1. Introduction

I’ve already covered some of the topics that fall into this category in my notes on malicious acts. In particular I’ve discussed viruses and related issues. I’ll get into a bit more detail here on these topics, but will mainly concentrate on other issues like hackers and phreaks.

2. Hackers

Hacking used to be considered an ethical profession, but then some hacking groups like the Legion of Doom, whose only goals were negative, changed the connotations of the name to where it is now almost universally thought of as a very negative term. Possibly, however, things might change back, since I have just got a new book called Hands-On Ethical Hacking and Network Defense. Ethical hacking describes is how we first thought of the hacking community before it got corrupted.

Levy’s hacker ethic, which was the moral code for hackers, had six principles:

1. Access to computers – and anything which might teach you something about the way the world works – should be unlimited and total. Always yield to the Hands-On Imperative.
2. All information should be free.
4. Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position.
5. You can create art and beauty on a computer.
6. Computers can change your life for the better.

So while the hacking code certainly implies lifestyle that is anarchistic in its underlying philosophy, it is not negative or destructive. The emphasis is on the benefits that can
come from computers, and certainly doesn’t imply a luddite approach where hacking can lead to destruction of computer systems.

A classic example of a positive hack was the approach taken when the Morris Internet Worm hit. Groups of programmers, in particular at MIT and Berkeley, worked without sleep to reverse engineer the worm code and to come up with fixes. They were motivated by two major goals: getting the Internet back from under the control of the worm and being the first group to solve the problem. This is hacking at its best.

The first real changes to the definition of hacking was when people began to use the name for those whose only goals were based on item 1 of the hacker code, getting access. It became a point of pride as to who could first break into a particular system from outside. However this didn’t start until there was outside access to computers, which meant that computers were networked, and that began long after hackers had been around. The trouble began when people wanted to prove to the world, and not just their friends, that they had broken into a particular system, and so they began to leave their mark on the systems that they had hacked. A nice example, which had unforeseen consequences, was when a certain state university (I’ll call it that name for anonymity, hacked their state Department of Motor Vehicles mainframe. That system output a message saying “This crash is brought to you by the Certain State University Computer Science Department” and the system then went down for 1½ days. While the message was amusing to those of us who were in a different state and not waiting in long lines at DMV offices, the legislature was not amused. It was believed to be a major reason why that university took a financial hammering in the next legislative session.

This led to escalation, where hackers had to not only break into systems but also attempt to prove something by damaging them. Related efforts included letting loose worms and viruses, although most people still believe that hacking involves directly entering a system.

**Hacker Groups:** There have been a number of hacker groups formed over the years including the 414 Group, the Legion of Doom, and the Cult of the Dead Cow.

The only apparent goal of the Cult of the Dead Cow was to find security holes in new releases of Microsoft’s various Windows releases. As soon as a new release came out they attacked it, and were always able to find security holes which they reported first to Microsoft and then to the community.

The Legion of Doom was a relatively small hacker group created, by invitation only, by Lex Luthor. After some notoriety it split into two groups after Phiber Optik was thrown out of the group by Erik Bloodaxe. The new Masters of Deception and LOD then competed as to which group could perform the “best” hacks in a contest called the Great Hacker War. This war ended badly because apparently once it was clear that they were losing badly some members of LOD informed on their opponents, the cardinal crime

---

1 Obviously these are their online names. I haven’t tried to chase down their real names.
amongst hackers. The groups disbanded once they came under a major federal and state attack.

While these hacker groups were usually by invitation only, more open hacker clubs have also been formed, of which the most famous was the 2600 club, which at first was more of a phreak club (see below)\(^2\). While this club has come and gone a few times over the years, they also started a magazine for hackers called 2600 – The Hacker Quarterly. To give a feel for this magazine, a recent table of contents was:

- One Step Forward, Two Steps Back
- Hacking Google AdWords
- Hacking Google Map's Satellite Imagery
- Googlejacking by Example
- Home Depot's Lousy Security
- SYN-ful Experiment
- The University of Insecurity
- Creating AIM Mayhem
- AIM Eavesdropping Hole
- Network Vigilantism Using Port 113
- Hacking Encrypted HTML
- Passwords from Windows
- Data Mining with Perl
- A Yahoo! Restriction Defeated
- Spying on the Library
- ParadisePoker.com Blackjack Cracked
- Where Have all the Implants Gone?
- Adding Sub-Domain Support to Your Free DotTK Domain
- Getting More from T-Mobile
- Remote Unix Execution Via a Cell Phone
- NCR: Barcodes to Passwords
- Defeating BitPim Restrictions
- Fun with School ID Numbers
- Remote Secrets Revealed

Over the last few years hackers have often redirected or modified sites as compared to attempting to destroy them. E.g., in 2002 Heidi Sherick, the MSU College of Engineering Assistant Dean, described an online mentoring group for women in science and engineering at a meeting of the MSU Association of Women in Computing student chapter. When students subsequently tried the site they found that it was a pornographic video site. They complained to me, as Department Head, and Heidi wouldn’t believe me for a while when I phoned her. The mentoring site had been hacked and redirected to the video site.

\(^2\) As I’ll discuss in the section below, the 2600 Hz frequency is very important to phreaks, which led to the name of the club.
On a larger scale, changes have either just been malicious or even dangerous. USA Today was hacked in 2002, and their online news page contained false news. Whether or not this was dangerous depends on how many people were fooled by the fake news (basically the Orson Welles War of the Worlds scenario).

Recently Western governments have been concerned by intensive hacking attempts that seem to be originating from the Chinese Liberation Army. On September 14th, 2007, the British Guardian newspaper reported that a number of British government agencies, including the Foreign Office, had been successfully attacked by these hackers. In 2006 the House of Commons computer system was shut down by what was believed to be an individual hacker, but is now believed to also have been the group from China. In June 2007 the group successfully hacked a military network in the Pentagon, in what is now being described as the most successful attack ever on the US Department of Defense and as the “most flagrant and brazen attack to date.” There have also been reports that the same group compromised an email system, which included the email in the office of Robert Gates, US Secretary of Defense. The attacks were initially assigned the codename “Titan Rain” by the US, but the current codename is classified. Wikipedia³ claims that the Titan Rain attacks also accessed networks at Lockheed-Martin, Sandia National Labs, the Redstone Arsenal, and NASA.

The German Chancellor, Angela Merkel, raised the issue of attacks on German government systems on her official visit to China in August, 2007. The German magazine Der Spigel reported that the attack was based on a Trojan horse in PowerPoint and Word systems, and that the disagreement overshadowed the Chancellor’s visit to Beijing. The Chancellor said at a TV interview as she left for the visit that “Germany is trying to ensure that its intellectual property is protected in its relations with China.” German intelligence and their federal Data Protection Office said that the attacks were occurring almost daily from Lanzhou, Canton, and Beijing, and that the Chancellor’s Office and the German Economics, Foreign, and Research and Development Office computer systems had been compromised.

The French have also confirmed attacks in 2007, without providing any details to the press that I have seen.

The Chinese government denies any connections to the attacks, which appear to have begun in about 2003. They also said that the reports were irresponsible speculation and completely unproven.

3. Phreaks

The name phreak was originally reserved for someone who broke into phone systems to get free access to telephone services, or just to explore around. Some traditional phreaks

did not attempt to even use the access once they got it, but instead reported security flaws to the telephone companies that they had infiltrated. I.e., they followed the traditional Hacker Code. Now the name has expanded to also include hackers who gain illicit access to computer networks.

Some phreaks have gained fame because of the skills that they used, or in some case because of their inventiveness. In other cases phreaks have become just because of their successes in other fields. I’ll start by looking at a few famous phreaks.

**The Badir brothers:** The Badir family, a Palestinian family living in Kafr Kassam, Israel, had four sons, three of whom were born blind. The sighted son became a baker and takes no part in the rest of this story. The three blind sons decided that a good life goal was to be able to out-think, out-program, and out-hack any sighted person, and after a while decided that this could also be a very profitable goal. They made a particular point of targeting Israeli telco companies. Yekutiel Lavi, a security specialist at an Israeli telco is famously quoted as saying “Every day people try to steal from us, but nobody has ever stolen from us the way the Badirs did. When they dial, they use the middle finger.”

The Badirs’ most profitable accomplishment, which also led to their arrest, was to set up their own telco by piggybacking onto the Israeli army’s telephone system. They sold long distance service at below normal cost, mainly to Arabs living in Israel, and had no overhead because the Israeli army provided all of the service. It is estimated that they made over $2 million in profit this way.

Whereas most phreaks use a single technology to gain access, the Badirs used a number of techniques. They most unusual skill was impersonation; they were shown to have impersonated security people, young friendly women, angry managers, and a variety of other types in order to get people to give out classified codes. They were also experts on the systems in use and the programming techniques needed to get into them.

They were charged with 44 crimes and Ramy Badir, who was their leader, served nearly four years in prison. His two brothers served no prison time. They are collectively known as “The three blind phreaks” and still claim in a recent interview that “a computer that is safe and protected is a computer stacked in a warehouse and unplugged.”

**Joe Engressia (“The Whistler”):** He was strange enough that he liked to phone up disconnected phone numbers just so that he could listen to the message. One day he whistled while listening and got cut off. He tried again, and once again when he whistled the song he got cut off when he reached the same point in the song. Fascinated he phoned AT&T technicians and asked them what was going on. An engineer there foolishly explained to him that a 2600Hz tone was used by the phone companies to “blow off” a call. The Whistler then taught himself to whistle all of the tones that he needed to be able to make phone calls, and could produce them at will.

---

4 Telephone company

5 This approach to getting information is called social engineering by hackers and phreaks.
**John Draper (Cap’n Crunch):** In 1971 Cap’n Crunch cereal included a 3” whistle toy as a giveaway with the cereal. It came in different colors and kids were encouraged to collect all of the colors.

John Draper is usually given the credit for discovering that the whistles gave out a surprisingly accurate 2600 Hz tone if you covered one of its two holes, although he says that “I actually didn't discover it. Some blind kids Dennie, Jimmie, and a few others had known this for quite some time. So although I used the name⁶, I can't really take credit for figuring it out.” He was much more sophisticated in his use of the tone than the Whistler had been. As mentioned above, the 2600 Hz tone was a drop out or blow off signal. Cap’n Crunch would dial an 800 number and then once connected he’d blow the whistle. After receiving the signal the telephone system dropped the call with a ker-chunk sound and then waited for more input. A special code, followed by a phone number, and then another special terminating code would connect you to the phone number that you’d dialed. As far as accounting went, the only record was that he’d dialed the 800 number. This became a widely used technique for phreaking long distance calls (which no longer works in the US, although apparently some pre-digital systems purchased from AT&T still exist in some other countries).

The idea was encoded into “blue boxes” which had a button for the 2600 Hz tone, ten buttons for the digits, and buttons for the opening and closing codes.

**Steve Wozniak (The Woz):** Famous mainly for creating the Apple 1, initially as free plans which he distributed at the Homebrew Computer Club, and later as a $666 device, and co-founding the Apple Company with Steve Jobs and Ron Wayne, the Woz was first a phreak, building blue boxes. He claimed to have perfected his blue box, and apparently sold a number of them, although he never appears to have been in either the computer or the blue box business for the money.

### 4. Software Security

The issue of software security has become much more visible over the last few years, and all software companies have started to worry more about the issue.

---

⁶ He’d used the name as an ID on a hackers bulletin board.
In 2002 the Computer and Telecommunications Board of the US National Academy of Sciences released a draft report which said that currently software makers do not have enough incentive to ensure their products are secure. It recommended that the US Government consider amending laws so that software makers can be held liable if their products put the public and businesses at risk. The report said that “Possible options include steps that would increase the exposure of software and systems vendors and system operators to liability for system breaches.”

The NAC report was initiated by post-9/11 concerns, but also looked at extreme cases where software has been known to kill people. The most extreme case is the Therac-25 case, where software controls let the system deliver lethal radiation doses to people who were receiving radiation treatments (it is unknown how many people were overdosed using the system, and how many will ultimately die from cancers caused by overdoses, but at least three people were killed by Therac). There were a number of things which caused the Therac failures, from design through testing, but I won’t go through them all in these notes.

The NASA Mars Program gave a good and very expensive ($0.3 billion) example of different ways in which insufficient attention to software security can cause system failures⁷. It was well publicized that the Mars Climate Orbiter was lost because one team (Lockheed) was using imperial measures while another team (JPL) was using metric measures. The NASA review of the failure, while agreeing that the immediate cause of the loss was this measurement discrepancy, laid the real blame on a software system failure. They had procedures in place which should have detected the problem, and the procedures were not followed. Ed Weiler, NASA's Associate Administrator for Space Science said that while the root cause of the failure was the units mix-up between navigation teams, the real problem was a systemic failure to follow NASA procedures. The navigation operations team came on the program just two months before launch, Stephenson said. Its members had not been involved in any of the orbiter's design reviews, and "they actually assumed that the spacecraft was much like the Mars Global Surveyor, which is really a different spacecraft," he said. The JPL navigators realized back in April that there was a problem in synchronizing the data from Lockheed Martin with their own, Stephenson said. Even though the two teams had a meeting to try to determine the cause of the problem, “this anomalous situation was never resolved.” Furthermore, the navigation team failed to follow procedures that would have alerted the rest of the mission to their concerns, and the team was never the subject of a peer review. The mission team also failed to perform a final thruster firing, and communications between team members were inadequate, the report said. The report also found the navigation team's staffing, training and communications between project elements to be “inadequate.”⁸

Subsequently the Mars Global Surveyor was also lost, when its software apparently got confused by elevation data.

---

⁷ It also led to a ripping by cartoonists and comedians. My favorite, which I think was on Leno, was “You don’t need to be a rocket scientist to be a rocket scientist any more.”
Another software integration case, which almost led to disaster, was on the first moon landing. Although all of the individual software components in the moon lander worked well, the integration of all of them overwhelmed the capabilities of the computer, which lagged well behind real time. A resourceful person on earth managed to redirect elevation data from earth-based computers, which only left them a few seconds behind their real elevation.

Probably the scariest software problem was when the US defense system computers detected the moon rise over the horizon as an incoming Soviet missile attack. They were on full alert before the “attack” vanished.

Software companies now all have software security sections with the responsibility to make software as secure as possible and to protect their software against attacks. Companies use “ethical hackers” or “penetration testers” to attempt to do what unethical hackers do – break into their systems – so that fixes can be made in advance, not just in reaction to security breaches. There are now even certifications available for ethical hackers, including Certified Ethical Hacker, Open Source Security Testing Methodology Manual Professional Security Tester, and Certified Information Systems Security Professional.

5. Network Security

This topic usually refers to network insecurity, and how to protect your networks from attack.

There are many sophisticated methods for scanning networks and systems for vulnerabilities that an unethical hacker can then take advantage of. For example port scanners are tools which scan large numbers of addresses so that they can decide what services are running on each system. They do this by probing specific ports on each system with a variety of scan modes with names like ACK, Connect, FIN, NULL, SYN, UDP, and XMAS. Most of these rely on the three-way handshaking that goes on when running TCP/IP connections, which is the standard for the Internet. These techniques will let them distinguish between filtered and unfiltered systems, or other potential security holes.

In most states port scanning is still legal, and it has been difficult to prosecute port scanners anywhere, because just the act of scanning doesn’t damage the system.

Enumeration is the next technique, which follows up port scanning by trying to penetrate vulnerable systems to get accounts and passwords. This is usually illegal.

Despite the fact that most known attacks target Microsoft-based systems, all systems (including Linux) have potential security holes. System managers with heterogeneous
systems need to be expert on the vulnerabilities of all of their systems, be able to probe their systems for weaknesses, and be able to provide protections.

As networks become more varied, vulnerabilities have increased. For example wireless networks, which are still relatively new, have opened up a whole range of new problems since everything is obviously being broadcast. A variety of tools are available for probing wireless networks.