

## **Security through Obscurity in Telecom by dual**

### **What is security through obscurity?**

Simply defined, security through obscurity is where secrecy of design, implementation, etc. is used to ensure security [1]. Examples are particular corporate guidelines regarding vulnerability disclosure and proprietary encryption algorithms.

This article gives significant examples of security through obscurity in telecommunications. Hiding numbers is not considered, as even one number in a seemingly vacant exchange is freely accessible.

The examples do not epitomize the state of telecom security. They do illustrate weaknesses, if not vulnerabilities, in telecommunications systems that may be in front of even the most aware phreak.

### **Qwest Security Screen**

Years ago most RBOCs rolled out in similar fashion, what amounts to be, telemarketing call protection. Qwest's offering was monikered Security Screen and cost \$2.95 per month, on top of the requisite caller ID service charges. Security Screen was inherently vulnerable to caller ID spoofing through ANI fails.

The fact that one can spoof caller ID to a number furnished with Security Screen is not that serious. The real vulnerability came with a little social engineering. One simply had to call Qwest as the target and add Security Screen to their line. The vulnerable numbers just grew from Security Screen subscribers to every Qwest customer.

Unfortunately, Qwest barely whispered the fact that this service actually made subscribers more vulnerable. In fact the only weaselly mention was found buried on a service description web page. Subscribers without internet access or those not internet-savvy were never exposed to that fact, as customer service representatives are infinitely more interested in sales than disclosure. Three dollars a month to get owned.

Of course Qwest has since dropped the price of Security Screen, added a distinctive ring for entered/spoofed numbers, and fully described the realities of the service on the description web page. Regardless, the initial deliberate obfuscation showed the "money first, customer security maybe" attitude at Qwest.

### **Corporate Obfuscation**

Not long ago I worked a short stint in corporate IT. The sysadmins at my conglomerate were frequently guinea pigs for new enterprise deployments and procedures. An email arrived touting a shiny, convenient telephone application, and asked the admins to bang on it to find any bugs. The submitter with the most or most serious finds received a prize. Oh joy.

A little background on the original application: It was only available for a short time annually at, let's say, 555-1111. Calling the app the remainder of the year got a reorder. An

unpublished number was sent out for the new application, 555-6662.

The new application started by asking for the caller's Social Security number. I won't tone my Social, nor should you. That was not the end of my testing. I punched fives until the application dropped me to an unfamiliar voice mail prompt where I dialed the old application number, 555-1111. I was not greeted by a reorder. I was greeted by the supposedly off-limits original application.

Diverting through the attendant didn't work. Diverting through a toll-free access number didn't work. Dialing 555-6662 and failing out of the new app did, bringing one straight to the, in their words, "busied-out" old application at 555-1111.

Again, this was not significant by itself. The fact that one could so easily bypass obfuscation by reoder was. I told the application developers about my find, not for the specific instance, but for the fact that it may be symptomatic of similar system configurations. My words were summarily dismissed.

### **Misrepresented Exchanges**

A CLEC's exchange came up at a recent gathering of hackers, 505-338. It's on a DMS-100 owned by Time Warner Telecom. Online telecommunications databases [2, 3] state the DMS serves seven exchanges: 338, 468, 563, 846, 853, 923, and 938. Two of the exchanges were particularly interesting, 846 and 853.

A cursory Google search showed that these exchanges belonged to Kirtland AFB. Some prior knowledge led me to believe that they were housed on the base itself, not some CLEC in a business park. Just think of the security implications if they were. I wanted to prove that the exchanges were not housed at an off-site CLEC with a telephone.

I called non-working numbers on the two exchanges and received standard telco SIT and error messages:

"[SIT] We're sorry. You have reached a number that has been disconnected or is no longer in service. If you feel you have reached this recording in error, please check the number and try your call again."

I knew of a base access number that allowed callers to call other numbers within the exchanges in question. I called the access number and then dialed the non-working numbers again:

"The number you have dialed is not in service. Please check your number or call the operator for assistance. Kirtland Air Force Base [reorder]"

An airman or contractor read back a custom error message. This proved the deliberate obfuscation of where the exchanges were really housed.

## Conclusions

Qwest's obfuscation of inherent vulnerabilities was borderline evil. Many corporations count on the fact that any significantly advanced technology is magic to the masses. Taking advantage of consumers to please stockholders supersedes false consideration of subscriber security.

To the corporate robot, such security-significant instances are often indicative of other similar, possibly larger, security issues. Imagine test, administration or outdial numbers "protected" by a reorder. No system is perfect and honest, hard-working people make mistakes. Management and others in power, and denial, make bigger mistakes by mistrusting their workforce and ignoring even perceived trivial disclosure.

Also realize that the online telecommunications databases are not misleading. They are only displaying the misinformation made available to them. How many other exchanges aren't where they really are? Only corporations and their government know for sure.

Shouts to ABQ 2600, and thanks to Natas and P(?)NYB(?)Y for their input.

[1] [http://en.wikipedia.org/wiki/Security\\_through\\_obscurity](http://en.wikipedia.org/wiki/Security_through_obscurity)

[2] <http://www.bellsmind.net>

[3] <http://telcodata.us>