

The growth of Voice over IP (VoIP) has led to the emergence of a new problem, VoIP toll Fraud. Toll fraud, where unauthorised calls are made at the target's expense, is not a new problem, but the use of VoIP and the interconnection of corporate phone systems and IP Networks creates new opportunities for fraudsters.

The Problem

There are a lot of good reasons for using VoIP for corporate telephony, including faster and more flexible service deployment, extending service to remote and mobile users and integration of voice and data services. To gain the full benefits of VoIP, the corporate PBX must be connected to external IP networks. In many cases this means connecting the corporate PBX to the Internet.

Linking a PBX to any external IP network and particularly to the Internet carries a number of risks. One of these risks is *toll fraud*. Toll fraud is simply allowing unauthorised users to make calls at your expense. Toll fraud is not a new problem; it has existed since phone services were introduced over a century ago. Connecting your PBX to the Internet magnifies the problem as anyone connected to the Internet can potentially connect to your PBX and start making calls at your expense.

VoIP toll fraud is a two stage process. Firstly an attacker finds a VoIP system by scanning the Internet for suitable systems. Secondly the attacker connects to an identified system posing as a remote extension and then attempts to make calls. These calls may be to land-line or mobile numbers or in some cases the attacker may set up premium rate numbers, make multiple calls to those numbers and pocket the revenue. Toll frauds have been observed using premium rate numbers in many countries including Belarus and North Korea. In all cases the targeted organisation is left facing a large bill.

Honey Pot Tests

UM Labs has observed a growing number of attempts to make fraudulent calls using their VoIP connection. These attempts are normally blocked by our security controls. However it appears from our system logs and from discussions with other organisations that the problem is escalating.

To quantify the problem, UM Labs recently ran a *honey pot* test. Honey pots, systems running without the normal security protection, are commonly used by email researchers to investigate the sources of spam and other unwanted emails. UM Labs have adapted this technique to quantify the toll fraud problem. To do this we simply disabled the normal controls on our SIP security controller and configured a PBX so that it would forward toll fraud calls via our SIP trunk. The resulting, poorly controlled, configuration is similar to that observed on many VoIP systems. We then just watched and waited.

In less than 24 hours this system was discovered by attacker, and in a period of less than one hour over 350 fraudulent call attempts were made. Some of these were allowed to connect so that we could determine the call destination and duration. A selection of those calls is detailed below.

Target Number	Country	Description	Date/Time	Duration
50934654---	HAITI	Haiti Mobile	21/02/2011 17:41	00:10
22379398---	MALI	Mali Mobile	21/02/2011 17:32	00:09
23233750---	SIERRA LEONE	Sierra Leone Mobile	21/02/2011 17:31	00:21
22379182---	MALI	Mali Mobile	21/02/2011 17:31	00:32
50937245---	HAITI	Haiti Mobile	21/02/2011 17:31	00:23
22370138---	MALI	Mali Mobile	21/02/2011 17:31	00:25
50935689---	HAITI	Haiti Mobile	21/02/2011 17:31	00:01
22370765---	MALI	Mali Mobile	21/02/2011 17:30	01:18

From the call pattern it is likely that these calls were made from a call shop offering cheap calls to overseas numbers.

Most the 350 calls were directed at mobiles in countries from the Caribbean to Africa with a few calls sent to mobiles in Eastern Europe and South East Asia. All of the calls in the above list originated from an IP address assigned to an ISP in Vladivostok, but we have seen similar attempts from many other locations including the UK, Australia and Texas.

This test clearly demonstrates that without the appropriate security controls, any VoIP system with an external IP connection is potentially vulnerable to a toll fraud attack and that an undetected attack can quickly become very expensive.

Solving the Problem

The obvious way to solve this problem is to ensure that the PBX is configured to block all call attempts from unauthorised caller when those calls target external numbers. This is not always easy and the mechanism used is dependent on the type of PBX. The task is further complicated by the requirements of some SIP trunk connections.

The UM Labs SIP Security Controller is designed to address this and other VoIP security problems. The SIP Security Controller is designed to block both the initial probes used by attackers to locate target systems and to detected and block fraudulent calls. For further information please contact UM Labs.

Web: www.um-labs.com
VoIP: sip:info@um-labs.com
Email: info@um-labs.com
Phone: +44 20 3021 3200