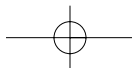


Chapter 5

For Whom Ma Bell Tolls

by Joe Grand as "The Don"

The sun had already sunk beyond the harbor as Don Crotcho woke up. He neither noticed nor cared. It had been a little more than a year since his flight from Boston after a successful theft of the United States' next-generation stealth landmine prototype, and he had been enjoying his self-prescribed seclusion in this land of fire and ice...

**136 Chapter 5 • For Whom Ma Bell Tolls**

Between the wonders of volcanic activity, the lush, moss-covered fields, beautiful countryside, and seductive nightlife, what was there not to like about Iceland? It was a nice change from the urban concrete playground and he was glad to get away.

Don Crotcho, affectionately called *The Don* by his associates, had become a local in his neighborhood of Norðurmýri in the city of Reykjavík. By word of mouth, his skills as a *phone phreak* were respected and feared by the underground world of computer misfits and organized (and not-so-organized) criminal enterprises, reaching far and wide.

The Call

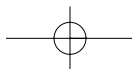
A few days ago, The Don got a phone call from some guy named Knuth. He was a friend of a friend. Rather, more like somebody who knew somebody who knew The Don. He didn't give The Don a lot of background information, which was probably for the better.

As Knuth so bluntly put it, the telephone systems were a key part of some operation he was involved in. He needed The Don to gain access to a specific cellular phone switch in the Republic of Mauritius (a small tropical island on the southeast coast of Africa), trace the phone calls made to and from a particular phone, and then disconnect the line. If he did it, he'd get paid a good chunk of change. If not, well, that wasn't really an option after Knuth described how The Don's anatomy would be creatively rearranged.

Now, The Don was used to threats on his life and limb by the bloated egos of underworld criminals, and Knuth was no exception. In this line of business, it came as no surprise. Since The Don had heard it all before, he brushed it off and got right to the point: payment.

The Don demanded a modest fee of \$100,000 cash. Low by criminal standards, but The Don enjoyed his work so much that sometimes he had to remind himself not to just do it for free.

That phone call was like a spark that lit a fire under The Don's sleeping baby soul. He was reenergized, invigorated. And he celebrated by taking a walk to the one place he frequented.



Maxim's

The Don lounged in a plush red velvet seat at Maxim's as he flicked dollar bills towards the stage. From the outside, settled on a small side street in downtown Reykjavík, Maxim's didn't seem to be much—fitting snugly between two brick row houses, the single wooden door into the establishment gave no clue as to its purpose.

Inside the smoke-filled club, the black walls reflected the multicolored lights that shined down onto the stage. The bar in the center was crowded with familiar faces, men and women obviously enjoying their night—drinking, laughing, and taking in the sights. Worn-out fabric couches lined the open spaces and a handful of individual seats were facing the stage. Rhythmic music pumped out of speakers hanging by chains from the ceiling.

Maxim's was a refuge for The Don. Finishing off the rest of his chilled Brennivín, he headed downstairs. The iron spiral staircase led to a few small “rooms,” each separated by a swatch of black velvet hung on old shower rods. As in any establishment like this, these rooms were reserved for the richer clientele—or for the select few who had earned *respect*. He walked past the cashier and around the dark corner to the room at the end of the hallway.

Brushing the velvet cloth aside, he made himself comfortable in the secluded room, usually kept free by Maxim's owners for The Don's frequent visits. The Don used this room as a makeshift office, because he wasn't always able to get back to his pad when the need for a computer was taunting him.

The room was illuminated with a single black-light tube nailed to the ceiling. There was a flimsy plastic table, the kind you see for \$2.99 at the local swapmeet, placed in the center of the room, and a vinyl couch as a seat. The walls were painted black, but years of neglect left them peeling, showing the drywall beneath. It wasn't luxury, but it got the job done.

The Don flipped his laptop open and set it down on the table. He stared into space for what seemed like an eternity as Windows finished loading.

From his basement location inside Maxim's, The Don could identify two wireless access points. Neither had WEP enabled (though that would have been just a temporary roadblock requiring him to monitor enough network traffic to then use wepcrack or aircsnort to determine the key). One access point used the typical default SSID of `default` and the other used `linksys`. He assumed that they were personal wireless networks set up by people living in

138 Chapter 5 • For Whom Ma Bell Tolls

nearby flats. They were wide open, issued IP addresses at request, and gave The Don full Internet access.

He dedicated the rest of the night to doing some initial research on the switch that Knuth wanted him to access. The Don did some preliminary Google searches to learn about Mauritius and to find the Web sites of the cellular telephone providers. He came across a page that gave him a listing of all available cellular technologies and operators in Africa. Mauritius was covered by two: Cellplus Mobile Comms and Emtel.

All Available Cellular Technologies and Operators in Africa

Country	Technology	Year	Operator	Service Area
Kenya	GSM900	1998	Safaricom	
Kenya	GSM900	4/96	Kencell	
Lesotho	GSM900	12/95	Vodacom Lesotho Pty.	Maseru
Liberia	GSM900	3/99		
Libya	GSM	5/95	ORBIT	
Madagascar	AMPS	7/25/94	TELECEL-Madagascar	Antananarivo & other cities
Madagascar	GSM900	05/97	Sacel Madagascar S.A.	all
Madagascar	GSM900	11/97	Madacom	all
Madagascar	GSM900	03/98	SMM	
Malawi	GSM900	6/99	Callpoint	
Malawi	GSM900	7/96	Celtel	Blantyre/Limbe & Lilongwe
Mali	AMPS	1/98	SOTELMA
Mauritius	ETACS	6/89	Emtel/Currimjee Jeevanjee Millicom	
Mauritius	GSM900	10/99	Emtel	
Mauritius	GSM900	1/96	Cellplus Mobile Comms	
Morocco	GSM900	4/94	Missalat Al-Maghrib S.A.	Rabat, Casablanca
Morocco	NMT-450	1989	Office National des Postes et Telecom.	main cities and roads
Morocco	GSM 900	1999	Medi Telecom	
Mozambique	GSM900	6/97	Empresa Nacional de Telecomunicacoes de Mocambique (TDM)	Maputo, Matola and "Maputo Corridor"

Knuth had requested that The Don trace all calls going into and coming from the mobile phone at 230-723-8424.

The Don checked more of the Google search results and found a document that described the current telephone numbering scheme for Mauritius. According to the document, all numbers with a “72” prefix belong to Emtel mobile subscribers. Knowing that, the Emtel cellular phone switch would be the target for Knuth’s request.

Telephone Numbering Scheme for Mauritius

5xx xxxx	Wireless Local Loop subscribers
6xx xxxx	MT Geographic Numbering - Region South
7xx xxxx	Cellplus Mobile subscribers (75x xxxx, 76x xxxx and 77x xxxx) Emtel Mobile subscribers (72x xxxx, 73x xxxx)
800 xxxx	Toll Free numbers (freephone service)
801 xxxx	Inbound IFS
810 xxxx	Home Country Direct (Inbound via Passe Partout)
83x xxxx	Geographic Numbering (Rodrigues)
9x	Short Codes
99x	Emergency Numbers (995 and 999 with new 11x codes)

Another simple search led The Don to the Emtel main Web site at www.emtel-ltd.com. Looking at the Customer Care page, he saw that the 465 prefix is used for both the main and fax numbers.

A whois of emtel-ltd.com provided some additional clues.

```
% GANDI Registrar whois database for .COM, .NET, .ORG.
```

```
domain: EMTTEL-LTD.COM
owner-address: Web Ltd
owner-address: Chancery House
owner-address: 99
owner-address: PORT LOUIS
owner-address: Mauritius
admin-c: EL534-GANDI
tech-c: WC169-GANDI
bill-c: SC721-GANDI
reg_created: 1997-05-20 00:00:00
expires: 2004-05-21 00:00:00
created: 2003-04-18 10:55:49
changed: 2004-02-04 13:19:24
```

140 Chapter 5 • For Whom Ma Bell Tolls

```
person: EMTTEL LTD
nic-hdl: EL534-GANDI
phone: +230.4657800
fax: +230.4657812
lastupdated: 2004-02-04 13:24:22
```

The 465 prefix also is used for the phone and fax numbers in this listing. So, chances are, the Emtel offices were issued a block of telephone numbers within the 465 prefix. The likelihood of success is high that The Don would encounter computer systems with modems connected to some of the lines within the block. The Don shut down his laptop and headed back up the spiral staircase into the excitement of the club.

Shall We Play a Game?

Wardialing, made famous by the movie *WarGames* in 1983, is like knocking on the door of 10,000 neighbors to see who answers. You make a note of those that do and come back later to check out the house.

The act of wardialing is as easy as it gets—a host computer dials a given range of telephone numbers using a modem. Every telephone number that answers with a modem and successfully connects to the host is stored in a log. At the conclusion of the scan, the log is manually reviewed and the phone numbers are individually dialed in an attempt to identify the systems.

You'd be surprised at what sorts of systems are accessible through the modem. Even today, most “security administrators” still ignore the threat of wardialing.

“Who's going to find this and why would they want to?” they think, “We need to focus on the security hot spots of our network, like the wireless and Internet connections.”

However, that poor, forgotten modem connected to the computer in the telephone closet will answer to anyone or anything that calls its assigned phone number. Unsecured modems are usually the easiest way into a target network.

Modems are equal opportunity—they don't discriminate. PBXs, UNIX, VAX/VMS systems, remote access servers, terminal servers, routers, bulletin board systems, credit bureaus, elevator control, hotel maintenance, alarm and

HVAC control, paging systems, and, of course, telephone switches. There's something for everyone if you just have the patience.

The Don's next step was to decide on a way to call the numbers in Africa for free from Iceland. Free phone calls are not a difficult thing to obtain. The Don could use a stolen credit card, calling card, or mobile phone, reroute his call through a corporate PBX, or take advantage of a misconfigured outdial, a feature of some remote access network equipment which allows you to call in to the device on one modem and dial out on another.

He chose to go with using a stolen mobile phone. Since wardialing a complete prefix takes usually three or four days of nonstop dialing, The Don needed to make sure to obtain a phone that wouldn't immediately be noticed as missing. One that was left in an office on a Friday afternoon would do just fine—the owner wouldn't return until Monday to notice that the phone had disappeared. Even then, the owner might fumble around for a few more days while thinking it had legitimately been lost.

Not only was a stolen phone easy to get hold of, The Don could wardial from any location within Iceland where Og Vodafone provided service. Better yet, it was untraceable. He'd just destroy the phone when he was done.

The next evening, The Don made a few calls and walked down to the Tjörn, the park and pond in city centre. Feeding the ducks, he waited.

As expected, one of The Don's acquaintances, a fence from the neighborhood, stopped by. They shook hands and exchanged pleasantries as they strolled the path along the water. The Don handed the fence a small envelope filled with currency and received a small plastic shopping bag in return. The bag contained a Nokia 6600 tri-band smartphone and stolen SIM card. Just what he had asked for.

Back in his flat, he grabbed the required drivers from the Nokia support Web site and connected the Nokia 6600 to the serial port of his computer. Now, the computer would simply treat the phone as a landline modem.

ToneLoc is The Don's wardialer of choice. Although it's a few years old, it works fine with current Windows versions. He set up a spare machine to dedicate to the task. He isn't worried about being in a fixed location. It will be obvious that thousands of numbers are being dialed from the same phone within the same cell location, but The Don would be done wardialing before the corporate wheels of fraud detection start turning, and the phone would be long gone by then.