



BLUEBOXING - MYTHS AND FEELINGS

AUTHOR: gamma & skyper

CHAPTER 1 - BEFORE THE INTERNET

In Germany of the early to mid-90s, the Internet was barely there. Some universities had a permanent connection and few people used the phone line to connect to the Internet.

The phone line was the real gateway for most: to information, messages, warez, hacking tools, and underground e-zines like 2600 and Phrack.

The Internet was rather empty. The cool stuff was still hosted on Bulletin Board Systems (BBS): A computer, run by an amateur, that you could dial in directly, using your own computer with a modem hooked up to the phone line.

But access cost money. Calls were billed per minute, especially to BBSes outside your city.

In the warez scene, time online meant status: the longer you stayed online, the more you could upload. For hackers, overseas dial-up meant access to the cooler BBSes, better tools, and direct exchange with other hackers through chats and message boards.

CHAPTER 2 - BLUEBOXING IS DEAD. LONG LIVE BLUEBOXING.

Many of the popular myths did not match how things actually worked.

The Captain Crunch whistle — the idea that a simple 2600 Hz tone was enough to place free calls — was basically useless. It simply did not work in practice.

Telcos used frequency filters to stop blueboxing and many countries switched to SS7.

"Blueboxing is dead" was a lie to stop newcomers, like us, from "boxing".

It wasn't dead. It just required a whole lot more skills and patience in the 90s.

Despite the name, this was usually not about a literal "blue box", but about software tools such as Scavenger Dialer or Dialomat generating the tones.

We "injected" the tones into the phone network by pressing an over-ear headphone onto the handset's microphone of an ordinary (rotary) phone.

It was "analog". Nothing behaved reliably.

Line quality was never the same, and trying the same thing a second time could produce different results. Most of the time, we did not know why our breaks failed.

And there were frequency filters: Today people would probably call them firewalls or IDSs: systems meant to detect malicious signalling tones and filter them. We had to overcome those filters:

If the filter was 2550-2650 Hz then we would try 2549 Hz or a combination of frequencies, to create more funky wave forms that would bypass the filter but still be recognized by the phone exchange as "valid" frequencies.

It was trial and error.

A crucial factor was the actual call path. You first needed a suitable toll-free number as an entry point; otherwise the call might still show up on the bill. But even that was not enough. What mattered more was how that toll-free call was routed. If it passed through older in-band signalling systems such as R1, R2, or C5 — or through interworking points — blueboxing could still work, even if other parts of the network were already using SS7.

Such entry points were called "C5 numbers". The easiest to guess were Home Country Direct (HCD) numbers: toll-free operator access numbers where the destination side could accept the call charges.

Blueboxing took time. Many attempts were needed to break the line: Every time you had to call the HCD Operator (a human) and then blast a shrill frequency into their sensitive ears.

They were least amused (and understandably so).

Not every country could be reached by toll-free HCD numbers. HCD numbers (so we believe) were also more strictly monitored for abuse (by the fedz) and every break-attempt caused distress to the Operator. Not ideal.

They were often easier to break, but we did not like using them for the reasons above (we were scared).

Wardialing mattered because the real prize was finding less common, non-HCD C5 numbers, which usually circulated only within trusted circles.

These were traded like 0days.

With many C5 numbers, some variation of 2400+2600 Hz, a delay, and then 2400 Hz worked. The exact timing varied, and sometimes it was 2420 Hz or so instead. This was known as the standard break. Every line and every break was different. There was no fixed recipe.

A successful break gave you silence. Not a dial tone. Dial tones are comfort noise for humans. Interconnected Telco switches did not need to comfort the calling Telco switch (in this case, the phreaker).

After that, KP1/KP2 + number + ST was sent to place the call.

This was a switched "phone" connection. This means the copper wire from my phone line was directly "connected" (as a single loop) all the way to the receiver in some C5 countries — through multiple countries, through the ocean, and through outdated telephone exchanges and amplifiers along the way.

The voice quality was never that great. And the modem would lose connection every 20-120 minutes. I only remember once that a modem line was still connected after I woke up from a night's sleep :->

CHAPTER 3 - A LINE THAT WOULD NOT BEHAVE

After endless attempts with the standard break, one thing became clear very early: Indonesia was different. It was a painfully slow process: dial the HCD number, wait for the system or operator to answer, send the break, fail, hang up by pressing the hook, wait for the line to clear, then dial the HCD number again. Hours disappeared like that, and most of the time we did not even know why it failed.

As far as I remember, I worked on this around that time with a friend from IRCnet. Memory gets blurry here. At some point, one of us found a frequency that did "something new": no hangup (which was good) but a gurgling noise.

However, seizing the line to place a new call was not possible. Nothing happened. Then, after roughly 30 seconds, the line dropped with a beep.

What finally seemed to matter was to send a tone just _ before_ or on top of the beep. The beep itself was not always at the same point either: sometimes closer to 29 seconds, sometimes closer to 31.

This was new. The Indonesian HCD call route followed its own rules.

UNPREDICTABLE. The "seizing tone" had to be sent PRECISELY (within 50ms?).



The excitement and pressure when the timer reached 30 seconds. I was in predator mode: My senses sharpening. Not breathing. Muscles tensing. Waiting for the "beep", ready to slam my hand with the speed of a snake down onto my space bar to send the tone and seize the line.

Missing the timing meant I had to start all over again and wait another 30 seconds or so. Muscles tensing and all that...

The relief and joy when it worked. When I heard the sweet sound of a ring tone from the receiving end. The call got connected: A single electric circuit, starting at my house and halfway across the globe to the receiver's phone.

I conquered the system. I tricked it. It yields to my commands. MY line.

Achieving a single successful break took a good 20-40 minutes.

The reward was immense: The Indonesian HCD allowed global calls instead of just domestic ones within Indonesia. This meant that I could call the entire world by breaking just Indonesia.

CHAPTER 4 - WHAT BLUEBOXING REALLY WAS

What started as experimenting with tones on a telephone line was, in retrospect, something else entirely.

It was learning how to explore complex systems that did not behave the way they were supposed to.

This was never really about getting rich. At best, it meant some pocket money; compared to the hours and days it took to get international free calls working, a normal job would have paid better.

In some ways, it was a sport. Breaks were collected, compared, and shown off. Some people used IBM Internet dialup accounts to get onto IRCnet; when they joined, others could see from the FQDN that they had successfully broken into a country route.

We also thought that blueboxed calls gave us a more anonymous way onto the Internet, even if that usually meant a slow 9.6k bits/second connection.

Looking back, I am not even sure whether that anonymity was real, or whether we were simply tolerated because the effort of stopping us was too high for a few small fish like us.

What we got from it was not money, but access, status, exploration, and for a brief moment the feeling of being inside a system that had never been meant to be understood from the outside, let alone used the way we used it.

It felt, for a brief moment, like having root on part of a country's telephone network.

I did my last "break" in 2006.

In a way, it is sad that blueboxing is no longer performed. It was a real art. We miss the sport. And we miss the scene. Anyone who has ever spent hours digging through a system until it finally gives way will know that feeling.

It's the most beautiful feeling in the world. I'm chasing that feeling.

|=====|

Shoutz: c0dak, noptrix, disq, kornicz, faceless,
giem0r, rpunk, darkcube,

fx (rip), stealth (rip), prdelka
(hackerfantastic), Sabre Wolf, scut,

vanhauser, pandazilla, larage, dash ... #bluebox
IRCnet.

|=====|

