KAMAILIO WORLD
CONFERENCE & EXHIBITION
BERLIN, GERMANY, MAY 27-29, 2015

The safety of your VoIP platform has a name
kamailio

Daniel-Constantin Mierla
Co-Founder Kamailio Project
www.asipto.com
@miconda

Very important to

- *protect your customers*
- *protect your business*

Attackers try to

- *penetrate customer premises equipment*
- *penetrate core platform*

The Goal

Protecting everything as much as possible in the core network

Expect new type of attacks every day

- *no universal solution*
- *security is a 24/7 duty*
- *very important*
  - *ability to adjust rules as needed*
  - *agile monitoring and alerting mechanisms*
  - *have access to a flexible toolset to enable new security policies*

Always good to consider

- *monitor, detect and block high traffic volume from same source address*
- *monitor and detect too many failed authentications in a row*
- *allow traffic only from your customers regions*
- *alert, block or two factor authentication for calls to expensive destinations*
- *alert and limit on number of active calls*
- *alert and limit on the duration for active calls*
- *alert and limit on the cost of overall calls*
- *check and allow only strong passwords*
- *enable TLS*

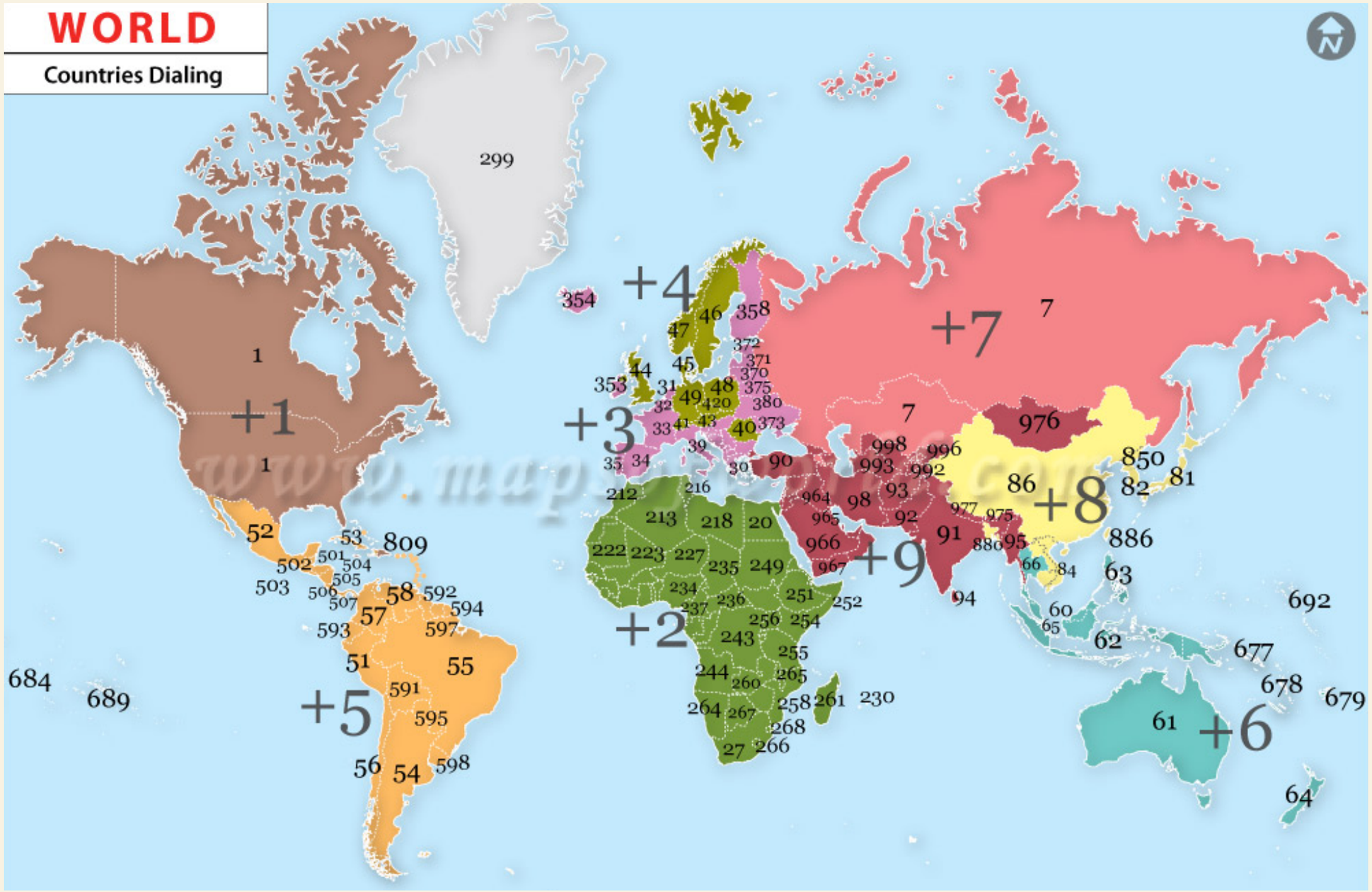
Extra little bits

- *allow calls only from registered users*
- *INVITE with To tag must match an existing dialog*
- *limit number of allowed registrations*
- *restrict allowed User-Agent header*
- *restrict capabilities when subscriber not in home country*
- *rules based on time frames*

Some Examples

Block calls to destinations by prefix or regexp

- *usefule kamailio modules: mtree, userblacklist or dialplan*



Blocking with mtree

```
loadmodule “mtree.so"

# ----- mtree params -----
modparam("mtree", "db_url", DBURL)
modparam("mtree", "char_list", "+0123456789")
modparam("mtree", "mtree", "name=pblock;dbtable=pblock")
modparam("mtree", "pv_value", "$var(mtval)")

request_route {
...
        $var(dstnr) = $rU;

        # match if  blocked prefix
        if(mt_match("pblock", "$var(dstnr)", "0")) {
                send_reply(“403”, “Destination blocked”);
                exit;
        }
...
}
```

```
CREATE TABLE `pblock` (
  `id` int(10) unsigned NOT NULL AUTO_INCREMENT,
  `tprefix` varchar(32) NOT NULL DEFAULT '',
  `tvalue` varchar(128) NOT NULL DEFAULT '',
  PRIMARY KEY (`id`),
  UNIQUE KEY `tprefix_idx` (`tprefix`)
);

mysql> select * from pblock;
+----+---------+--------+
| id | tprefix | tvalue |
+----+---------+--------+
|  1 | +44     | 1      |
|  2 | +49     | 1      |
+----+---------+--------+
```

Block traffic based on source address

- *usefule kamailio modules: geoip, geoip2, permissions, sqlops*

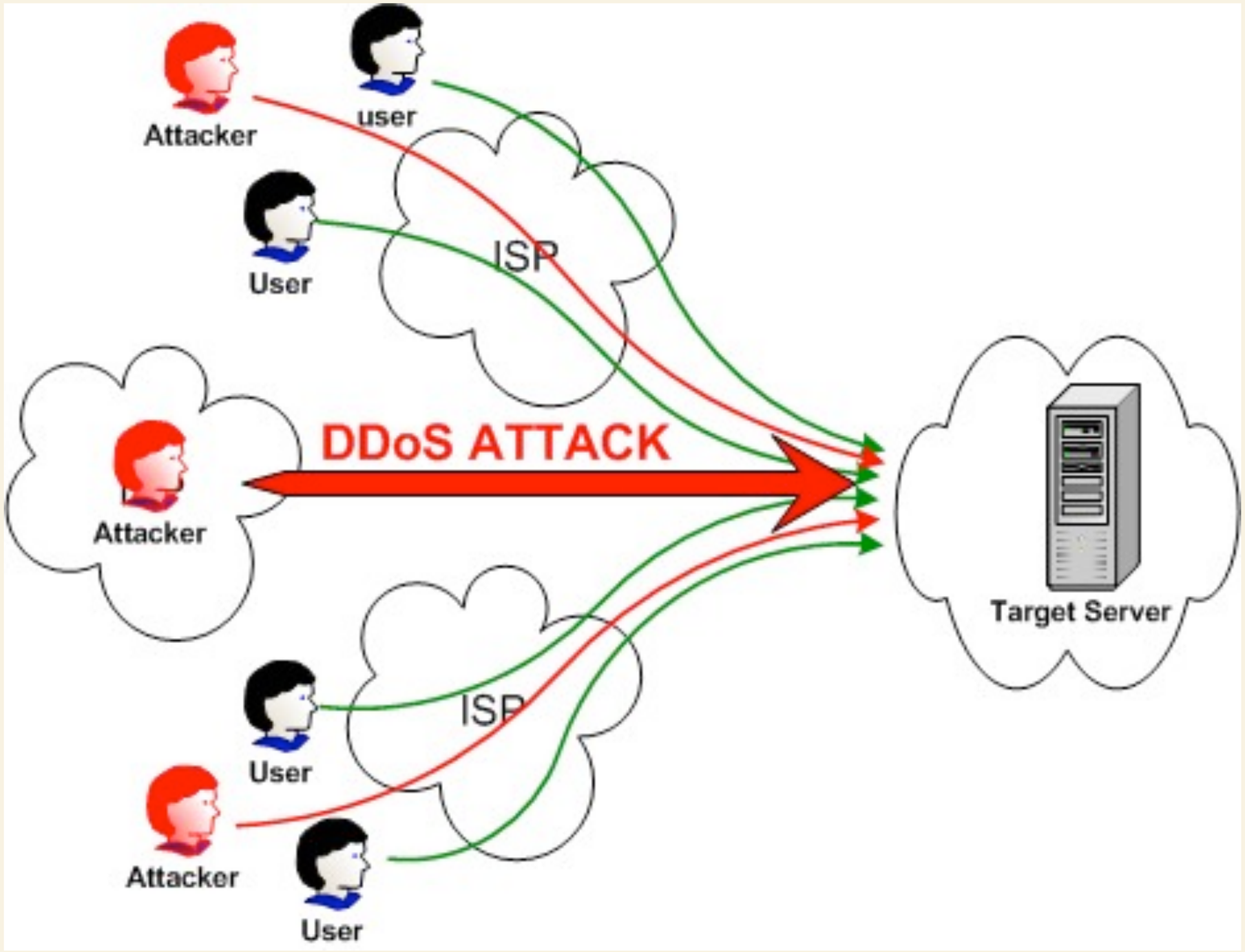
Blocking countries with GeoIP

```
loadmodule “geoip.so"

# ----- geoip params -----
modparam("geoip", "path", "/usr/local/share/GeoLiteCity.dat")

request_route {
…
    if(geoip_match("$si", “src”)) {
        xlog("SIP message from: $gip(src=>cc) \n”);
        if($gip(src=>cc) =~”DE|UK”) {
            send_reply(“403”, “Originating country not allowed”);
            exit;
        }
    } else {
        send_reply(“403”, “Unknown originating country not allowed”);
        exit;
    }
…
}
```

Block addresses due to high traffic rate



Block addresses due to high traffic

- *pike or pipelimit and htable modules — htable can be replaced by fail2ban*

```
#!ifdef WITH_ANTIFLOOD
loadmodule "htable.so"
loadmodule "pike.so"
#!endif

#!ifdef WITH_ANTIFLOOD
# ----- pike params -----
modparam("pike", "sampling_time_unit", 2)
modparam("pike", "reqs_density_per_unit", 16)
modparam("pike", "remove_latency", 4)

# ----- htable params -----
# ip ban htable with autoexpire after 5 minutes
modparam("htable", "htable", "ipban=>size=8;autoexpire=300;")
#!endif
```

```
# Per SIP request initial checks
route[REQINIT] {
#!ifdef WITH_ANTIFLOOD
        # flood dection from same IP and traffic ban for a while
        # be sure you exclude checking trusted peers, such as pstn gateways
        # - local host excluded (e.g., loop to self)
        if(src_ip!=myself) {
                if($sht(ipban=>$si)!=$null) {
                        # ip is already blocked
                        xdbg("request from blocked IP - $rm from $fu (IP:$si:$sp)\n");
                        exit;
                }
                if (!pike_check_req()) {
                        xlog("pike blocking $rm from $fu (IP:$si:$sp)\n");
                        $sht(ipban=>$si) = 1;
                        exit;
                }
        }
        if($ua =~ "friendly-scanner") {
                sl_send_reply("200", "OK");
                exit;
        }
#!endif
...
```

Block addresses due to high traffic

- *using pipelimit*

```
loadmodule "pipelimit.so"

# ----- pipelimit params -----
modparam("pipelimit", "timer_interval", 1)
modparam("pipelimit", "reply_code", 505)
modparam("pipelimit", "reply_reason", "CPS limit exceeded")
modparam("pipelimit", “db_url", DBURL)
modparam("pipelimit", "rlp_table_name", "traffic_limits")

request_route {
…
        $var(pipe) = “all-traffic”;
        if (!pl_check(“$var(pipe)")) {
                pl_drop();
                exit;
        }
…
}
```

Block too many failed authentications

```
route[AUTH] {
        if( $sht(userban=>$au::auth_count) >= 10 ) {
                $var(exp) = $Ts - 900;
                if($sht(userban=>$au::last_auth) > $var(exp)) {
                        xlog("L_DBG", "auth - id[$mi] m[$rm] r[0] [$fu -> $ru ($tu)]: User blocked - IP: $si\n");
                        sl_send_reply("403", "Try later");
                        exit;
                } else {
                        $sht(userban=>$au::auth_count) = 0;
                }
        }
        if(!(is_present_hf("Authorization") || is_present_hf("Proxy-Authorization"))) {
                auth_challenge("$fd", "0");
                exit;
        }
        # authenticate requests
        if (!auth_check("$fd", "subscriber", "1")) {
                $var(auth_count) = $shtinc(userban=>$au::auth_count);
                if( $var(auth_count) >= 10 )
                        xlog("many failed auth in a row - [$rm] from <$fu> src ip: $si\n");
                $sht(userban=>$au::last_auth) = $Ts;
                auth_challenge("$fd", "0");
                exit;
        }
        $sht(userban=>$au::auth_count) = $null;
        # user authenticated - remove auth header
        if(!is_method("REGISTER|PUBLISH"))
                consume_credentials();
        xlog("L_INFO", "id[$mi] m[$rm] r[0] [$fu -> $ru ($tu)]: User $fu Authenticated Correctly\n");
        return;
}
```

Rules:

- allow 10 failed authentications
- block user for 15 minutes
- reset when authentication is ok
- could be combined with IP ban

Restrict number of active calls

- ***dialog***, *htable or sqlops modules*

```
$xavp(caller=>active_calls) = 1;
```

```
# active calls/dialog management
# execute route(DIALOG) inside route(RELAY) before t_relay()
route[DIALOG] {
    if (is_method("CANCEL")
                || (has_totag() && is_method("INVITE|BYE|ACK"))) {
        dlg_manage();
        return;
    }
    if (is_method("INVITE") && !has_totag() && !isflagset(FLT_ACALLS)) {
        if( $xavp(caller[0]=>active_calls) != $null
                && $xavp(caller[0]=>active_calls) > 0 ) {
            if(!get_profile_size("caller", "$fU@$fd", "$var(acsize)")) {
                send_reply("500", "No more active calls");
                exit;
            }
            if($var(acsize)>=$xavp(caller[0]=>active_calls)) {
                send_reply("403", "No more active calls");
                exit;
            }
            set_dlg_profile("caller", "$fU@$fd");
        }
        setflag(FLT_ACALLS);
        dlg_manage();
    }
}
```

Kamailio, Lua and MongoDB

- *track active calls and history, then rise alarms based on various rules*
- *it's all about caching data for a while and searching*
  - *initial request of dialog (new call)*
    - *check if active calls limit is reached, if yes, alert/reject*
    - *check if limit per day is reached, if yes, alert/reject*
  - *requests within dialog*
    - *remove from active calls*
- *Lua: flexible language and fast embedded interpreter in Kamailio*
- *MongoDB: fast storage, replication, easy access from many Kamailio instances as well as from web portal due to JSON documents*
- *tbd: watch the news …*

Kamailio and In-Memory MySQL

- *again: track active calls and history, then rise alarms based on various rules*
- *again: it's all about caching data for a while and searching*
- *four important events*
  - *a new call: initial INVITE*
  - *call is not answered: 300 or higher response code to initial INVITE (covers CANCEL)*
  - *call is answered: 200 ok to initial INVITE*
  - *call is terminated: BYE*

Kamailio and In-Memory MySQL

```
route[AC_ADDNEW] {
    # ---------------------------------
    # Insert active call and then relay
    # ---------------------------------
    # set mutex for counting active calls per user from database table
    if($au!=$null) lock("u-$au");
    route(AC_LIMIT);      # Check, if call is allowed
    sql_query("ca", "INSERT INTO active_calls (call_id, init_time, state, caller,"
        " callee, username) VALUES ('$ci', $Ts,'INITIAL', '$fU', '$rU', '$au')",
        "ra");
    # unlock the mutext for counting active calls per user from database table
    if($au!=$null) unlock("u-$au");

    return;
}
```

Kamailio and In-Memory MySQL

```
route[AC_LIMIT] {
    # ---------------------------------------------------------------
    # Get the number of active calls on destination route and caller id
    # ---------------------------------------------------------------
    if(is_avp_set("$avp(max_calls)"))
    {
        sql_query("ca", "SELECT username FROM active_calls WHERE"
            " username='$au'", "ra");
        if($dbr(ra=>rows)>=$avp(max_calls) && ($avp(max_calls)>0))
        {
            # - mutex set before calling this route
            if($au!=$null) unlock("u-$au");
            send_reply("403", "Too many calls");
            exit;
        }
    }
}
```

Kamailio and In-Memory MySQL

```
route[AC_RINGING] {
    # ---------------------------------
    # Update the state of active calls
    # ---------------------------------
    sql_query(“ca", "UPDATE active_calls SET state=‘RINGING'
          WHERE call_id='$ci' and start_time=0", "ra");
}
```

```
route[AC_ANSWERED] {
    # ---------------------------------
    # Update the state of active calls
    # ---------------------------------
    sql_query(“ca", "UPDATE active_calls SET state=‘ANSWERED',
          start_time=$var(time) WHERE call_id='$ci' and start_time=0", "ra");
}


route[AC_TOBILLING] {
    # ---------------------------------------------------------------------
    # Set active call-state to BILLING after normal call-clearing with BYE
    # ---------------------------------------------------------------------
    sql_query(“ca", "UPDATE active_calls SET state=‘BILLING',
          end_time=$Ts WHERE call_id='$ci'", "ra");
}
```

Kamailio and In-Memory MySQL

```
route[AC_CANCELED] {
    # ------------------------------------------------
    # Delete active calls from failure route or CANCEL
    # ------------------------------------------------
    sql_query(“ca", "UPDATE active_calls SET state='CANCEL', end_time=$Ts
          WHERE call_id='$ci'", "ra");
}
```

```
route[AC_CLEAN] {
    # ------------------------------------------------------
    # Detele uncleared active calls on timer after a while
    # ------------------------------------------------------
    sql_query("ca",
        "DELETE FROM active_calls WHERE start_time <$Ts - 28810",
        "ra");
}
```

Useful resources

- *http://www.kamailio.org/wiki/tutorials/security/kamailio-security*
- *http://kb.asipto.com/kamailio:usage:k31-sip-scanning-attack*
- *SIP Security Book:*
  - *http://eu.wiley.com/WileyCDA/WileyTitle/productCd-0470516364.html*
- *http://kb.asipto.com*
- *http://www.kamailio.org/wiki/*

http://www.kamailio.org/events/

KamailioWorld Channel on YouTube

https://www.youtube.com/channel/UCElq4JNTPd7bs2vbfAAYVJA

asipto

Fraunhofer FOKUS

sip:wise

sipgate

Fraunhofer Forum Berlin

Simwood

KAMAILIO WORLD
CONFERENCE & EXHIBITION
BERLIN, GERMANY, MAY 27-29, 2015

ngvoice

digium

matrix

tyntec

OBIHAI technology, inc.

vuc

core net dynamics
Build your own Professional Networks

VoiceTel

2600hz CLOUD TELECOM

pascom

Kamailio World ***2016***

Planning a Special Edition

Kamailio Project

15 YEARS OF DEVELOPMENT

2001-2016

from SER to Kamailio

www.kamailioworld.com

Thank you!

Questions?

Daniel-Constantin Mierla
Co-Founder Kamailio Project
www.asipto.com
@miconda