is connected to the system. If he has a correct pair it is assumed the worst that could happen is a spurious call to some legitimate user which will do no harm and might even result in a security investigation.

Many installations depend on dial-back operation of modems for their principle protection against penetration via their dial up ports on the incorrect presumption that there is no way a penetrator could get connected to the modem on the call back call unless he was able to tap directly into the line being called back. Alas, this assumption is not always true - compromises in the design of modems and the telephone network unfortunately make it all too possible for a clever penetrator to get connected to the call back call and fool the modem into thinking that it had in fact dialed the legitimate user.

The problem areas are as follows:

Caller control central offices

Many older telephone central office switches implement caller control in which the release of the connection from a calling telephone to a called telephone is exclusively controlled by the originating telephone. This means that if the penetrator simply failed to hang up a call to a modem on such a central office after he typed the legitimate user's user-name and password, the modem would be unable to hang up the connection.

Almost all modems would simply go on-hook in this situation and not notice that the connection had not been broken. If the same line was used to dial out on as the call came in on, when the modem went to dial out to call the legitimate user back the it might not notice (there is no standard way of doing so electrically) that the penetrator was still connected on the line. This means that the modem might attempt to dial and then wait for an

answerback tone from the far end modem. If the penetrator was kind enough to supply the answerback tone from his modem after he heard the system modem dial, he could make a connection and penetrate the system. Of course some modems incorporate dial tone detectors and ringback detectors and in fact wait for dial tone before dialing, and ringback after dialing but fooling those with a recording of dial tone (or a dial tone generator chip) should pose little problem.

Trying to call out on a ringing line

Some modems are dumb enough to pick up a ringing line and attempt to make a call out on it. This fact could be used by a system penetrator to break dial back security even on joint control or called party control central offices. A penetrator would merely have to dial in on the dial-out line (which would work even if it was a separate line as long as the penetrator was able to obtain it's number), just as the modem was about to dial out. The same technique of waiting for dialing to complete and then supplying answerback tone could be used - and of course the same technique of supplying dial tone to a modem which waited for it would work here too.

Calling the dial-out line would work especially well in cases where the software controlling the modem either disabled auto-answer during the period between dial-in and dial-back (and thus allowed the line to ring with no action being taken) or allowed the modem to answer the line (auto-answer enabled) and paid no attention to whether the line was already connected when it tried to dial out on it.

The ring window

However, even carefully written software can be fooled by the ring window problem. Many central offices actually will connect an incoming call to a line if the line goes off hook just as the call comes in without first having put the 20 hz. ringing voltage on the line to make it ring. The ring voltage in many telephone central offices is supplied asynchronously every 6 seconds to every line on which there is an incoming call that has not been answered, so if an incoming call reaches a line just an instant after the end of the ring period and the line clairvoyantly responds by going off hook it may never see any ring voltage.

This means that a modem that picks up the line to dial out just as our penetrator dials in may not see any ring voltage and may therefore have no way of knowing that it is connected to an incoming call rather than the call originating circuitry of the switch. And even if the switch always rings before connecting an incoming call, most modems have a window just as they are going off hook to originate a call when they will ignore transients (such as ringing voltage) on the assumption that they originate from the going-off-hook process. [The author is aware that some central offices reverse battery (the polarity of the voltage on the line) in the answer condition to distinguish it from the originate condition, but as this is by no means universal few if any modems take advantage of the information supplied]

In Summary

It is thus impossible to say with any certainty that when a modem goes off hook and tries to dial out on a line which can accept incoming calls it really is connected to the switch and actually making an outgoing call. And because it is relatively easy for a system penetrator to fool the tone detecting circuitry in a modem into believing that it is seeing dial tone, ringback and so forth until he supplies answerback tone and connects and penetrates system security should not depend on this sort of dial-back.

Some Recommendations

Dial back using the same line used to dial in is not very secure and

cannot be made completely secure with conventional modems. Use of dithered (random) time delays between dial in and dial back combined with allowing the modem to answer during the wait period (with provisions made for recognizing the fact that this wasn't the originated call - perhaps by checking to see if the modem is in originate or answer mode) will substantially reduce this window of vulnerability but nothing can completely eliminate it.

Obviously if one happens to be connected to an older caller control switch, using the same line for dial in and dial out isn't secure at all. It is easy to experimentally determine this, so it ought to be possible to avoid such situations.

Dial back using a separate line (or line and modem) for dialing out is much better, provided that either the dial out line is sterile (not readily traceable by a penetrator to the target system) or that it is a one way line that cannot accept incoming calls at all. Unfortunately the later technique is far superior to the former in most organizations as concealing the telephone number of dial out lines for long periods involves considerable risk. The author has not tried to order a dial out only telephone line, so he is unaware of what special charges might be made for this service or even if it is available.

A final word of warning

In years past it was possible to access telephone company test and verification trunks in some areas of the country by using mf tones from so called "blue boxes". These test trunks connect to special ports on telephone switches that allow a test connection to be made to a line that doesn't disconnect when the line hangs up. These test connections could be used to fool a dial out modem, even one on a dial out only line (since the telephone company needs a way to test it, they usually supply test connections to it even if the customer can't receive calls).

Access to verification and test ports and trunks has been tightened (they are a kind of dial-a-wiretap so it ought to be pretty difficult) but in any as in any system there is always the danger that someone, through stupidity or ignorance if not mendacity will allow a system penetrator access to one.

** Some more recent comments **

Since posting this I have had several people suggest use of PBX lines that can dial out but not be dialed into or outward WATS lines that also cannot be dialed. Several people have also suggested use of call forwarding to forward incoming calls on the dial out line to the security office. [This may not work too well in areas served by certain ESS's which ring the number from which calls are being forwarded once anyway in case someone forgot to cancel forwarding. Forwarding is also subject to being cancelled at random times by central office software reboots]

And since posting this I actually tried making some measurements of how wide the incoming call window is for the modems we use for dial in at CRDS. It appears to be at least 2-3 seconds for US Robotics Courier 2400 baud modems. I found I could defeat same-line-for-dial-out dialback quite handily in a few dozen tries no matter what tricks I played with timing and watching modem status in the dial back login software. I eventually concluded that short of reprogramming the micro in the modem to be smarter about monitoring line state, there was little I could do at the login (getty) level to provide much security for same line dialback.

Since it usually took a few tries to break in, it is possible to provide some slight security improvement by sharply limiting the number of unsuccessful callbacks per user per day so that a hacker with only a couple of passwords would have to try over a significant period of time.

Note that dialback on a dedicated dial-out only line is somewhat secure.

David I. Emery Charles River Data Systems 617-626-1102
983 Concord St., Framingham, MA 01701.
uucp: decvax!frog!die

--

David I. Emery Charles River Data Systems
983 Concord St., Framingham, MA 01701 (617) 626-1102 uucp: decvax!frog!die

% = % = % = % = % = % = % = %
= =
% P h r a c k X V I I %
= =
% = % = % = % = % = % = %

Phrack Seventeen
07 April 1988

File 9 of 12 : Data-Tapping Made Easy

--FEATURE ARTICLES AND REVIEWS-

TAPPING COMPUTER DATA IS EASY, AND CLEARER THAN PHONE CALLS !

BY RIC BLACKMON, SYSOP OF A FED BBS

Aquired by Elric of Imrryr & Lunatic Labs UnLtd

Note from Elric: This file was written by the sysop of a board for computer security people (run on a CoCo), as far as I know the board no longer exists, it was being crashed by hackers too much... (hehe).

FOR SEVERAL YEARS, I ACCEPTED CERTAIN BITS OF MISINFORMATION AS TECHNICALLY ACCURATE, AND DIDN'T PROPERLY PURSUE THE MATTER. SEVERAL FOOLS GAVE ME FOOLISH INFORMATION, SUCH AS: A TAP INTERRUPTS COMPUTER DATA TRANSMISSIONS; DATA COULD BE PICKED UP AS RF EMANATIONS BUT IT WAS A MASS OF UNINTELLIGIBLE SIGNAL CAUSED BY DATA MOVING BETWEEN REGISTERS; ONE HAD TO BE IN 'SYNC' WITH ANY SENDING COMPUTER; DATA COULDN'T BE READ UNLESS YOU HAD A DIRECT MATCH IN SPEED, PARITY & BIT PATTERN; AND ONLY A COMPUTER OF THE SAME MAKE AND MODEL COULD READ THE SENDING COMPUTER. THIS IS ALL PLAIN SWILL. IT IS IN FACT, AN EASIER CHORE TO TAP A COMPUTER THAN A TELEPHONE. THE TECHNIQUE AND THE EQUIPMENT IS ALMOST THE SAME, BUT THE COMPUTER LINE WILL BE MORE ACCURATE (THE TWO COMPUTERS INVOLVED, HAVE ERROR CORRECTING PROCEDURES) AND CLEARER (DIGITAL TRANSMISSIONS HAVE MORE DISTINCT SIGNALS THAN ANALOG TRANSMISSIONS).

FIRST, RECOGNIZE THAT NEARLY ALL DATA TRANSMISSIONS ARE SENT IN CLEARTEXT ASCII SIGNALS. THE LINES CARRYING OTHER BIT-GROUPS OR ENCIPHERED TEXTS ARE RARE. SECOND, THE SIGNAL APPEARS ON GREEN AND RED (WIRES) OF THE PHONE LINE ('TIP' AND 'RING'). THE DATA IS MOST LIKELY ASYNCHRONOUS SERIAL DATA MOVING AT 300 BAUD. NOW THAT 1200 BAUD IS BECOMING MORE CHIC, YOU CAN EXPECT TO FIND A GROWING USE OF THE FASTER TRANSMISSION RATE. FINALLY, YOU DON'T NEED TO WORRY ABOUT THE PROTOCOL OR EVEN THE BAUD RATE (SPEED) UNTIL AFTER A TAPED COPY OF A TRANSMISSION IS OBTAINED.

IN A SIMPLE EXPERIMENT, A TAPED COPY OF A DATA TRANSMISSION WAS MADE WITH THE CHEAPEST OF TAPE RECORDERS, TAPPING THE GREEN AND RED LINES BEYOND THE MODEM. THE RECORDING WAS THEN PLAYED INTO A MODEM AS THOUGH IT WERE AN ORIGINAL TRANSMISSION. AT THAT POINT, HAD IT BEEN NECESSARY, THE PROTOCOL SETTINGS ON RECEIVING TERMINAL COULD HAVE BEEN CHANGED TO MATCH THE TAPE. NO ADJUSTMENTS WERE NECESSARY AND A NICE, CLEAR ERROR-FREE DOCUMENT WAS RECEIVED ON THE ILLICIT VIDEO SCREEN AND A NEAT HARD-COPY OF THE DOCUMENT CAME OFF THE PRINTER. THE MESSAGE WAS INDEED CAPTURED, BUT HAD IT BEEN AN INTERCEPTION INSTEAD OF A SIMPLE MONITORING, IT COULD HAVE BEEN ALTERED WITH A SIMPLE WORD PROCESSOR PROGRAM, TO SUIT ANY PURPOSE, AND PLACED BACK ON THE WIRE.

WERE I TO HAVE AN INTEREST IN INFORMATION ORIGINATING FROM A PARTICULAR COMPANY, AGENCY, OR OFFICE, I THINK THAT I WOULD FIND IT FAR MORE PRODUCTIVE TO TAP A DATA TRANSMISSION THAN TO TAP A VOICE TRANSMISSION, AND EVEN MORE REWARDING THAN GETTING HARDCOPY DOCUMENTS.

*SIGNIFICANT & IMPORTANT INFORMATION IS MORE CONCENTRATED IN A DATA TRANSMISSION.
*SIGNIFICANT & IMPORTANT INFORMATION IS MORE EASILY LOCATED IN DATA

TRANSMISSIONS THAN IN MASSES OF FILES OR PHONE CALLS.
*TRANSMITTED DATA IS PRESUMED TRUE, AND WHEN ALTERATION IS DISCOVERED, IT'S READILY BLAMED ON THE EQUIPMENT.\024
*THE LAWS CONCERNING TAPS ON UNCLASSIFIED AND NON-FINANCIAL COMPUTER DATA ARE EITHER QUITE LACKING OR ABJECTLY STUPID.

THE POINT OF ALL THIS IS THAT THE PRUDENT MANAGER REALLY OUGHT TO ENCRYPT ALL DATA TRANSMISSIONS. ENCRYPTION PACKAGES ARE CHEAP (A 'DES' PROGRAM IS NOW PRICED AT $30) AND ARE EASY TO USE.

PHRACK PRESENTS ISSUE 17

^*^*^*^ Phrack World News, Part 1 ^*^*^*^

**** File 10 of 12 ****

- P H R A C K W O R L D N E W S -

(Mainly Compiled By Sir Francis Drake)

2/1/88

BUST UPDATE

==========

All the people busted by the Secret Service last July were contacted in September and asked if they "wanted to talk." No one but Solid State heard from the S.S. after this. Solid State was prosecuted and got one year probation plus some required community service. The rest: Ninja NYC, Bill >From RNOC, Oryan QUEST, etc. are still waiting to hear. Some rumors have gone around that Oryan QUEST has cooperated extensively with the feds but I have no idea about the validity of this. The following is a short interview with Oryan QUEST. Remember that QUEST has a habit of lying.

PHRACK: Did you hear from the SS in September? It seems everybody else has.

QUEST: No. I haven't heard from them since I was busted. Maybe they forgot me.

P: What's your lawyer think of your case?

Q: He says lay low. He says it's no problem because of my age.

P: What do your parents think?

Q: They were REALLY pissed for about a week but then they relaxed. I mean I think my parents knew I went through enough... I mean I felt like shit.

P: Do you plan to keep involved in Telecom legit or otherwise?

Q: Uhh, I wanna call boards... I mean I can understand why a sysop wouldn't give me an access but... I'm thinking of putting a board up, a secure board just to stay in touch ya know? Cause I had a lot of fun I mean I just don't want to get busted again.

P: Any further words of wisdom?

Q: No matter what anyone says I'm *ELITE*. NOOOO don't put that.

P: Yes I am.

Q: No I don't want people to think I'm a dick.

P: Well...

Q: You're a dick.

- On a completely different note, Taran King who as some of you know was busted, is going to be writing a file for Phrack about what happened real soon now.

MEDIA

=====

The big media thing has been scare stories about computer viruses,

culminating in a one page Newsweek article written by good old Sandza and friends. John Markoff of the San Francisco Examiner wrote articles on viruses, hacking voice mailboxes, and one that should come out soon about the July Busts (centering on Oryan QUEST). A small scoop: He may be leaving for the New York Times or the San Jose Mercury.

Phreak media wise things have been going downhill. Besides PHRACK (which had a bad period but hopefully we're back for good) there is 2600, and Syndicate Report. Syndicate Report is dead, although their voice mail system is up. Sometimes. 2600 has gone from a monthly magazine to a quarterly one because they were losing so much money. One dead and 2 wounded.

MISCELLANEOUS

Taran King and Knight Lightning are having a fun time in their fraternity at University of Missouri. Their respective GPA's are 2.1 and 2.7 approximately.... Phantom Phreaker and Doom Prophet are in a (punk/metal) band... Lex Luthor is alive and writing long articles for 2600... Sir Francis Drake sold out and wrote phreak articles for Thrasher... Jester Sluggo has become vaguely active again...

CONCLUSION

Less and less people are phreaking, the world is in sorry shape, and I'm going to bed. Hail Eris.

sfd

PHRACK PRESENTS ISSUE 17

^*^*^*^ Phrack World News, Part 2 ^*^*^*^

**** File 11 of 12 ****

"Illegal Hacker Crackdown"
from the California Computer News - October 1987
Article by Al Simmons - CCN Editor

Hackers beware!

Phone security authorities, the local police, and the Secret Service have been closing down on illegal hacking - electronic thievery - that is costing the long-distance communications companies and their customers millions of dollars annually. In the U.S., the loss tally on computer fraud, of all kinds, is now running between $3 billion and $5 a year, according to government sources.

"San Francisco D.A. Gets First Adult Conviction for Hacking"
(After about 18 years, it's a about time!)

San Francisco, District Attorney Arlo Smith recently announced the first criminal conviction in San Francisco Superior Court involving an adult computer hacker.

In a report released August 31, the San Francisco District Attorney's office named defendant Steve Cseh, 25, of San Francisco as having pled guilty earlier that month to a felony of "obtaining telephone services with fraudulent intent" (phreaking) by means of a computer.

Cseh was sentenced by Superior Court Judge Laurence Kay to three years probation and ordered to preform 120 hours of community service.

Judge Kay reduced the offense to a misdemeanor in light of Cseh's making full restitution to U.S. Sprint - the victim phone company.

At the insistence of the prosecuting attorney, however, the Court ordered Cseh to turn his computer and modem over to U.S. Sprint to help defray the phone company's costs in detecting the defendant's thefts. (That's like big money there!)

A team of investigators from U.S. Sprint and Pac Tel (the gestapo) worked for weeks earlier this year to detect the hacking activity and trace it to Cseh's phone line, D.A. Arlo Smith said.

The case centered around the use of a computer and its software to illegally acquire a number of their registered users to make long-distance calls.

Cseh's calls were monitored for a three-week period last March. After tracing the activity to Cseh's phone line, phone company security people (gestapo stormtroopers) were able to obtain legal authority, under a federal phone communications statute, to monitor the origin and duration of the illegal calls.

Subsequently, the investigators along with Inspector George Walsh of the San Francisco Police Dept. Fraud Detail obtained a search warrant of Cseh's residence. Computer equipment, a software dialing program, and notebooks filled with codes and phone numbers were among the evidence seized, according to Asst. D.A. Jerry Coleman who prosecuted the case.

U.S Sprint had initially reported more than $300,000 in losses from the use of their codes during the past two years; however, the investigation efforts could only prove specific losses of a lesser amount traceable to Cseh during the three-week monitoring period.

"It is probable that other computer users had access to the hacked Sprint codes throughout the country due to dissemination on illegal computer bulletin

boards," added Coleman (When where BBS's made illegal Mr. Coleman?)

"Sacramento Investigators Breakup Tahoe Electronic Thefts"

Meanwhile, at South Shore Lake Tahoe, Secret Service and phone company investigators arrested Thomas Gould Alvord, closing down an electronic theft ring estimated to have rung up more than $2 million in unauthorized calls.

A Sacramento Bee story, filed by the Bee staff writers Ted Bell and Jim Lewis, reported that Alvord, 37, was arrested September 9, on five felony counts of computer hacking of long-distance access codes to five private telephone companies.

Alvord is said to have used an automatic dialer, with computer programmed dialing formulas, enabling him to find long-distance credit card numbers used by clients of private telephone companies, according to an affidavit filed in Sacramento's District Court.

The affidavit, filed by William S. Granger, a special agent of the Secret Service, identified Paula Hayes, an investigator for Tel-America of Salt Lake City, as the undercover agent who finally brought an end to Alvord's South Shore Electronic Co. illegal hacking operation. Hayes worked undercover to purchase access codes from Alvord.

Agent Garanger's affidavit lists U.S. Sprint losses at $340,000 but Sprint spokesman Jenay Cottrell said that figure "could grow considerably," according to the Bee report.

One stock brokerage firm, is reported to have seen its monthly Pacific Bell telephone bill climb steadily from $3,000 in April to $72,000 in August. The long-distance access codes of the firm were among those traced to Alvord's telephones, according to investigators the Bee said.

Alvord was reportedly hacking access codes from Sprint, Pacific Bell, and other companies and was selling them to truck drivers for $60 a month. Alvord charged companies making overseas calls and larger businesses between $120 and $300 a month for the long-distance services of his South Shore Electronics Co.

>From The $muggler

PHRACK PRESENTS ISSUE 17

^*^*^*^ Phrack World News, Part 3 ^*^*^*^

**** File 12 of 12 ****

+---+
-[PHRACK XVII]---

"The Code Crackers are Cheating Ma Bell"
Typed by the Sorceress from the San Francisco Chronicle
Edited by the $muggler

The Far Side.....(415)471-1138
Underground Communications, Inc.....(415)770-0140

+---+

In California prisons, inmates use "the code" to make free telephone calls lining up everything from gun running jobs to visits from grandma.

In a college dormitory in Tennessee, students use the code to open up a long-distance line on a pay phone for 12 straight hours of free calls.

In a phone booth somewhere in the Midwest, a mobster uses the code to make untraceable calls that bring a shipment of narcotics from South America to the United States.

The code is actually millions of different personal identification numbers assigned by the nation's telephone companies. Fraudulent use of those codes is now a nationwide epidemic that is costing America's phone companies more than $500 million each year.

In the end, most of that cost is passed on to consumers, in the form of higher phone rates, analysts say.

The security codes range form multidigit access codes used by customers of the many alternative long-distance companies to the "calling card" numbers assigned by America Telephone & Telegraph and the 22 local phone companies, such as Pacific Bell.

Most of the loss comes form the activities of computer hackers, said Rene Dunn, speaking for U.S. Sprint, the third-largest long-distance company.

These technical experts - frequently bright, if socially reclusive, teenagers - set up their computers to dial the local access telephone number of one of the alternative long-distance firms, such as MCI and U.S. Sprint. When the phone answers, a legitimate customer would normally punch in a secret personal code, usually five digits, that allows him to make his call.

Hackers, however, have devised computer programs that will keep firing combinations of numbers until it hits the right combination, much like a safecracker waiting for the telltale sound of pins and tumblers meshing.

Then the hacker- known in the industry as a "cracker" because he has cracked the code- has full access to that customer's phone line.

The customer does not realize what has happened until a huge phone bill arrives at the end of the month. By that time, his access number and personal code have been tacked up on thousands of electronic bulletin boards throughout the country, accessible to anyone with a computer, a telephone and a modem, the device that allows the computer to communicate over telephone lines.

"This is definitely a major problem," said one telephone security expert, who declined to be identified. "I've seen one account with a $98,000 monthly bill."

One Berkeley man has battled the telephone cheats since last fall, when his

MCI bill showed about $100 in long-distance calls he had not made.

Although MCI assured him that the problem would be taken care of, the man's latest bill was 11 pages long and has $563.40 worth of long-distance calls. Those calls include:

[] A two-hour call to Hyattsville, Maryland, on January 22. A woman who answered the Hyattsville phone said she had no idea who called her house.

[] Repeated calls to a dormitory telephone at UCLA. The student who answered the phone there said she did not know who spent 39 minutes talking to her, or her roommate, shortly after midnight on January 23.

[] Calls to dormitory rooms at Washington State University in Pullman and to the University of Colorado in Boulder. Men who answered the phones there professed ignorance of who had called them or of any stolen long-distance codes.

The Berkeley customer, who asked not to be identified, said he reached his frustration limit and canceled his MCI account.

The phone companies are pursing the hackers and other thieves with methods that try to keep up with a technological monster that is linked by trillions of miles of telephone lines.

The companies sometimes monitor customers' phone bills. If a bill that averages about $40 or $50 a month suddenly soars to several hundred dollars with calls apparently placed from all over the country on the same day, the phone company flags the bill and tries to track the source of the calls.

The FBI makes its own surveillance sweeps of electronic bulletin boards, looking for stolen code numbers. The phone companies occasionally call up these boards and post messages, warning that arrest warrants will be coming soon if the fraudulent practice does not stop. Reputable bulletin boards post their own warnings to telephone hackers, telling them to stay out.

Several criminal prosecutions are already in the works, said Jocelyne Calia, the manager of toll fraud for U.S. Sprint.

If the detectives do not want to talk about their methods, the underground is equally circumspect. "If they (the companies) have effective (prevention) methods, how come all this is still going on?" asked one computer expert, a veteran hacker who says he went legitimate about 10 years ago.

The computer expert, who identified himself only as Dr. Strange, said he was part of the original group of electronic wizards of the early 1970s who devised the "blue boxes" complex instruments that emulate the tones of a telephone and allowed these early hackers to break into the toll-free 800 system and call all over the world free of charge.

The new hacker bedeviling the phone companies are simply the result of the "technology changing to one of computers, instead of blue boxes" Dr. Strange said. As the "phone company elevates the odds... the bigger a challenge it becomes," he said.

A feeling of ambivalence toward the huge and largely anonymous phone companies makes it easier for many people to rationalize their cheating. A woman in a Southwestern state who obtained an authorization code from her boyfriend said, through an intermediary, that she never really thought of telephone fraud as a "moral issue." "I don't abuse it," the woman said of her newfound telephone privilege. "I don't use it for long periods of time - I never talk for more than an hour at a time - and I don't give it out to friends." Besides, she said, the bills for calls she has been making all over the United States for the past six weeks go to a "large corporation that I was dissatisfied with. It's not as if an individual is getting the bills."

There is one place, however, where the phone companies maybe have the upper hand in their constant war with the hackers and cheats.

In some prisons, said an MCI spokesman, "we've found we can use peer pressure. Let's say we restrict access to the phones, or even take them out, and there were a lot of prisoners who weren't abusing the phone system. So the word gets spread to those guys about which prisoner it was that caused the telephones to get taken out. Once you get the identification (of the phone-abusing prisoner) out there, I don't think you have to worry much" the spokesman said. "There's a justice system in the prisons, too."