# Pika µFirewall

EMPOWERING TELECOM INNOVATORS

PIKA Technologies Inc. is an original equipment manufacturer (OEM) of telephony enabling technology. Headquartered in Ottawa, Canada, the company has been in business since 1987.

In today's modern telecommunications world, using VoIP (voice over internet protocol) trunks to connect the office telephone system to the outside world is clearly the technology of choice. VoIP offers many advantages, the greatest of these being reduced cost – something that every business is focused on in these challenging times.

## Hardware Features

- 2 Full duplex Ethernet ports
- 10/100Mbps
- Ethernet LEDs and status LEDs
- Reset button
- Hardware watchdog reset
- Unit dimensions: 98mm x 38mm x 27mm (~ 3.8" x 1.5" x 1.1")
- Box dimensions: 250mm x 170mm x 60mm (~9.75" x 6.75" x 2.4")
- External power supply with USB type A plug (AC 110-240V, 50-60Hz)
- Power consumption: 4W
- Operating temperature: 0°C to 45°C
- Storage temperature: -20°C to +85°C
- Humidity, non-condensing: 5% – 95%

Besides a lot of advantages, the improved technology of VoIP actually makes the process of hacking into business telephone systems easier, quicker and more successful. There are even specialized software programs developed to perform hacking which are commonly available to be downloaded from the internet with a high rate of success just because of misconfiguration, weak password usage and inadequate security systems or policies. If this has not happened to you yet, it probably will. And, VoIP service suppliers are less and less willing to forgive these large amount of bills.

## General Features

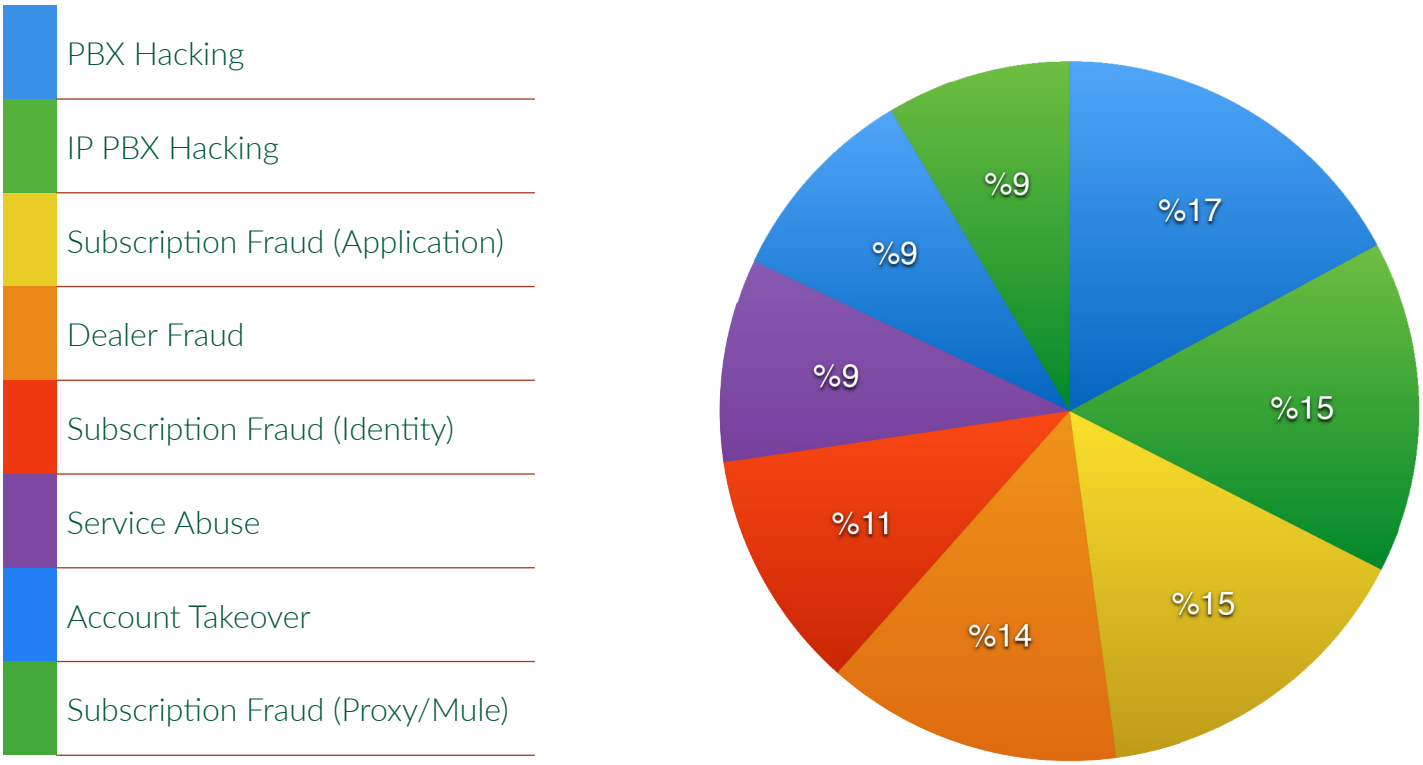
- Analyzes SIP packets through deep packet inspection
- Stops abnormal SIP protocol usage based on predetermined parameters
- Prevents SIP denial-of-service attacks
- Helps to prevent continued attacks by quietly dropping malicious SIP packets rather than responding with an error
- Analyzes patterns within SIP packets and adapts to identify and block hacking attempts
- Neutralizes SIP attacks in real-time
- ZERO ongoing maintenance in stand alone mode.
- Cloud Management and/or RESTFul API
- Requires ZERO special skills, ZERO configuration and Easily plugs in front of your existing PBX
- Power supplied through the USB power Cable (included)
- Operates at Layer 2, so device is transparent to existing IP infrastructure – no changes required to add device to the existing network
- Small form factor – measures just 3.8 x 1.5 x 1.1 inches
- No measurable latency

# Threat Analysis

EMPOWERING TELECOM INNOVATORS

## Worldwide loss caused by fraud*

According to Communications Fraud Control Association (CFCA) worldwide telecom fraud survey in 2013; estimated loss caused by fraud is at $46,3 billion which is up by 15% from 2011. The top five countries where fraud terminates are: Latvia, Gambia, Somalia, Sierra Leone, and Guinea. PBX Hacking is second from top in methods for committing fraud with a total loss of $4.42 Billion.




If we look at the results of the survey in 2015, total estimated loss is lowered by %17,8 with $38.1 Billion. Top countries where fraud terminates are:Cuba, Somalia, Bosnia&Herzegovina, Estonia, Latvia, Guinea, Serbia, UK and Lithuania. PBX and IP PBX related fraud loss is at top with a total estimation of $7,46 Billion which is ~%68.7 higher than the survey taken in 2013.

As you can see from the results, the trend is going down for total loss but PBX/IP PBX related fraud loss is still going up. This shows us that users and operators does still have vulnerabilities for Fraud attempts.

*** Source: Communications Fraud Control Association (CFCA) 2015 and 2013 Global Fraud Loss Survey reports**

# Q&A

EMPOWERING TELECOM INNOVATORS

## I have a firewall in my network. Why shall I use Pika µFirewall?

Traditional Firewalls are data centric and even if they support Deep Packet Inspection (DPI), analysing all ports and protocols may create performance issues or requires expensive hardware. In general terms, IP firewalls are looking for source and destination ip address and ports . If the traffic is permitted , they'll accept the packet. Which means that if you open SIP ports to public internet, everybody will be able to send requests to your system. On the other hand Pika µFirewall is able to analyse and keep track of SIP sessions by focusing on SIP only. Also IP Firewall systems require configuration which means they are open for Human errors. Pika µFirewall requires zero configuration to operate and less vulnerable for human errors.

## I have a software on my PBX that prevents attacks, isn't it enough?

Most of the open source solutions are coming with applications like Fail2ban which analyses the logs that are created by the PBX service or filtering connections using Iptables and other software. The problem about these solutions are:

- They require a log to detect the attacks. The application won't take any action if there isn't any log. µFirewall is analysing the SIP packets and tracking the sessions. So it does not depend on the PBX service. You can use this solution with any PBX system that supports SIP.
- It's a daemon/service running on the server. It can stop or be stopped. µFirewall is a hardware and there isn't any option to disable or turn it off other than removing it.
- These kind of solutions are reactive. The system will expose itself to the attacker during a scan. µFirewall is proactive, it senses the scan attempt and drops the packet without replying it. So the attacker doesn't know that there is a PBX running on that IP.
- Managing multiple instances of these solutions are nearly impossible. µFirewall has a cloud management portal so you can configure or upgrade your systems from single web page.
- These services are running on the server so any attack can increase the load of the server and consume traffic. µFirewall is positioned in front of the PBX and it reduces the traffic and load of the server.
- Software like Fail2ban works on Linux systems, µFirewall is PBX agnostic and can be used with any PBX that supports SIP protocol, including black boxes in which you can't install any 3rd party software.

## Can I use µFirewall to protect my IP Phone/ Gateway?

No. µFirewall is designed to work with B2BUA which means that it needs a PBX behind one of the ethernet ports. IP Phones and Gateways does not have the B2BUA feature.

# Q&A

EMPOWERING TELECOM INNOVATORS

## Can µFirewall protect me for all kind of threats?

No. µFirewall protects your system to scanner,DDOS, Brute force and Dictionary attacks. If you use weak passwords like “1234” and the attacker knows that there is a PBX running behind your IP, the attacker may gain access to your system as they have a pretty good probability to match the correct user credentials at their first attempt. You have to apply necessary security precautions like using strong passwords for your systems.

## My VoIP operator says that they have a mechanism to prevent frauds. Do I still need Pika µFirewall?

VoIP operators are dealing with huge amounts of sessions so they may not be able to react in a timely fashion. The systems used by VoIP operators run periodic checks through accounts and it may take some time. If some one is making fraudulent calls through your system they can still cause damage but it will be limited. You can prevent these damages by using the µFirewall.

## I have multiple sites using VoIP systems. What kind of advantages does µFirewall can provide to me?

You can manage all the µFirewall units located at your sites through the cloud management portal provided by Pika. You can create Blacklists and Whitelists based on devices or based on your user. Also you can upgrade the units remotely.

## Can I protect my PBX running on Virtual Server?

Yes. If you have a single instance of PBX running on your virtual environment, then there is no need for an extra configuration. If you are running multiple instances of PBX applications on the same virtual environment, then you have to assign one of the ethernet ports of your server to the Virtual server and connect µFirewall to that ethernet port.

## Do I need to register my device to the cloud portal?

No. You can still use the device without registering to the Pika µFirewall cloud management portal but you’ll loose the advantages provided by this service like receiving email notifications about blocked ip addresses. Also you’ll have to configure or upgrade the unit from the USB port using configuration files.

## What happens in an event of failure at µFirewall ?

You have to replace the unit with a new one or remove the unit. This solution is an active system and does not provide any passive failover feature.