```
                  .-------------------------------------.
                  ---   U H C A`s Technical Journal     -
                  ---                                   -
                  ---        By Digital Phreak          -
                  ---                                   -
                  ---         a.k.a FoneFreak           -
                  ---                                   -
                  ---       Issue Number # two          -
                  `-------------------------------------'

.--------------------------[ WARNING ]--------------------------.
|!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!|
`---[ NO PHONES OR COMPUTERS WHERE HARMED IN THIS PRODUCTION ]---'
    `-----------------------------------------------------------'
```



```
          .-----------------------------------------.
        -[Ok, i think thats enough topics for this issue]-
          `-----------------------------------------'
```

.-[**U H C A**]----------[**0.1**]-.
| **-[Introduction]-** |
`-------------------------'

Ok, this issue will rock your nuts. Really it just kicks ass. After doing a shit load of research on this stuff, i desided to put it all together and call it a e/zine type thing. Issue three will (maybe) be out March 1st. If you want to help, type up something about computers or phones and send it to Digital_Freak@hotmail.com. You will get full credit for your work. Also, if anyone wants to host this zine, please contact me at Digital_Freak@hotmail.com, and tell me.

That is all
-Digital Phreak

.----------[**1.2**]-.|
-[NEWS]- |
`-------------'

A new version of the tool Hunt has been released. Version 1.2 is the first version which is capable of successfully spoofing hosts on switched ports. This means that Level 2 ethernet switches don't protect you against sniffing or hijacking unless they are carefully configured with security in mind.

2.3 -[ATM Routing Fabric]-

The ATM Routing Fabric is primarily responsible for routing cells among the different cards in the DSLAM. These cells may contain user data, operations and maintenance (OAM), performance monitoring (PM), signaling, and intra-DSLAM proprietary cells.

There are many different architectures which can realize this routing function. One of the most popular is the bus-based method, which is often implemented using custom-designed ASICs coupled with memories. This approach, therefore, enables designers to add differentiating features to their product.

Another way to realize the bus-based architecture is to utilize the UTOPIA interface available on many ATM components, such as Motorola's MC92501 ATM Cell Processor. Although the UTOPIA interface was not specifically developed with this application in mind, it may be a cost-effective way to implement bus interconnect, with some slight modifications to support point-to-multipoint requirements.

3.4 -[Digital Subscriber Line Access Multiplexer]-

A**symmetrical **D**igital **S**ubscriber **L**ine **(ADSL) technology uses existing twisted-pair copper plant to potentially offer subscribers broadband services such as high-speed internet access, LAN nterconnect for telecommuters, and video-on-demand.

A**synchronous **T**ransfer **M**ode **(ATM) supports multi-media service delivery, and supports specific Quality of Service (QoS) guarantees for the various kinds of data traffic.

The DSLAM is a network element (NE) that has been defined to support high-bandwidth applications at the edge of the public network. With the ability to support data and voice services over existing subscriber lines, the DSLAM can help RBOCs and ISPs minimize the cost and maximize the efficiency of their networks.

On the subscriber side, the DSLAM supports the transmission of both voice and data over the existing twisted-pair copper infrastructure with the use of ADSL transceivers. On the public network, or CO, side, the DSLAM separates the voice from the data, and routes these services onto separate networks optimized to support them. Data services supported with the DSLAM NE include, but are not limited to, internet access, remote workstation LAN/WAN access, frame relay and native ATM.

The remainder of this section examines the ATM-based DSLAM architecture in greater detail and suggests Motorola products that apply to this application. For the sake of simplicity, the voice support through the DSLAM will not be addressed.

The requirements of the DSLAM remain somewhat vague, but continue to solidify as companies generate their marketing requirement documents, which are then reviewed by the RBOCs and ISPs. Some requirements of the ATM-based solution are already understood:

The interface between the DSLAM and the ATM network will be OC-12, OC-3 or DS3. If DS3 is used, it should be field upgradable to an OC-12 or OC-3.

The interface between the DSLAM and the ATM network will be compliant with the ATM Forum UNI 3.1 specification, with the exception that the GFC field shall be allocated to the VPI subfield.

The DSLAM should support statistical multiplexing, traffic management, cell buffering, cell queuing, priority schemes and fairness algorithms i accordance to the ATM Forum TM 4.0 specification.

On the surface, these requirements suggest that the DSLAM is a small ATM switch; however, some debate continues as to how much intelligence is imbedded in this type of NE. From a hardware perspective, the DSLAM and ATM edge switch are very similar.

In general, the DSLAM Network Element (NE) is comprised of a single card cage (called a shelf) populated with severa types of cards. Of course, several shelves can b e grouped together into a rack to construct a larger DSLAM.

.--[**4.5**]-.
| **-[Transmitting Digital Signals]-** |
`---'

[Intro]
`-------'

Transmission rules! It's the way a signal gets from one place to another. FDM, TDMA, CDMA, and sending information Don't confuse PCS with the way it sends information. Wireless systems use frequency division multiplex (FDM), time division multiple access (TDMA), or code division multiple access (CDMA) to send information. Those techniques by themselves, however, aren't operating systems. They are part of one. None stnds by themselves.

A TDMA scheme first digitizes and then combines or multiplexes several conversations into one digital stream on a single frequency. CDMA, on the other hand, assigns a unique code to each bit of information, transmitting these little pieces over a broader frequency range. But whatever transport mechanism used, it takes a larger operating system to make the whole thing work. Got it? So when someone says, "Is PCS TDMA?" they usually mean, or should mean, "Is PCS TDMA based?"

Okay, now we know a little about digitizing. Going digital by itself, though, as we've seen, isn't the most important thing.
A multiplexed digital signal is what is key. That's combining several signals together to save space or radio bandwidth. Ordinarily a single call takes up an entire frequency.

In conventional cellular or AMPS that's 30Khz. But what if you run out of room? What if you have more customers in a cell than the frequencies to handle them? Well, you better start multiplexing, at least the voice traffic. In IS-54, otherwise known as D-AMPS, or digital AMPS, that's exactly what happens. It puts three callers on the same frequency, tripling a carrier's system's capacity. The principle D-AMPS uses is TDMA.

Frequency Division Multiplexing Its useful to review an analog technique before getting into a digital discussion

Time Division Multiple Access Time division multiple access or TDMA divides each cellular channel into three time slots. That increases the amount of calls that can be carried. GSM, D-AMPS, and D-AMPS 1900 (IS-136), and Motorola's iDEN all use or can use TDMA. This scheme assigns a specific time slot, a regular space in a digital stream, for each call's use during the call. Think of a not so drunken cocktail party, wih each person speaking one at a time. Everyone gets to speak over time, much as in TDMA. Let's try another analogy.

Think of a circus carousel and three groups of kids waiting for a ride. The horses represent a time slot. Let's say there are eight horses on the carousel. Each group of kids gets told to jump on a different colored horse when it comes around. One group rides a red horse, one rides a white one and the other one rides a black horse. They ride the carousel until they get off at a designated point. Now, if our kids were orderly, you'd see three lines of children descending on the carousel with one line of kids moving away. In the case of TDMA, one revolution of the ride might represent one frame. This precisely synchronized system keeps everyone's call in order. This synchronization continues throughout the call, with timing information in every frame of every call. As another writer puts it:

"Effectively, the IS-54 and IS-136 implementations of TDMA immediately tripled the capacity of cellular frequencies by dividing a 30-kHz channel into three time slots, enabling three different users to occupy it at the same time. Currently, systems are in place that allow six times capacity. In the future, with the utilization of hierarchical cells, intelligent antennas, and adaptive channel allocation, the capacity should approach 40 times analog capacity. 40 times analog capacity! That's quite a hope. David Crowe says Imagine 3 mobiles. 1 right at the cellsite, 1 at 10km distance and 1 at 100 km distance. The base station has to transmit to the three mobiles in sequence, and the messages will arrive at three different times. The response will make it even worse. Now, the base station can tell the far mobiles to back off, but this will degrade voice quality (the 'satellite' phenomenon). I think this is what keeps TDMA systems down to the less than 10 km cellsite radius. Analog obviously has no such limitation. CDMA might not have a time limitation, but it has similar problems with power.

[Code division multiple access]
`------------------------------'

AMPS DISCUSSION FOLLOWS -- TO BE REWRITTEN FOR DIGITAL
Without getting ahead of ourselves, I should say something about digital vulnerability. One might think an operating system could be as separated from its radio system, that is, an AMPS system should provide similar coverage to PCS1900, GSM or the mostly digital D-AMPS1900. That's given the same frequency assignments, power, topography, number of base stations, and so on. But for many reasons all digital systems are less robust than analog. In an AMPS system, for example, one can understand and speak through heavy static, since the mind is so forgiving of errors. A digital transcever, however, will drop the same call under those conditions since the data stream contains so many errors. It's like picking up the phone when someone is on line. Keep the phone off too long and you trash the communication link. Thus, all digital systems tend to have more base stations, smaller cell sites, and drop more calls.

Another problem is distance. TDMA systems They attempt to compensate for the distance that a mobile is from the cellsite, but it isn't possible to eliminate the distortions.

[CDMA]
`------'

But CDMA is nevertheless moving toward U.S. dominance. According to market-research firm Dataquest Inc., the technology accounted for 31% of the nation's 12.9 million digital-phone subscribers as of September, up from 21% a year earlier. "By 2002, CDMA should easily have over 50% of the total," says Matt Hoffman, a Dataquest analyst. Internationally, however, CDMA lags far behind a standard called GSM, which is similar to TDMA.

[Channel Names and Functions]
`----------------------------'

FDM. Don't panic! It's a complicated phrase for a simple idea. First things first. Voice trans-mission uses the voice fre-quency or *VF channel* to carry a conversation on a twisted pair. You'll also hear terms like pass band, base band, voice channel and voice path. Whatever. This channel sets up naturally in a wire when you start talking, roughly from 300 to 3,000 hertz. (By compari-son, middle C on a piano is about 261 hertz, a piccolo 4,186 Hz and a door squeak 16,000Hz.) This voice channel remains as the first channel of two on split carrier. Transmitting a ra-dio frequency or *carrier frequency* on the wire at, say, a constant 100 kilohertz or one hundred thou-sand cycles per second creates the second channel. (By comparison, the AM radio band be-gins at 540 kilohertz.) Sending the sec-ond call is easy. The sec-ond conversation gets im-pressed on the steady carrier fre-quency of 100 kilo-hertz. This causes the carrier signal to move up and down or *modulate* ac-cording to changes in speech. It's simi-lar to how conversation varies the elec-trical current in a normal telephone line.

.---[**5.6**]-.
| **-[Personal Communications Services (PCS)]-** |
`---'

In the United States personal communication systems or PCS means products or services using the Federal Communication Commission's two designated PCS radio bands. Equipment like multi-purpose phones, advanced pagers, "portable facsimile and other imaging devices, new types of multi-function cordless phones, and advanced devices with two-way data capabilities." By regulation the FCC says PCS are "Radio communications that encompass mobile and ancillary fixed communication that provide services to individuals and businesses and can be integrated with a variety of competing networks." In other words, just about any high tech wireless gadget or service imaginable. PCS includes many present wireless services, too, like conventional cellular, modified for the higher, newly allotted PCS frequencies. An example is AT&T's PCS offering, "Pure Digital PCS, more precisely known as IS-136. It's the foundation for their digital one rate plan. Outside the United States, and sometimes even within, defining PCS further gets tricky. Mobility Canada says they "don't believe that PCS can be defined as a technology, a radio spectrum, or a market. It is whatever the wireless communications customer wants it to be." Perhaps. But their quote reminds me of Humpty Dumpty's exhortation that "When I use a word, it means just what I choose it to mean -- neither more nor less." Calling something PCS is now sexy and it implies that your technology, however old and dusty it may be compared to the competition, is actually happening and cutting edge. AT&T, in fact, deliberately planned to "blur the distinction between cellular and PCS" when they called their cellular service PCS. Please look over this table to see the names wireless offerings go by today.

No matter the definition, a PCS system shares many things with cellular. A network of base stations, arranged in a cell like fashion around a large area ensures coverage and easy roaming. Calls must be registered and then validated for billing. But not all PCS systems are created equal and a higher radio frequency assignment doesn't make any service special. For example, GSM in Europe operates around the 900 Mhz band but its features

aren't frequency dependent. It can also operate around 1900 MHz where it does in most of North America.

[The two basic types or divisions]
`---------------------------------'

Two PCS types exist: narrowband and broadband. PCS narrowband uses 900 megahertz (MHz) frequencies for many advanced paging services. Broadband uses 2 gigahertz (GHz) frequencies for voice, data, and video services. In general broadband PCS systems use higher frequencies, lower power, smaller cells and more of them, than conventional cellular at 800 MHz. That reflects the spectrum's properties: higher frequency waves are smaller, travel less distance than low frequency signals, and thus need more base stations spaced more closely together. Base station requirements are, in fact, 50% to 100% more than 800 MHz cellular.These characteristics, in turn, reflect the main problem with PCS systems: lack of coverage! Until PCS networks are completely built out in America, conventional cellular service will continue to lead in coverage and lack of dropped calls.

[The five main PCS systems]
`--------------------------'

David Crowe of the outstanding Cellular Networking Perspectives says five PCS systems exist, along with a smaller, more different group of three. By way of explanation, 'upband' means a wireless service operating at a higher frequency than it normally does.

PCS1900 Upbanded GSM cellular

TIA IS-136 Upbanded TDMA digital cellular

TIA IS-95 Upbanded CDMA digital cellular

TIA IS-88 Upbanded NAMPS narrowband analog cellular

TIA IS-91 Upbanded Plain old analog cellular

As anyone can see, the major players are all existing cellular radio systems put at higher frequencies. And since they are all cellular, it makes sense to discuss them below in the cellular discussion. We'll see there what differences exist between
Since I can't afford TIA documents (who can?) I rely on patent searching and the patient help of a few telecom experts TDMA
Ericsson says that, "There are more than 90 million subscribers using TDMA/AMPS networks in morethan 100 countries worldwide. Nearly 18 million of these subscribers are already using TDMA (IS-136) digital services. TDMA (IS-136) already delivers
over 85 percent of the IMT-2000 functionality and is being further enhanced to deliver all IMT-2000 capabilities in the existing 800 and 1900 MHz frequency bands and in the new 2 GHz band.

[CDMA]
`------'

Jeffry Bartash reported on January 21, 1999 for CBS MarketWatch that Sprint sold US $500 million dollars of stock "to expand Sprint's wireless service, whose number of new customers more than doubled to 830,000 in the fourth quarter from the previous quarter, the company said. For the year, Sprint PCS added 1.7 million customers and now has more than 2.58 million. In the fourth quarter of 1998, Sprint spent nearly $700 million building its network, which now encompasses more than half the U.S. population."

[The three lessor]

`------------------'

J-STD-014 PACS Bellcore WACS and Japan's PHS
TIA IS-661 Omnipoint composite CDMA/TDMA
TIA IS-665 OKI/Interdigital Wideband CDMA
TIA IS-661

Omnipoint uses GSM almost exclusively, as well as, supposedly, a proprietary scheme called TIA IS-661. Omipoint said on Luly 13, 1995 that IS-661 "was developed "specifically for the challenges of the new PCS marketplace, unlike other PCS standards which were originally designed to add capacity to analog cellular systems." A publicity wonk named Smith prattled "The primary benefits of IS-661 include greatly reduced infrastructure costs and deployment time,wireline quality voice, and high speed data and digitized video capability." Sounds good to me. But there hasn't been much written about it since then, at least on the web, although Ericsson and Nortel signed on early as development partners. So what the heck is it? August 18, 1997, Omnipoint Chairman George Schmitt said: Attention is now focused on Omnipoint's IS-661 technology, which was developed by the manufacturing side of Omnipoint Corp. The GSM overlay is intended to boost bandwidth and data rates on the network by tapping into unlicensed frequencies to allow the carrier to diversify its offerings. "What I expect to happen next is sometime late this year, we'll demo wireless
local loop in New York, then find out if we can make a business case of it," Schmitt says. "Assuming we can make some fashion of IS-661 a viable business in New York, we intend to roll it out wherever it makes sense." Meyers, Jason. To the point Telephony, Aug 18, 1997,30-32. Language: English. Pub type: Company Profile
[Abstract] [Long Display] Copyright Intertec Publishing Corp 1997

The PCS 1900 and Omnipoint radio technologies can coexist within a single 30 MHz allocation. Therefore, within the context of a PCS 1900 operator's business interests, there are choices as to how best to maximize the revenue opportunity of acquiring new spectrum. Fixed Wireless Access The system can provide an alternative local loop system with comparable voice quality and the ability to support common telephony devices in use today. Wireless and Wireline Integration Allows the mobile handset to become a virtual extension on the existing PBX or centrex system. Subscribers have the same business features and services as those available on their existing system when they are at their
normal business location.

TIA IS-136 looks like an elemental cellular system, employing three standard cells throughout a wide area. The original patent calls it a "Three-cell wireless communication system. Such physical simplicity may indeed reduce cost, although at the expense of a more complicated operating system.

This is where Omnipoint will launch its PCS services based on a combination of Ericsson's GSM-derived PCS 1900 technology and the operator's own patented IS-661 transmission standard. A wireless communication system including a repeated pattern of cells, in which base station transmitters and user station transmitters for each cell may be assigned a spread-spectrum code for modulating radio signal communication in that cell. Radio signals used in that cell are spread across a bandwidth sufficiently wide that both base station receivers and user station receivers in an adjacent cell may distinguish communication which originates in one cell from another. Adjacent cells may use distinguishable frequencies and distinguishable codes, but it is sufficient if adjacent cells use distinguishable frequencies and identical codes. A repeated pattern of cells allows the codes each to be reused in a plurality of cells.

A time division multiple access wireless communication system, comprising

- a repeated pattern of three cells, each cell having a base station; and
- a user station;
- wherein said base station and said user station communicate using time division multiple access;
- wherein transmitters in a first cell are assigned a first spread-spectrum code for modulating radio communication in said first cell;
- whereby radio signals used in said first cell are spread across a bandwidth sufficiently wide that receivers in a second cell, said second cell being adjacent to said first cell, may distinguish communication which originates in said first cell from communication which originates in said second cell; and
- whereby said first spread-spectrum code is reused in a plurality of cells such that said first cell in said pattern using said first spread-spectrum code is not adjacent to any other cell using said first spread-spectrum code.

[Cellular]
`----------'

GSM (Global System for Mobile Communications): Like iDEN, the European Cellular Standard utilizes TDMA technology, dividing a 200 kHz channel into 8 time slots. Each GSM time slot is the
size of one undivided 25 kHz iDEN Channel. Analog phone service in North America is called AMPS. That stands for Advanced Mobile Phone Service, a technology AT&T pioneered back in the late 1970s and early 1980s. It's conventional cellular service. XXXXXXX
AMPS (Advanced Mobile Phone System): Analog Cellular represents the majority of cellular phone systems in the United States. AMPS provides one voice conversation per channel and does not offer
multiple services like GSM, USDC, and iDEN. USDC (United States Digital Cellular): USDC utilizes TDMA to offer phone and paging service over a 25 kHz channel divided into two time slots.
iDEN is the only fully integrated digital wireless network. A 25 kHz channel can be divided up to six times providing dispatch, interconnect phone, data, and text messaging in a seamless
communications package.

.----------[**6.7**]-.
| **-[Digital wireless history]-** |
`----------'

[Intro]
`-------'

In the future the landline telephone system and wireless communications may act alike with no difference in services or quality. We're not there yet but progress gets made every day. Coming soon are wireless phones that double as a home cordless and a regular mobile. Video and fast data transfer over wireless might be next. Let's look at the past, though, before we speculate on the future. We'll see why so many wireless solutions

exist in North America, and why a unifed digital standard will be very difficult to achieve.

Firstly, AMPS systems aren't completely analog like most people think. They're analog *and* digital. Voice traffic is analog as well as signaling tones, audio markers that put a mobile on frequency and keep it there. AMPS nessaging is mostly digital, though, like the signaling that identifies a mobile, identifies a base station, assigns a cell frequency, pages a mobile, and so forth. Those are data bursts. A mobile, for example, sends its identifying electronic serial number or ESN, using a 32 bit code. 0s and 1s. Let's call AMPS systems first generation instead of analog, since they pioneered cellular.

[The First systems]

In 1978 Advanced Mobile Phone Service or AMPS started operating in North America. In that year, in AT&T labs in Newark, New Jersey, and most importantly in a beta trial in Chicago, Illinois Bell and AT&T jointly rolled out analog based cellular telephone service. Ten cells covering 21,000 square miles made up the Chicago system. It operated in the newly allocated 800 MHz band. This early network, using large scale integrated circuits throughout, a dedicated computer and switching system, custom made mobile telephones and antennas, proved that cellular could work. worldwide AMPS deployment followed quickly. A two cell system started operating in Bahrain, Saudi Arabia in May, 1978, an 88 cell system in Tokyo in December, 1979, and the first North American system in Mexico City, a one cell affair, in August, 1981. United States cellular development didn't keep up. The Bell System's impending breakup and a new FCC competition requirement delayed its rollout. The Federal Communication Commission's 1981 regulations required the Bell System or a regional operating company, such as Bell Atlantic, to have competition in every cellular market. That's unlike the landline monopoly those companies had. The theory being that competition would provide better service and keep prices low.

Ameritech began providing the first United States commercial service in Chicago, consequently, on October 12, 1983. United States cellular service developed from this AT&T model, along with Motorola's analog system known as Dyna-TAC or TACS, first introduced commercially in Baltimore and Washington D.C. by Cellular One on December 16, 1983. Canadian AMPS service got going when Alberta Government Telephones, now Telus , launched the AURORA-400 system in February, 1983, using GTE and NovAtel equipment. This so called decentralized system operates at 420 MHZ, using 86 cells but featuring no handoffs. As David Crowe explains, "It provides much better rural coverage, although its capacity is low."

Europe saw cellular service introduced in 1981, when the Nordic Mobile Telephone System or NMT450 began operating in Denmark, Sweden, Finland, and Norway in the 450 MHz range. In 1985 Great Britain started using theTotal Access Communications System or TACS at 900 MHz. Later, the West German C-Netz, the French Radiocom 2000 <http://www.ericsson.com.au/Connexion/connexion1-95/market.html>, and the Italian RTMI/RTMS helped make up Europe's nine analog incompatible radio telephone systems. Plans were afoot during the early 1980s, however, to create a single European wide digital mobile service with advanced features and easy roaming. While North American groups concentrated on building out their robust but increasingly fraud plagued and featureless analog network, Europe planned for a digital future.

The United States, by comparison, suffered no welter of incompatible systems. Roaming from one city or state to another wasn't difficult like Europe. Your telephone usually worked as long as there was coverage. Little desire existed, therefore, to design an all digital system when the present one was working well and proving popular. To illustrate that point, the

American cellular phone industry grew from less than 204,000 subscribers in 1985, to 1,600,000 in 1988 <http://www.wow-com.com/images/view_98datasurvey3.gif>. And with each analog based phone sold, chances dimmed for an all digital future. To keep those phones working (and producing money for the carriers) any technological system advance would have to accommodate them.

Europeans saw things differently because of their needs and a clearly focused vision. No new telephone system could work with so many existing services on so many frequencies. They decided, therefore, to start a new technology in a new radio band. Cellular structured but fully digital, the new service would incorporate the best thinking of the time. They patterned their new wireless standard after landline requirements for ISDN, hoping to make a wireless counterpart to it. The new service was called GSM. GSM first stood for Groupe Speciale Mobile, after the study group that created the standard. It's now known as Global System for Mobile Communications, although the "C" isn't included in the abbreviation. GSM development began in 1982 by a group of 26 European national phone companies.

This Conference of European Postal and Telecommunications Administrations or CEPT, sought to build a uniform, European wide cellular system around 900 MHz. A rare triumph of European unity, GSM achievements became "one of the most convincing demonstrations of what co-operation throughout European industry can achieve on the global market." Planning began in earnest and contnued for several years. In 1989 The European Telecommunication Standards Institute or ETSI took responsibility for further developing GSM. In 1990 the first recommendations were published. Pre-dating American PCS, the United Kingdom asked for and got a GSM plan for higher frequencies. The Digital Cellular System or DCS1800 works at 1.8 GHz, uses lower powered base staions and has greater capacity because more frequencies are available than on the continent. Aside from these "air interface" considerations, the system is pure GSM. The specs were published in 1991.

The late 1980s saw North American cellular becoming standardized. In 1988 the analog cellular standard called TIA-IS-41 was published. [Crowe]This interim standard let manufacturers and cellular carriers develop equipment and practices that worked better together. Building and modifying cellular networks became easier, even if agreeing on standards did not. IS-41 continues to be revised 10 years later. And unfortunately for full digital working, two years passed before the trade decided how to develop cellular further. [Levine]The result? More digital but not completely digital. In March, 1990, IS-54B or D-AMPS (Digital AMPS) became the first North American dual mode digital cellular standard. This protocol saved bandwidth by digitizing and multiplexing voice traffic.

It kept, however, analog AMPS' routines to first set up calls. Using IS-54, a cellular carrier could convert any of its system's analog voice channels to digital. A dual mode phone then used digital channels where available and defaulted to regular AMPS where it was not. CANTEL got IS-54 going in Canada in 1992.At this time I should point out that no radio service can be judged on whether it is all digital or not. PCS 1900, for example, the American GSM equivalent, operates at a higher frequency than it does in most of Europe. As we will see later, nearly twice as many base stations are required as on the continent, leaving gaps and holes in coverage that do not exist with lower frequency, conventional cellular. And data transfer remains no higher than 9.6 kbs, a fifth the speed of an ordinary landline modem.

So there is tremendous potential but until the network is built out and other problems solved, that potential remains unfulfilled. By the beginning of 1995, there were 60 countries with operational or planned GSM networks in Europe, the Middle East, the Far East, Australia, Africa, and South

America, with a total of over 5.4 million subscribers. . ."Commercial GSM networks started operating in mid-1991 in European countries. GSM developed later than conventional cellular, therefore, and in many respects was better designed. IS-54 did increase call capacity for cellular carriers and it did not leave behind any customers. Certain channels could be converted to digital while leaving others analog. By 1993 American cellular was running out of room. the American cellular business continued with tremendous growth. Subscribers rose from when we last checked in, 1988, with 1 and a half million customers, to more than 13 million subscribers in 1993. Customers numbered, Many carriers were at their system capacity in densely populated cities The FCC began auctioning space in the PCS band, from December 5, 1994 to January. 14, 1997 By 1994In the darker side of cellular, the Cellular Telecommunication Associaton began pushing federal legislation to outlaw cloning and scanning radios that could tune in the cellular band, to prevent by law what their industry failed to do themselves.

Years behind the fraud curve compared to GSM, the CTIA worked with the Secret Service to create a posionous anti-cloning and anti-hacker hysteria. Fueling their self-made flames by ridicously inflated loss numbers, the CTIA became a shadow arm of federal law enforcement, striking out at cloners rather than immediately implementing authentication to prevent cloning, or creating low price companion plans to satisfy the demand for second phones, or mild encryption to prevent easy eavesdropping. GSM, by comparison, easily caried out authentication and encryption. GSM phones have never been cloned in the field, using over the air techniques. Rather than admitting that authenticating phone lack of authentication doomed American cellular companies to fraud and lack of encrypted voice traffic made snooping easy with over the counter radio scanners. As of October, 1998, GSM's popularity remains unrivaled. Consider these points:

- 100 million subscribers
- 5 million new users each month
- 120 countries served
- 300 GSM system operators worldwide
- 60% of all digital mobiles produced are GSM

Moving toward a fully digital, completely intergrated wireless   system will allow digital working from end to end, the holy grail of telephony.

[References]
`------------'

Gibson, Stephen W. Cellular Mobile Radiotelephones. Englewood Cliffs, NJ: Prentice-Hall, 1987. 18. Now historical and of little current import, Gibson's text remains a good state of the art report on North American cellular circa 1987.

.---[**7.8**]-.
| **-[L0pht Security Advisory]-** |
`---'

```
    Release date:  February 18, 1999
     Application:  Microsoft Windows NT 4.0
        Severity:  any local user can gain administator privileges
                   and/or take full control over the system

          Author:  dildog@l0pht.com
             URL:  http://www.L0pht.com/advisories.html
---
Overview :
---
```

Microsoft Windows NT 4.0 implements a system-wide cache of
file-mapping objects for the purpose of loading system dynamic link
libraries (DLLs) as quickly as possible. These cache objects, located in
the system's internal object namespace, are created with permissions such
that the 'Everyone' group has full control over them. Hence, it is possible
to delete these cache objects and replace them with others that point to
different DLLs.

When processes are created, the loader maps/loads the loading
executable's imported DLLs into the process space. If there is a DLL cache
object available, it is simply mapped into the process space, rather than
going to the disk. Hence, there is an exploitable condition, when a low-
privilege user replaces a DLL in the cache with a trojan DLL, followed by a
high-privelege account launching a process. The high priveleged process
will map in the trojan DLL and execute code on behalf of the low privelege
use r.

Affected systems:

Windows NT 4.0 Server SP4
Windows NT 4.0 Workstation SP4

Other service packs are likely to be vulnerable, but the exploit has not
been tested on them, neither has the fix presented below.

Description :

The Windows NT object namespace is the place where the kernel
keeps the names of mutexes, semaphores, filemapping objects, and other
kernel objects. It is organized hierarchically, like a directory structure.
Amongst the directories are:

\Device
\BaseNamedObjects
\Driver
\KnownDlls

...

The NT object namespace is browsable with a tool called 'WinObj
2.0' from System Internals (their website is http://www.sysinternals.com).
You may wish to look around this namespace and browse the default
permissions of objects. It is quiet entertaining, really.
The "\Knowndlls" directory contains a list of DLLs in the
c:\winnt\system32 directory, like:

\KnownDlls\COMCTL32.dll
\KnownDlls\MPR.dll
\KnownDlls\advapi32.dll
\KnownDlls\kernel32.dll

All of these objects are created at boot time, and are 'permanent
shared objects'. Normally, users can not create permanent shared objects
(it's an advanced user right, and it is normally not assigned to any group,
even Administrators). But the system pr eloads this cache for you.
Permanent shared objects differ from regular shared objects only in the
fact that they have a flag set, and an incremented reference count, such
that if you create one, and then terminate the creating process or close
all handle s to the object, it does not disappear from the object space.

To exploit the poor permissions on this cache, one first needs to delete one of the shared objects by name, in order to later replace it. So we make a call to the NTDLL.DLL native function "OpenSection()", getting a handle to the object. Then we call the

NTOSKRNL.EXE native function "ZwMakeTemporaryObject()" which removes the 'permanent' flag and decrements the reference counter from the object. Now we just call NTDLL.DLL:NtClose() on the handle and it is destroyed.

To create a section, one calls NTDLL.DLL:CreateSection(), which is undocumented. There are other calls one needs to make in order to set up the object and open the KnownDlls directory, but they are trivial and will not be discussed here. Feel free to bro wse the source code presented at the end of this advisory to see what you need to do though. Anyway, you create a section (aka file-mapping) object that points to a trojan DLL. A good candidate for DLL trojan is KERNEL32.DLL, since it is loaded by pretty much every executable you're going to run.

Note that any DLL cache objects you create as a user can not be 'permanent', hence, when you log out, the cache object _will_ disappear. So how can we get a higher privelege process to run while we're logged in? There are many ways. We can wait for an 'A t' job to go off, or we can set up the DLL hack as an 'At' job that goes off when someone else is logged in. But more reliable is this:

When a new Windows NT subsystem is started, it creates a subsystem process to handle various system details. Examples of these processes are LSASS.EXE and PSXSS.EXE. The PSXSS.EXE is the POSIX subsystem. But since no one ever really uses the POSIX subsys tem under NT. So, chances are, it won't be loaded into memory yet. Once it is, though, it's loaded until the machine reboots. If it loaded, reboot the machine, and it won't be :P.

So, we launch our DLL cache hack, and then run a POSIX subsystem command, thus launching PSXSS.EXE (which runs as 'NT AUTHORITY\SYSTEM', the system account), and running our DLL with local administrator privileges. Incidentally, other subsystems have the
same effect, such as the OS/2 subsystem (the only other one that probably isn't started yet).

Workarounds/Fixes:

I developed a patch for this security problem in the form of a Win32 Service program that can be installed by the Administrator of the system. It sets itself to run every time the system is started, and before the user has the opportunity to start a program, it adjusts the permissions of the DLL cache to something much safer. The source code for this service is also provided, along with a compiled version. Links to the programs can be found at http://www.l0pht.com/advisories.html. One can verify the validity of the patch by downloading the WinObj v2.0 tool from System Internals (www.sysinternals.com) and inspecting the permissions of the KnownDlls directory, and the section objects within it. Microsoft has been sent a copy of this advisory, and I would expect a hotfix from them at some point in the near future.

Example :

I wrote up a trojan to test exploitability, and it was a simple 'forwarder' DLL that had the same exported names as KERNEL32.DLL, but a different 'DllMain()' function, to be called when the DLL is loaded. The

function calls in my trojan, simply forward o ff to the real KERNEL32.DLL calls located in a copy of the kernel that you make in 'REALKERN.DLL' in the c:\temp directory.

To try out this vulnerability, obtain an account as a low-privilege guest user (referred to as 'Dick') and do the following:

1. Log in as Dick at the console.

2. Start up two "cmd.exe" shells. Do the following in one of them.

3. Copy c:\winnt\system32\kernel32.dll to c:\temp\realkern.dll
(The egg dll is hard coded to use the c:\temp directory to find this file. If you can't put it in c:\temp, then modify the source '.def' file to point to a different location and recompile eggdll.dll)

4. Copy the provided hackdll.exe and eggdll.dll to c:\temp

5. Ensure that there is no file named c:\lockout. If there is, delete it. The exploit uses this file as a lockfile.

6. Delete the KERNEL32.DLL file-mapping object from the system cache:
```
c:\> cd\temp
c:\temp> hackdll -d kernel32.dll
```

7. Insert the new file-mapping object with:
```
c:\temp> hackdll -a kernel32.dll c:\temp\eggdll.dll
```
Don't hit a key in this window after hitting enter.

8. Now move to the other cmd.exe window that you started.

9. Run a POSIX subsystem command. A good way to start it is:
```
c:\temp> posix /c calc
```

10. Now the EGGDLL.DLL will prompt you with a few message boxes:
Say no to the "User is DOMAIN\DICK, Spawn Shell?" box.
Say no to the "User is \[garbage], Spawn Shell?" box.
Say YES to the "User is NT AUTHORITY\SYSTEM, Spawn Shell?" box.
Say YES to the "Winsta0" window station message box.
Say YES to the "Desktop" window desktop message box.
You will now see a "System Console" command.com shell open up.
saying yes to the next 'winlogon' box will give you something funny when you log out, btw :P)

11. Now go back to your first cmd.exe window and hit a key to unpoison the DLL cache.

12. In the System Console window, run the User Manager program, and modify Dick's account or anyone else's for that matter) to your hearts content.

```
NT Server) c:\winnt\system32> usrmgr
NT Workstation) c:\winnt\system32> musrmgr
```

Source and Compiled Code:

Exploit code can be downloaded from L0pht's website at http://www.l0pht.com/advisories.html. It is available in compiled form, and in pure source form as two zipfiles. The L0pht patch for this advisory is also available in both source form and compiled f orm from the same URL.

[dildog@l0pht.com]
,----------------------------------
For more L0pht (that's L - zero - P - H - T) advisories check out:
http://www.l0pht.com/advisories.html
`----------------------------------

.--[**8.9**]-.
| Digital`s Projects: |
`--'

  Operation Infowar- This is a project to get a UNIX box for my
  fucking windows infected school. And bring fourth a new
  anti windows revlution (spelling)

  Project TINY- This is a top secret project yada yada yada
  takeing out goverment communications and so on...

  I am working on a highly top secret project thing
  called uhh uhmmm Operation Thingy. It will
  be inafect by March 1st. Its prupose:

  Take out all T3 routers in the US. Aww CRAP!
  i am thinking out loud aggian!

  More projects comming soon.

`--'
 Digital`s   Home   Advertiseing   Thing
.--.

   .-----------------------------------ITS BEEN 4 FUCKING YEARS.
.=/ FREE KEVIN \==.
| If you do not know who Kevin Mitnick is |
| then vist www.kevinmitnick.com or www.2600.com |
|------------Support 2600.com and the Free Kevin----------------|
|--------------defense fund site, visit it now!-----------------|
`-----------------F--R--E--E---K--E--V--I--N--------------------'
                     \ Fight the system! /
                      `-----------------'

.-[#Phone-Knowledge]---.
[#Phone-Knowledge   ]
[Come to #Phone-Knowledge for a great learning source.   ]
[--]
[We Have disscussions on everthing phone related, and   ]
[i am planing on setting up a GSM dissucssion on the 1st of   ]
[Marh 1999.   ]
[--]
[Channel Stats:]
[Server: Undernet   ]
[Ops: FoneFreak, Random APB.   ]
[Number of people: 5-10   ]
`------------------------------[ Digital Phreak`s own channel]-'

  .-------T H E---H A C K E R---N E W S---N E T W O R K--------.
 ------   ------
----   For up-to-date hacking news, visit the Hacker   ----
----   News Network at http://www.hackernews.com   ----

.----------[**9.0**]-.
| **-[Overview Of the GSM System]-** |
`----------'

Architecture of the GSM network

The GSM technical specifications define the different entities that form the GSM network by defining their functions and interface requirements. The GSM network can be divided into four main parts:

- The Mobile Station (MS).
- The Base Station Subsystem (BSS).
- The Network and Switching Subsystem (NSS).
- The Operation and Support Subsystem (OSS).

Mobile Station

A Mobile Station consists of two main elements:

- The mobile equipment or terminal.
- The Subscriber Identity Module (SIM).

The Terminal

There are different types of terminals distinguished principally by their power and application:

- The `fixed' terminals are the ones installed in cars. Their maximum allowed output power is 20 W.
- The GSM portable terminals can also be installed in vehicles. Their maximum allowed output power is 8W.
- The handhels terminals have experienced the biggest success thanks to thei weight and volume, which are continuously decreasing. These terminals can emit up to 2 W. The evolution of technologies allows to decrease the maximum allowed power to 0.8 W.

The SIM

The SIM is a smart card that identifies the terminal. By inserting the SIM card into the terminal, the user can have access to all the subscribed services. Without the SIM card, the terminal is not operational.

The SIM card is protected by a four-digit Personal Identification Number (PIN). In order to identify the subscriber to the system, the SIM card contains some parameters of the user such as its International Mobile Subscriber Identity (IMSI).
Another advantage of the SIM card is the mobility of the users. In fact, the only element that personalizes a terminal is the SIM card. Therefore, the user can have access to its subscribed services in any terminal using its SIM card.

The Base Station Subsystem

The BSS connects the Mobile Station and the NSS. It is in charge of the transmission and reception. The BSS can be divided into two parts:

- The Base Transceiver Station (BTS) or Base Station.

•The Base Station Controller (BSC).

The Base Transceiver Station

The BTS corresponds to the transceivers and antennas used in each cell of the network. A BTS is usually placed in the center of a cell. Its transmitting power defines the size of a cell. Each BTS has between one and sixteen transceivers depending on the density of users in the cell.

The Base Station Controller

The BSC controls a group of BTS and manages their radio ressources. A BSC is principally in charge of handovers, frequency hopping, exchange functions and control of the radio frequency power levels of the BTSs.

The Network and Switching Subsystem

Its main role is to manage the communications between the mobile users and other users, such as mobile users, ISDN users, fixed telephony users, etc. It also includes data bases needed in order to store information about the subscribers and to manage their mobility. The different components of the NSS are described below.

The Mobile services Switching Center (MSC)

It is the central component of the NSS. The MSC performs the switching functions of the network. It also provides connection to other networks.

The Gateway Mobile services Switching Center (GMSC)

A gateway is a node interconnecting two networks. The GMSC is the interface between the mobile cellular network and the PSTN. It is in charge of routing calls from the fixed network towards a GSM user. The GMSC is often implemented in the same machines as the MSC.

Home Location Register (HLR)

The HLR is considered as a very important database that stores information of the suscribers belonging to the covering area of a MSC. It also stores the current location of these subscribers and the services to which they have access. The location of the subscriber corresponds to the SS7 address of the Visitor Location Register (VLR) associated to the terminal.

Visitor Location Register (VLR)

The VLR contains information from a subscriber's HLR necessary in order to provide the subscribed services to visiting users. When a subscriber enters the covering area of a new MSC, the VLR associated to this MSC will request information about the new subscriber to its corresponding HLR. The VLR will then have enough information in order to assure the subscribed services without needing to ask the HLR each time a communication is established. The VLR is always implemented together with a MSC; so the area under control of the MSC is also the area under control of the VLR.

The Authentication Center (AuC)

The AuC register is used for security purposes. It provides the parameters needed for authentication and encryption functions. These parameters help to verify the user's identity.

The Equipment Identity Register (EIR)

The EIR is also used for security purposes. It is a register containing information about the mobile equipments. More particularly, it contains a

list of all valid terminals. A terminal is identified by its International Mobile Equipment Identity (IMEI). The EIR allows then to forbid calls from stolen or unauthorized terminals (e.g, a terminal which does not respect the specifications concerning the output RF power).

The GSM Interworking Unit (GIWU)

The GIWU corresponds to an interface to various networks for data communications. During these communications, the transmission of speech and data can be alternated.

The Operation and Support Subsystem (OSS)

The OSS is connected to the different components of the NSS and to the BSC, in order to control and monitor the GSM system. It is also in charge of controlling the traffic load of the BSS.
However, the increasing number of base stations, due to the development of cellular radio networks, has provoked that some of the maintenance tasks are transfered to the BTS. This transfer decreases considerably the costs of the maintenance of the system.

The geographical areas of the GSM network

As it has already been explained a cell, identified by its Cell Global Identity number (CGI), corresponds to the radio coverage of a base transceiver station. A Location Area (LA), identified by its Location Area Identity (LAI) number, is a group of cells served by a single MSC/VLR. A group of location areas under the control of the same MSC/VLR defines the MSC/VLR area. A Public Land Mobile Network (PLMN) is the area served by one network operator.

The GSM functions

In this paragraph, the description of the GSM network is focused on the differents functions to fulfil by the network and not on its physical components. In GSM, five main functions can be defined:

- Transmission.
- Radio Resources management (RR).
- Mobility Management (MM).
- Communication Management (CM).
- Operation, Administration and Maintenance (OAM).

Transmission

The transmission function includes two sub-functions:
- The first one is related to the means needed for the transmission of user information.
- The second one is related to the means needed for the trasnmission of signaling information. Not all the components of the GSM network are strongly related with the transmission functions. The MS, the BTS and the BSC, among others, are deeply concerned with transmission. But other components, such as the registers HLR, VLR or EIR, are only concerned with the transmission for their signaling needs with other components of the GSM network. Some of the most important aspects of the transmission are described in section 5.

Radio Resources management (RR)

The role of the RR function is to establish, maintain and release communication links between mobile stations and the MSC. The elements that are mainly concerned with the RR function are the mobile station and the base station. However, as the RR function is also in charge of maintaining a connection even if the user moves from one cell to another, the MSC, in

charge of handovers, is also concerned with the RR functions. The RR is also esponsible for the management of the frequency spectrum and the reaction of the network to changing radio environment conditions. Some of the main RR procedures that assure its responsabilities are:

- Channel assignment, change and release.
- Handover.
- Frequency hopping.
- Power-level control.
- Discontinuous transmission and reception.
- Timing advance.

Some of these procedures are described in section 5. In this paragraph only the handover, which represents one of the most important responsabilities of the RR, is described.

Handover

The user movements can produce the need to change the channel or cell, specially when the quality of the communication is decreasing. This procedure of changing the resources is called handover. Four different types of handovers can be distinguished:

- Handover of channels in the same cell.
- Handover of cells controlled by the same BSC.
- Handover of cells belonging to the same MSC but controlled by different BSCs.
- Handover of cells controlled by different MSCs.
- Handovers are mainly controlled by the MSC. However in order to avoid unnecessary signalling information, the first two types of handovers are managed by the concerned BSC (in this case, the MSC is only notified of the handover).

The mobile station is the active participant in this procedure. In order to perform the handover, the mobile station controls continuously its own signal strengh and the signal strengh of the neighboring cells. The list of cells that must be monitored by the mobile station is given by the base station. The power measurements allow to decide which is the best cell in order to maintain the quality of the communication link. Two basic algorithms are used for the handover:

- The `minimum acceptable performance' algorithm. When the quality of the transmission decreases (i.e the signal is deteriorated), the power level of the mbbile is increased. This is done until the increase of the power level has no effect on the quality of the signal. When this happens, a handover is performed.
- The `power budget' algorithm. This algorithm performs a handover, instead of continuously increasing the power level, in order to obtain a good communication quality.

Mobility Management

The MM function is in charge of all the aspects related with the mobility of the user, specially the location management and the authentication and security.

Location management

Then a mobile station is powered on, it performs a location update procedure by indicating its IMSI to the network. The first location update procedure is called the IMSI attach procedure.
The mobile station also performs location updating, in order to indicate its current location, when it moves to a new Location Area or a different PLMN. This location updating message is sent to the new MSC/VLR, which

gives the location information to the subscriber's HLR. If the mobile station is authorized in the new MSC/VLR, the subscriber's HLR cancells the registration of the mobile station with the old MSC/VLR. A location updating is also performed periodically. If after the updating time period, the mobile station has not registered, it is then deregistered. When a mobile station is powered off, it performs an IMSI detach procedure in order to tell the network that it is no longer connected.

Authentication and security

The authentication procedure involves the SIM card and the Authentication Center. A secret key, stored in the SIM card and the AuC, and a ciphering algorithm called A3 are used in order to verify the authenticity of the user. The mobile station and the AuC compute a SRES using the secret key, the algorithm A3 and a random number generated by the AuC. If the two computed SRES are the same, the subscriber is authenticated. The different services to which the subscriber has access are also checked. Another security procedure is to check the equipment identity. If the IMEI number of the mobile is authorized in the EIR, the mobile station is allowed to connect the network. In order to assure user confidentiality, the user is registered with a Temporary Mobile Subscriber Identity (TMSI) after its first location update procedure. Enciphering is another option to guarantee a very strong security but this procedure is going to be described in section 5.

Communication Management (CM)

The CM function is responsible for:
- Call control.
- Supplementary Services management.
- Short Message Services management.

Call Control (CC)

The CC is responsible for call establishing, maintaining and releasing as well as for selecting the type of service. One of the most important functions of the CC is the call routing. In order to reach a mobile subscriber, a user diales the Mobile Subscriber ISDN (MSISDN) number which includes:

- a country code
- a national destination code identifying the subscriber's operator
- a code corresponding to the subscriber's HLR

The call is then passsed to the GMSC (if the call is originated from a fixed network) which knows the HLR corresponding to a certain MISDN number. The GMSC asks the HLR for information helping to the call routing. The HLR requests this information from the subscriber's current VLR. This VLR allocates temporarily a Mobile Station Roaming Number (MSRN) for the call. The MSRN number is the information returned by the HLR to the GMSC. Thanks to the MSRN number, the call is routed to subscriber's current MSC/VLR. In the subscriber's current LA, the mobile is paged.

Supplementary Services management

The mobile station and the HLR are the only components of the GSM network involved with this function. The different Supplementary Services (SS) to which the users have access are presented in section 6.3.

Short Message Services management

In order to support these services, a GSM network is in contact with a Short Message Service Center through the two following interfaces:

•The SMS-GMSC for Mobile Terminating Short Messages (SMS-MT/PP). It has the same role as the GMSC.
•The SMS-IWMSC for Mobile Originating Short Messages (SMS-MO/PP).

Operation, Administration and Maintenance (OAM)

The OAM function allows the operator to monitor and control the system as well as to modify the configuration of the elements of the system. Not only the OSS is part of the OAM, also the BSS and NSS participate in its functions as it is shown in the following examples:

•The components of the BSS and NSS provide the operator with all the information it needs. This information is then passed to the OSS which is in charge of analize it and control the network.
•The self test tasks, usually incorporated in the components of the BSS and NSS, also contribute to the OAM functions.
•The BSC, in charge of controlling several BTSs, is another example of an OAM function performed outside the OSS.

```
.-----------------------------------------------------[ 9.1 ]-. |Work
Cited: And Greets:                                             |
`--------------------------------------------------------------'
|--------\-------------\Books]                                  |
|WEB SITES\-----\        \An introduction to GSM                |
|www.l0pht.com  |         \The GSM System                       |
|www.iec.org    |          \Mobile Radio Communications         |
|---------------'           \Telecommunications Engineering     |
`--------------------------------------------------------------'
                 .-----------------------------.
               -[Greets: Yea thats right GREETS!]-
                 `-----------------------------'
```

-The FBI : Why are you always in that pizza van outside my house?

-The SS : aCk! Where? Hey you guys don`t seem so secret to me!

-Random APB : Hey, thanks for suporting my E/Zine!

-Mind Plug : Hey where are you? Did the Canada police get you?

-Sector : :(Sorry you cant read this because you are locked away but i will try to mail you this issue. Who am i talking to, i just said he was locked away! I hope you do good and don`t drop the soap. There i go agian!

-Beer : Yumm, You guys make my day much better

-Linus : I just have to think this guy for makeing Linux, what would i have done with out it? Used windows!?! aCk!!!

-The L0pht : Well you guys have to be some of the savvist computer security guys around. I would like to say thank you for all work that you do to to secure are computer world.

-Bob : WTF? Why the hell am i greeting you? Who are you? and why is your name in my head? GET OUT!!!!

-Ma Bell : Thanks for makeing my life better! Where would i be without you?

```
                        .--------------------.
.-----------------------[ U H C A - I N F O ]------------[ 9.2 ]-.
```

|U H C A stands for Ugly Hair Cuts Association, we help|
|people with there ugly ass hair cuts. We do not affilliate with|
|computer crime in any way shape or form. We have been helping|
|people with there ugly ass hair cuts sense 1909 and we are|
|stell going strong! Do you have a ugly ass hair cut? Then|
|call 260-009-2600 for more info. Or vistit www.uhca.jp|
| for up to date info on ugly ass hair cuts. |
| .---------------------------. |
`-----------------[Ugly Hair Cuts Association]---------------'
`---------------------------'

.=[HELPING OUT]===.
| If you want to help with this e/zine, just type up a text |
| and send it to Digital_Freak@hotmail.com. You will get |
| full credit for your work. And a trip to Canada. |
`=='

-------------------------------. --- "The new Age" ---
-E N D I N G - C O M M E N T S |----------------------------------
-------------------------------' Now days i see a lot of this -
--- "new age hacking" stuff. I see programs like BackOrfice -
--- and NetBuss. I see web pages hacked everyday. What - --- is
the hacking world commeing to? I would feel better - --- being
called a hacker if the other so called hackers -
--- would grow up. I like the fact that there are some true -
--- hacking / security groups out there like The L0pht. -
--- but when i here Dr.Mudge telling a reporter -
--- BackOrfice "rocks" i am forced to push away from there -
--- expertise. I see BackOrifce as a DoSing tool for -
--- newbie, warez loveing kids and same with all the other -
--- trojans. If the hacker ethics are shoved any -
--- further down the trash can, the whole hacking culture -
--- will become a rejected and hated seen. All i am asking -
--- from this is that we push away from things like -
--- BO, netbuss, and web page cracking. And move to -
--- a new era of hacking where people want to learn -
--- and want to follow the hacker code. If anyone is -
--- pissed of by this comment, I do not care -
--- because you choose to do these things. So by -
--- that, you will have to ackowledge the fact that -
--- people will critize you for your actions. -

.-------------------------[WARNING]---------------------------.
|!!|
`---[NO PHONES OR COMPUTERS WHERE HARMED IN THIS PRODUCTION]---'
`---'