Kamailio SIP Server

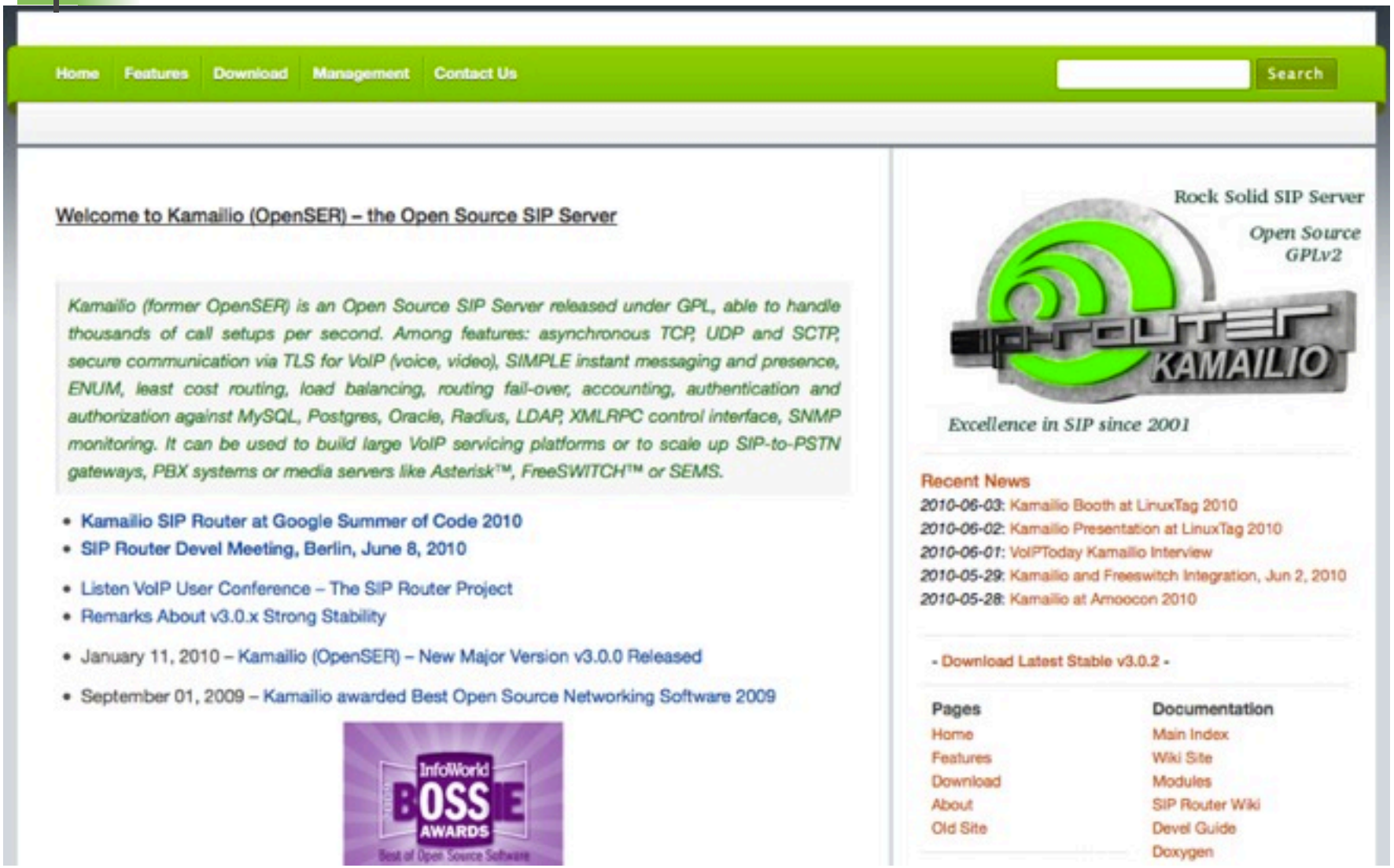
Secure Communication

Daniel-Constantin Mierla
Co-Founder

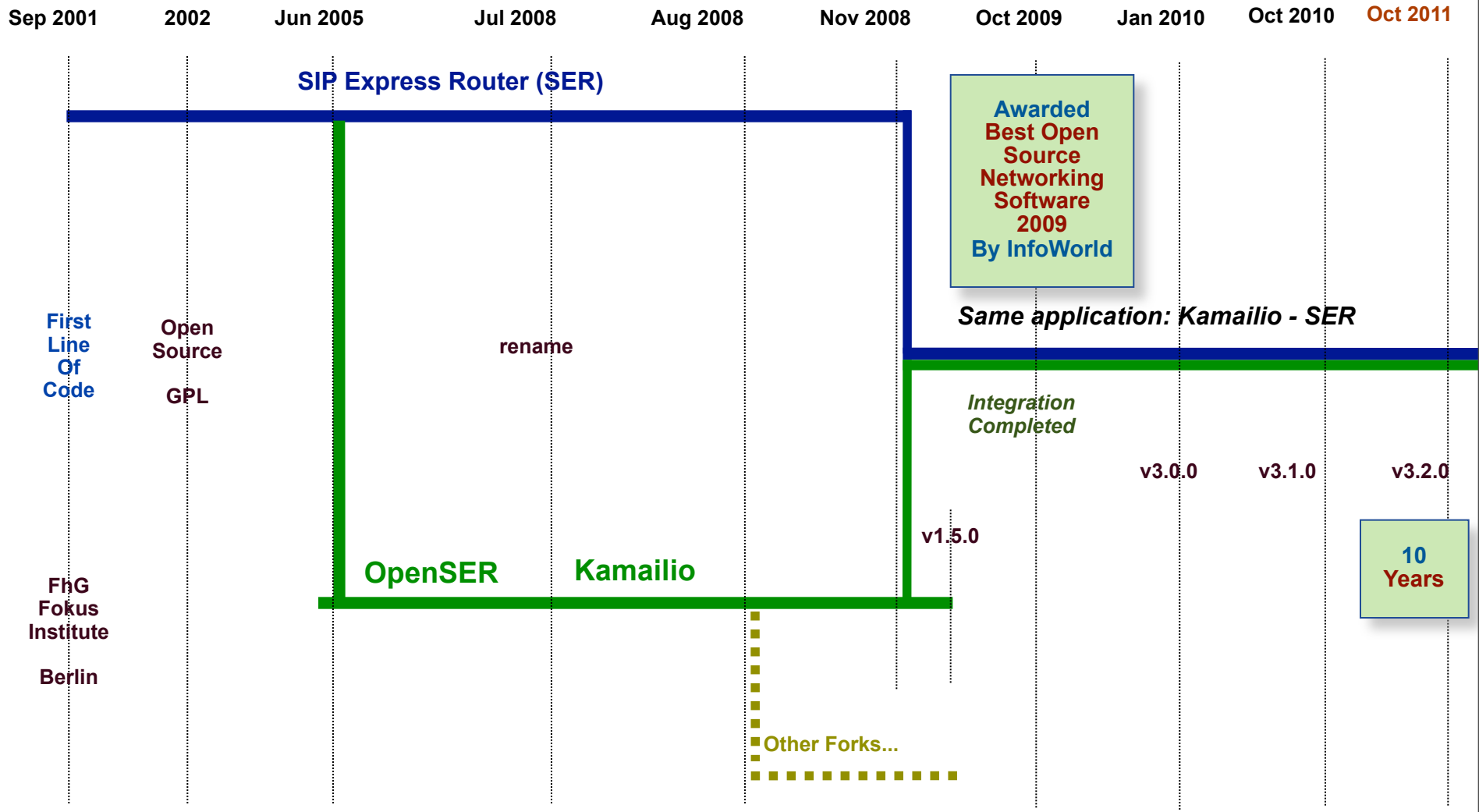
www.kamailio.org

www.asipto.com

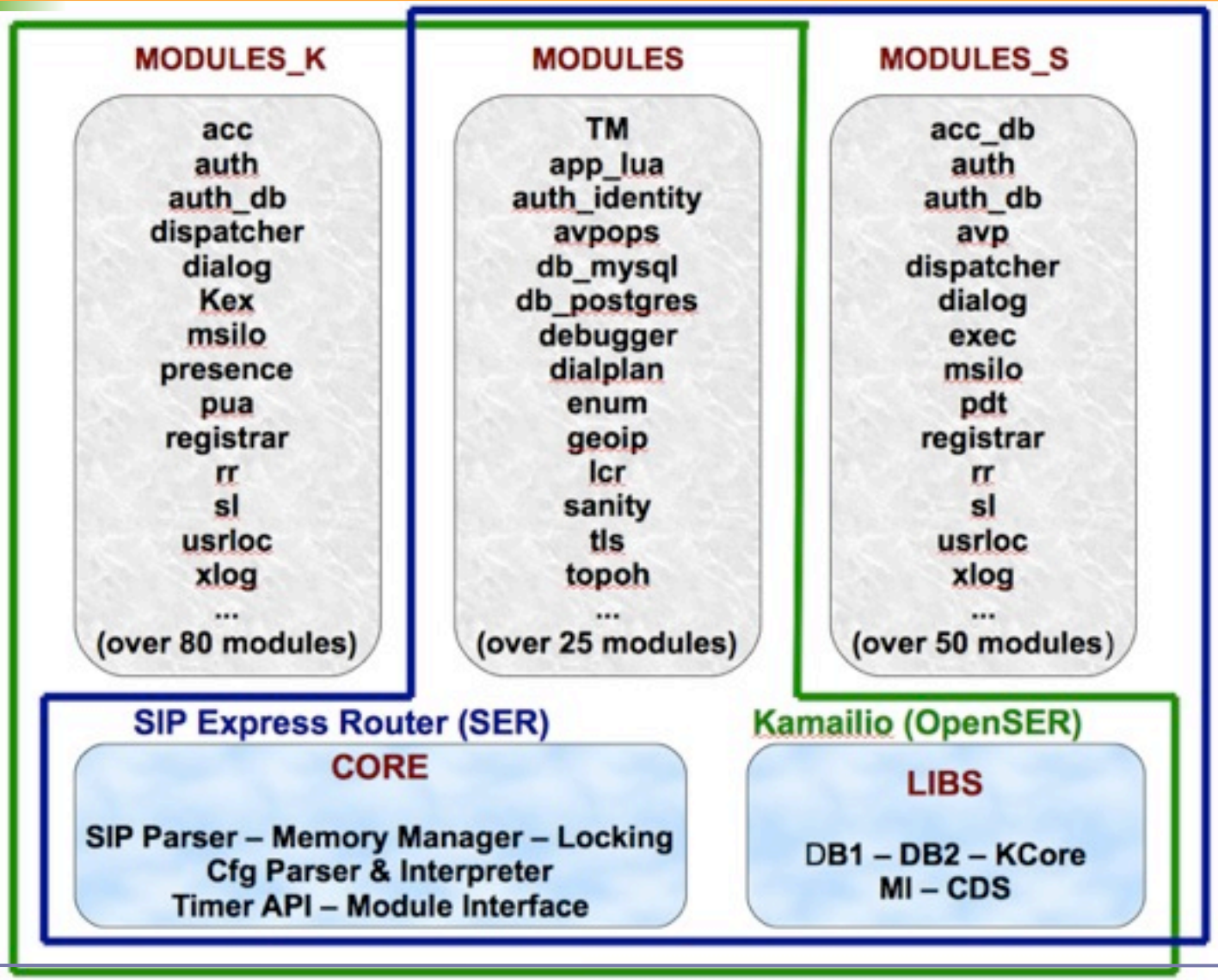
www.kamailio.org



History


Sep 2001
2002
Jun 2005
Jul 2008
Aug 2008
Nov 2008
Oct 2009
Jan 2010
Oct 2010
Oct 2011
SIP Express Router (SER)
Awarded Best Open Source Networking Software 2009 By InfoWorld
First Line Of Code
Open Source
GPL
rename
Same application: Kamailio - SER
Integration Completed
v3.0.0
v3.1.0
v3.2.0
v1.5.0
10 Years
FhG Fokus Institute
Berlin
OpenSER
Kamailio
Other Forks...

Kamailio & SER



State of the union

- Internal architecture refactored for v3.0.0
  - support asynchronous processing
    - TCP and TLS
    - SIP request handling
  - transaction management
  - internal libraries

Right now

- very stable core and main components
- ➡ toped with our well known scalability and flexibility
- safe framework for future development
- ➡ your work (extensions and deployments) is safe from now on for many years - there is no need to change the architecture again
- focus is on new features
- ➡ 3.x.x (and the next slides) show that

Scalability (info from public domain)

- services with millions of active subscribers
- ➡ 1&1 Germany (> 3M)
- services routing billions of call minutes per month
- ➡ might be the guy next to you (or pay attention tomorrow)

Stats

Kamailio and SIP Express Router

Main Language: C

Total Lines of Code: 489,210

Active Contributors: 39

Commit Activity Timeline:

5 year commit count

Updated Feb 04, 2012

Cocomo

Kamailio and SIP Express Router - Project Cost

Include	Avg. Salary
Markup And Code	$ 55000 /year
Codebase	**Effort (est.)**
635,457 Lines	171 Person Years
Estimated Cost	**$9,379,931**

Updated Feb 04, 2012 more at

Factoids

- Mostly written in C
- Mature, well-established codebase
- Very large, active development team

Kamailio and SIP Express Router, updated Feb 04, 2012 more at

Features

SIP Application Server
proxy, redirect, registrar, location

Plug in module interface
(over 150 mods)
Small footprint
Customizable routing policy

IPv4-IPv6
Asynchronous
UDP/TCP/TLS/SCTP
DNS NAPTR & SRV
DNS Failover and Load Balancing
DNS Internal Cache

Presence & IM Services
End-to-End
SIMPLE Server
RCS - RCS-e
Presence User Agent
Resource Lists
XCAP Client & Server
MSRP Relay

Carrier Routing
Dynamic Routng
ENUM lookup support
Advanced routing
(Load Balancing and LCR)
DID, Aliases & speeddial

Multi-domain support
LDAP/H.350 support
Embedded HTTP Server

Features

Embedded Lua, Perl
Python, C#
Java SIP Servlet
programming interface

No-SQL
Memcached
Redis
Cassandra

NAT traversal
Security
permissions
anti-DOS attacks
User call preferences
Call Processing
Language

Link any application to Kamailio using
FIFO/UNIXSOCK/DATAGRAM/XMLRPC interfaces

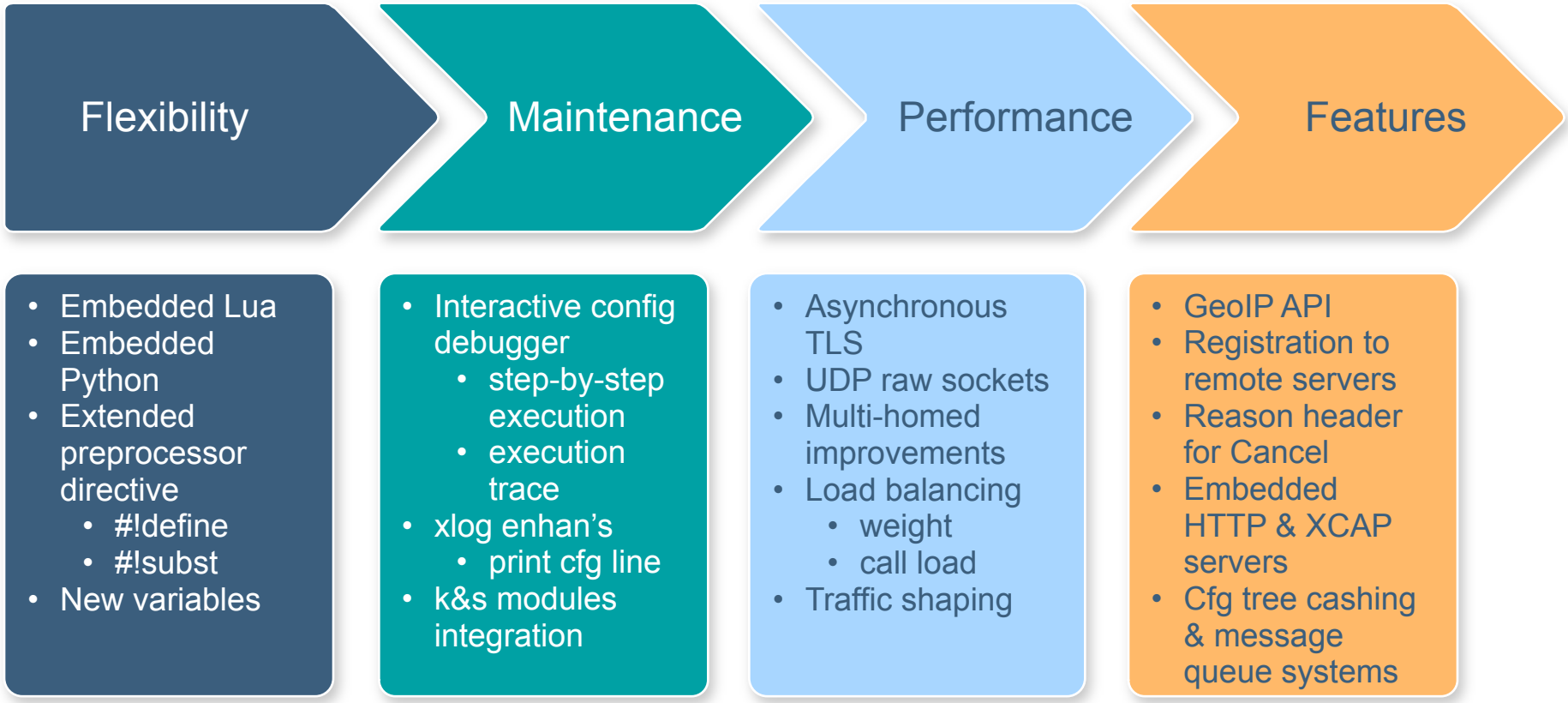
Database API
MySQL
PostgreSQL
SQLite
UNIXODBC
BERKELEYDB
ORACLE
Text files
RADIUS

Gateway

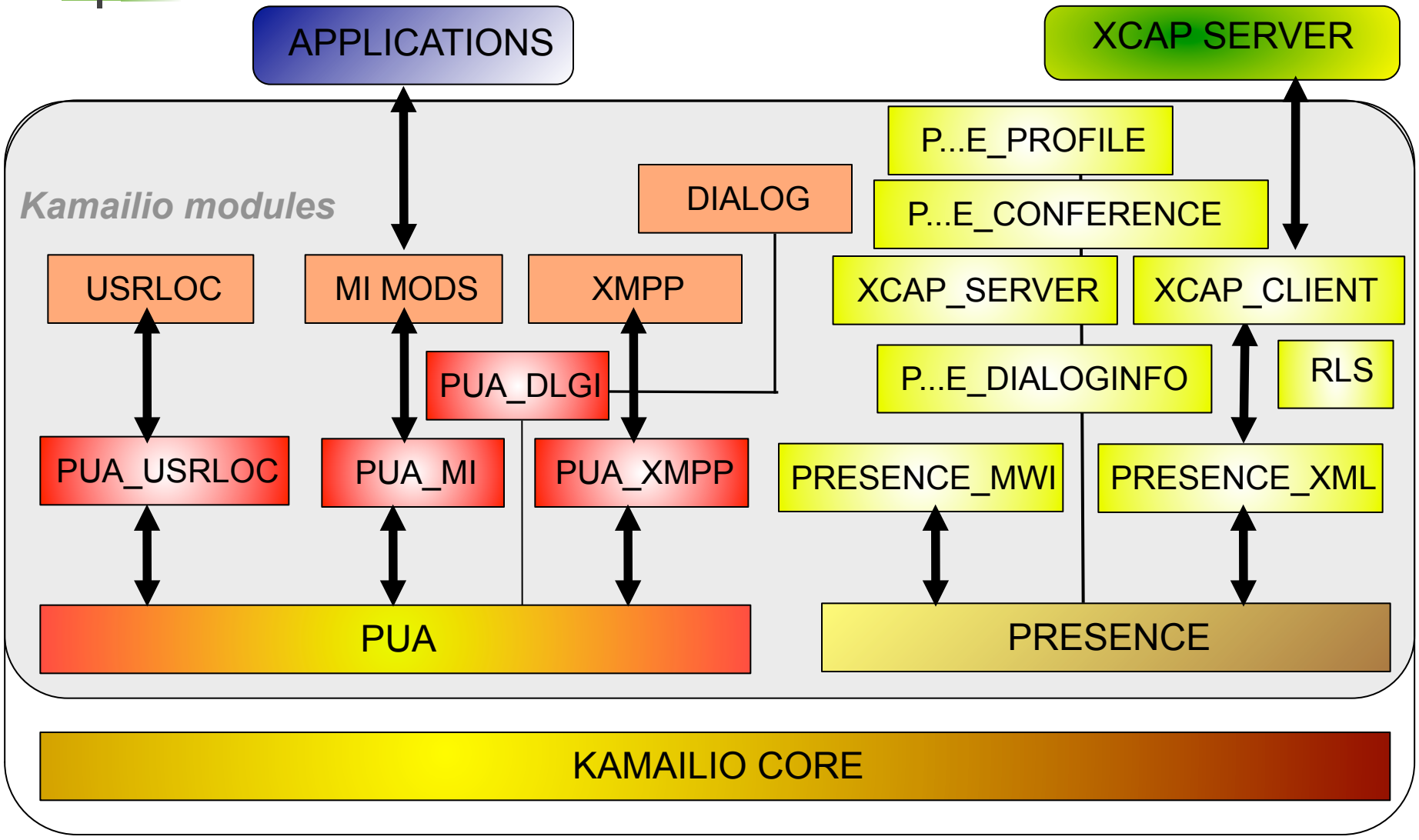
SMS
XMPP

Accounting through log file,
database or Radius/DIAMETER
servers

New in 3.1.0


Flexibility
Maintenance
Performance
Features
• Embedded Lua
• Embedded Python
• Extended preprocessor directive
  • #!define
  • #!subst
• New variables
• Interactive config debugger
  • step-by-step execution
  • execution trace
• xlog enhan's
  • print cfg line
• k&s modules integration
• Asynchronous TLS
• UDP raw sockets
• Multi-homed improvements
• Load balancing
  • weight
  • call load
• Traffic shaping
• GeoIP API
• Registration to remote servers
• Reason header for Cancel
• Embedded HTTP & XCAP servers
• Cfg tree cashing & message queue systems

SIP Beyond VoIP - Presence Services



New in 3.2.0 - *Oct 2011*

Reg-Info Implementation

RFC3860
pub-sub service for
location data

Embedded XCAP server

OMA - specs
If-Match cond

RLS

OMA specs
split NOTIFY bodies
XPath support within doc

Presence Server

data distribution across
many instances through
database

Presence User Agent

updates for latest
RL services

SQLite connector

use file based
database for
embedded
systems

Many native extensions to Lua

cfg routing logic all in Lua

Distributed Message Queue

Using SIP and Peer-to-Peer

New in 3.2.0

async module

run asynchronously parts of config file (route blocks)

Redis No-SQL

connector from config

Partitioned user location service

many nodes sharing location data

ipops module

a set of operations for handling IPv4/IPv6 addresses

New features in old parts

acc - write full CDR at once
dialog - attach extra attributes
core - more pre-processor directives
pv - new variables and transformations
tmx - export of async TM functions
sqlops - support for xavps
uac - enhancements to remote registration
siptrace - traffic replication enhancements
.....

sdpops module

SDP body management

JSON
JSONRPC

IMS Extensions
about 10 new modules (P-CSCF, I-CSCF, S-CSCF...)

New in 3.2.0

http://www.kamailio.org/w/kamailio-openser-v3-2-0-release-notes/

http://www.kamailio.org/wiki/features/new-in-3.2.x

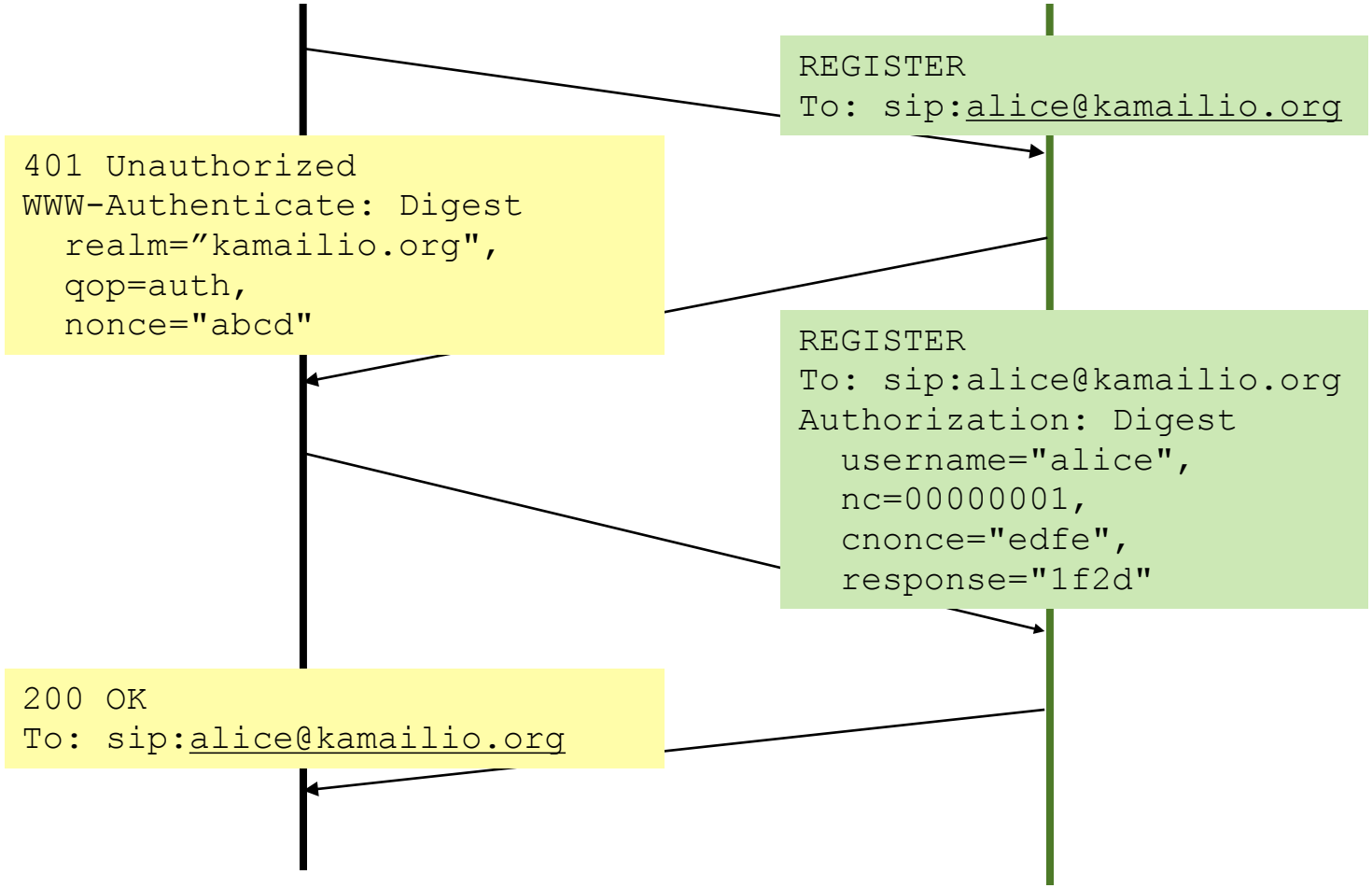
New in devel (3.3.0) - ***2012 before the summer***

- Enhancements to existing modules
  - auth, auth_db
  - rr, app_lua, tls, textops
  - dialog, dialplan
  - New in core - tls connections, fork delay, tcp buffer clone, socket workers, RPC commands
- New modules
  - xhttp_rpc - execute RPC commands via HTTP
  - presence_profile - get phone configuration via SIP Presence mechanisms
  - app_mono - embedded execution of managed code (C#)
  - db_cassandra - DB connector for Cassandra
  - msrp - embedded MSRP relay
  - tmrec - time based recurrence matching (RFC2445)
- http://www.kamailio.org/wiki/features/new-in-devel

Secure Communication

Authorization and Confidentiality

Digest authentication



Auth Modules

- **auth**
  - common frame for authentication
  - provides functionalities for auth challenge and nonce management
  - functions to do authentication taking password from a script variable
- **auth_db**
  - authentication check against database
- **auth_radius**
  - authentication check against a RADIUS server
- **auth_diameter**
  - authentication check against a DIAMETER server (alpha)

Auth modules – DB backend

- subscribers are stored in DB - table **subscriber**
- password may be store in plain text (insecure) or in a pre-computed format (HA1)

```
modparam("auth_db", "password_column", "password")
```

versus

```
modparam("auth_db", "calculate_ha1", 1)
modparam("auth_db", "password_column", "ha1")
```

- authentication means checking the user profile (password) in DB and. in most scenarios, we need more than only the password:
  - Kamailio provides a mechanism to configure a custom set of attributes to be loaded from DB during the authentication process
  - advantage: reduce the number of DB hits

```
modparam("auth_db", "load_credentials",
                "$avp(i:12)=rpid; $avp(i:14)=email_address")
```

Auth modules – DB backend

- `www_challenge(realm, qop)`
- `proxy_challenge(realm, qop)`
- `www_authorize(realm, table)`
- `proxy_authorize(realm, table)`

```
...
if (www_authorize("kamailio.org", "subscriber")) {
        www_challenge("kamailio.org", "1");
        exit;
};
...
```

```
...
if (!proxy_authorize("$fd", "subscriber")) {
        proxy_challenge("$fd", "1");
        exit;
};
...
```

Auth modules – DB backend

```
mysql> select * from subscriber;
+----+----------+--------------+----------+---------------+----------------------------------
| id | username | domain       | password | email_address | ha1
+----+----------+--------------+----------+---------------+----------------------------------
|  1 | 101      | kamailio.org | 101      |               | 38cf5979c2cf97258016bdfe036e5968
|  2 | 102      | kamailio.org | 102      |               | ab7d1e902521ac605f4143161f1de59d
|  3 | 103      | kamailio.org | 103      |               | f447a36d68b2dd05b1aaa8b0876c461a
+----+----------+--------------+----------+---------------+----------------------------------
```

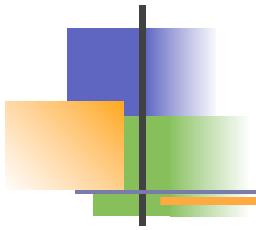
```
+----------------------------------+------+
| ha1b                             | rpid |
+----------------------------------+------+
| 0f075cdb8bd8ed0d4fb00e5d83e84da1 | NULL |
| b3eb7619ddefbcbfef98f19868615124 | NULL |
| 2a878ac26b5c14b0c486cf91a8466479 | NULL |
+----------------------------------+------+
```

Manage users with kamctl:

- add, remove, change password

 # kamctl add user@domain.com passwd

AAA
Authorization



Authorization

- AUTHENTICATION
  - I know now who you are...

- AUTHORIZATION
  - What are you allowed to do?
  - access control list

Authorization

- help implementing authorization mechanisms
- it is very important to be fast and reliable, being the way to allow the access to resources in the system
- have in mind the provisioning system, ACL update should apply in real-time
- having a well-designed ACL system can be extended to be used as a user capability list

- Kamailio capabilities for ACLs
  - group membership
  - binary acl
  - string acl
  - custom acl

Authorization - group

```
mysql> select * from grp;
+----+----------+-------------+---------------+---------------------+
| id | username | domain      | grp           | last_modified       |
+----+----------+-------------+---------------+---------------------+
|  1 | 101      | kamailio.org | international | 2011-02-19 09:37:22 |
|  2 | 102      | kamailio.org | international | 2011-02-19 09:37:31 |
|  3 | 103      | kamailio.org | international | 2011-02-19 09:37:56 |
+----+----------+-------------+---------------+---------------------+
```

Manage users' group ACL with kamctl:

- grant, revoke, show

 # kamctl acl grant user@domain.com groupid

Authorization - group

- example of usage: group module with SQL backend

```
loadmodule “group.so”
modparam("group", "db_url","mysql://openser:openserrw@localhost/openser")
....
if (method=="INVITE") {
    if (uri=~"sip:00[1-9][0-9]+@.*") {
        if (!is_user_in("From", "international")) {
            sl_send_reply("403", "No permission for international calls");
            exit;
        }
    }
}
```

AAA
IP Authorization

IP Auth - Config

```
if(src_ip==10.1.1.10)
{
    # deny traffic from this ip
    sl_send_reply("403", "Forbiden");
    exit;
}
```

```
if(src_ip==10.1.1.0/24)
{
    # deny traffic from this network
    sl_send_reply("403", "Forbiden");
    exit;
}
```

```
if($si=="10.1.1.10")
{
    # deny traffic from this ip
    sl_send_reply("403", "Forbiden");
    exit;
}
```

```
$var(myip) = "10.1.1.10";
if($si==$var(myip))
{
    # deny traffic from this ip
    sl_send_reply("403", "Forbiden");
    exit;
}
```

IP Auth - Permissions - by address

```
grp = 1
ip_addr = 192.168.0.1
mask = 32
port = 5060
```

```
if(!allow_source_address("1")) {
    # not matching
    sl_send_reply("403", "Forbidden");
    exit;
}
```

```
grp = 1
ip_addr = 192.168.0.0
mask = 24
port = 0
```

```
# $var(ip) = $dd;
# $var(ip) = "10.1.1.10";
if(!allow_address("1", "$var(ip)", "0")) {
    # not matching
    sl_send_reply("403", "Forbidden");
    exit;
}
```

Security

Encrypted Transmission

TLS and Kamailio

- Dependencies
  - openssl, libssl
  - openssl-dev, libssl-dev
- Completely re-factored since v3.0.0
  - scalability
  - simplified installation
  - flexible configuration (modparams or own config file)
  - asynchronous communication
- Kamailio Config Requirementents
  - compile and install TLS module
  - load TLS module
    - loadmodule "tls.so"
  - enable tls in config
    - disable_tls=0
    - listen=tls:10.0.0.1:5061
  - *default config file -- add:* #!define WITH_TLS

TLS Config

- Config by module parameters
  - set tls attributes via modparam
  - tls method (sslv1, sslv2, tlsv1), ciphers list, certificates, timeouts, ...

```
...
loadmodule "tls.so"

modparam("tls", "private_key", "/etc/kamailio/kamailio-selfsigned.key")
modparam("tls", "certificate", "/etc/kamailio/kamailio-selfsigned.pem")
modparam("tls", "ca_list", "/etc/kamailio/calist.pem")
```

TLS Config

- Config by .ini-like file
  - dedicated file which can contain tls attributes
  - can include config for more than one server
  - can include config specific for clients

```
...
modparam("tls", "config", "/etc/kamailio/tls.cfg")
...
```

```
[server:default]
method = TLSv1
verify_certificate = no
require_certificate = no
private_key = default_key.pem
certificate = default_cert.pem
ca_list = default_ca.pem
```

TLS module

```
xlog("L_INFO","$$tls_version                    = '$tls_version'\n");
xlog("L_INFO","$$tls_description                = '$tls_description'\n");
xlog("L_INFO","$$tls_cipher_info                = '$tls_cipher_info'\n");
xlog("L_INFO","$$tls_cipher_bits                = '$tls_cipher_bits'\n");
xlog("L_INFO","$$tls_peer_subject               = '$tls_peer_subject'\n");
xlog("L_INFO","$$tls_peer_issuer                = '$tls_peer_issuer'\n");
xlog("L_INFO","$$tls_my_subject                 = '$tls_my_subject'\n");
xlog("L_INFO","$$tls_my_issuer                  = '$tls_my_issuer'\n");
xlog("L_INFO","$$tls_peer_version               = '$tls_peer_version'\n");
xlog("L_INFO","$$tls_my_version                 = '$tls_my_version'\n");
xlog("L_INFO","$$tls_peer_serial                = '$tls_peer_serial'\n");
xlog("L_INFO","$$tls_my_serial                  = '$tls_my_serial'\n");
xlog("L_INFO","$$tls_peer_subject_cn            = '$tls_peer_subject_cn'\n");
xlog("L_INFO","$$tls_peer_issuer_cn             = '$tls_peer_issuer_cn'\n");
xlog("L_INFO","$$tls_my_subject_cn              = '$tls_my_subject_cn'\n");
xlog("L_INFO","$$tls_my_issuer_cn               = '$tls_my_issuer_cn'\n");
```

TLS Routing with Kamailio

- Nothing special to do when destination address is over TLS
  - t_relay() detects the destination transport layer and uses appropriate outgoing socket
- Dedicated functions to enforce TLS transport layer
  - t_relay_to_tls(address, port);
  - t_relay_to(“tls:address:port);
- Checking if request was coming via TLS
  - if(proto==TLS) { ... }
- Checking if the request is going out via TLS
  - in: onsend_route { ... if($snd(proto)==3 { ...} ... }

Out there

- TLS Tutorial - The README for TLS Module
  - http://kamailio.org/docs/modules/stable/modules/tls.html

GREEN VoIP Research Project at Columbia University

Some interesting results:

- one instance of SIP server with *500 000 online users* (mixed users – behind and not NAT routers) – consumed energy *210W*
- one instance of SIP server with *1 000 000 online users* (no NAT involved) – consumed energy *190W*
- on a 32-bit machine with 4GB of memory and with 2.5GB reserved for SIP server, the server could support *43 000 simultaneous TLS connections* – consumed energy *209W*

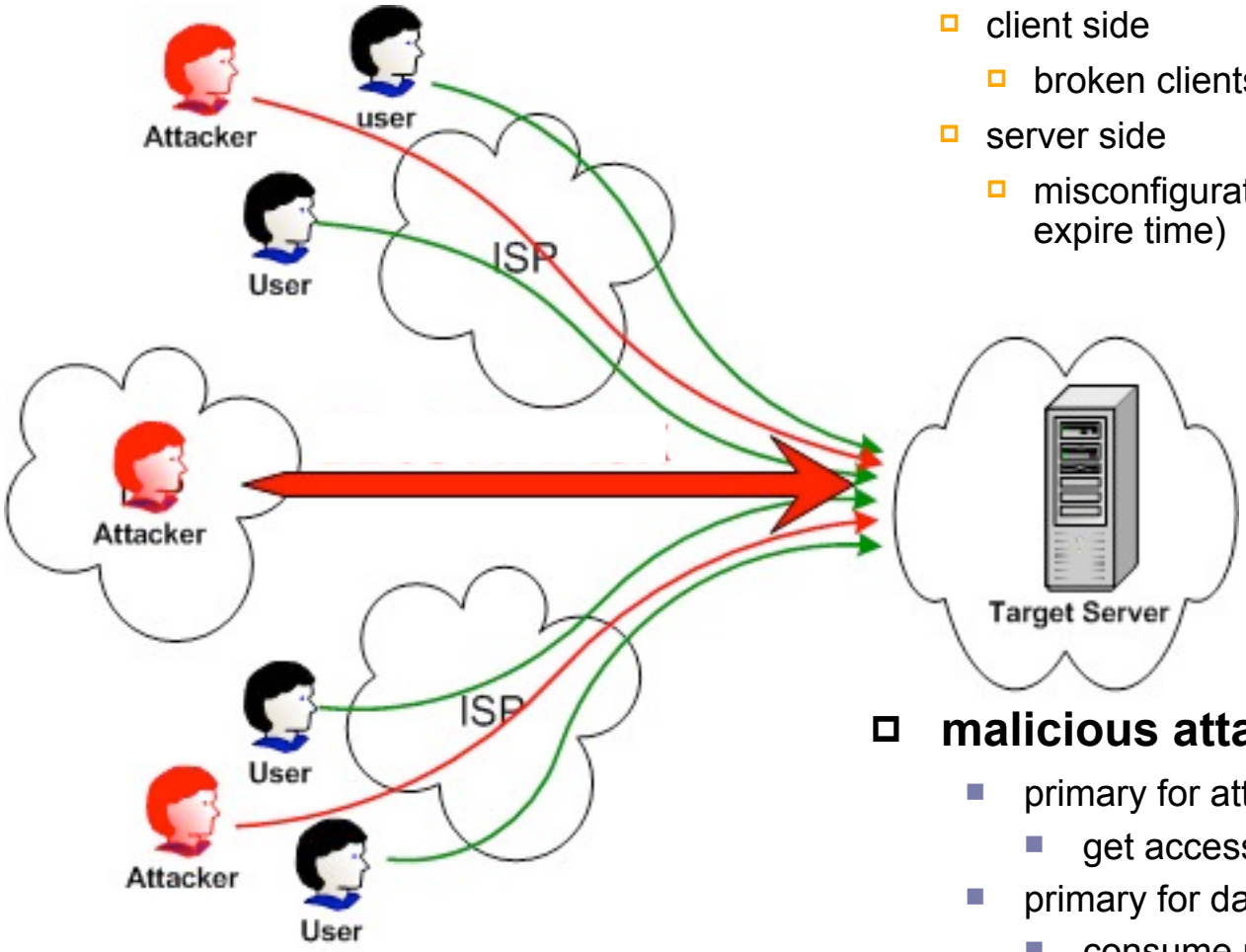
http://www.kamailio.org/w/2011/05/green-voip-energy-efficiency-and-performaces-of-v3-0/

Security

Flood detection

Brute force attacks

DoS Attacks



- **involuntary attacks**
  - client side
    - broken clients
  - server side
    - misconfigurations (e.g., too low max expire time)

- bandwidth
- cpu
- memory

- **malicious attacks**
  - primary for attacker benefits
    - get access to the host and call for free
  - primary for damages on target
    - consume resources on target

Pike

- **PIKE** module
  - keeps track of all or selected incoming request's IP source
- blocks the ones that exceeded the threshold
- support for IPv4 and IPv6 addresses
- use it at top of your cofig file
  - initial checks
- no internal actions for blocking
  - reports that the there is an high traffic from an IP
    - is the administrator decision in the config file
      - drop silently
      - send stateless reply

Pike Config

```
# -- pike params --
modparam("pike", "sampling_time_unit", 2)
modparam("pike", "reqs_density_per_unit", 32)
modparam("pike", "remove_latency", 4)
```

```
if((src_ip != 192.168.1.25)
            && !pike_check_req()) {
    xlog("pike filter: $rm from $fu (IP:$si:$sp)\n");
    exit;
}
```

Brute force attack

- **HTABLE** module
  - generic cache system

- track failed authentication
- forbid new attempts if a threshold is reached in a certain period of time - 3 failed authentication in a raw, block for 15min
- send alerts to admin, etc.

- example with registrations
  - prevent discovery of user passwords
  - detect mistyped passwords

Brute force attack

```
...
modparam("htable", "htable", "a=>size=8;")
...
if(is_present_hf("Authorization"))
{
    if($sht(a=>$au::auth_count)==3)
    {
                $var(exp) = $Ts - 900;
        if($sht(a=>$au::last_auth) > $var(exp))
        {
            sl_send_reply("403", "Try later");
            exit;
        } else {
            $sht(a=>$au::auth_count) = 0;
        }
    }
```

```
    if(!www_authenticate("$td", "subscriber"))
    {
        switch ($retcode) {
            case -1:
                sl_send_reply("403", "Forbidden");
            exit;
            case -2:
                if($sht(a=>$au::auth_count) == null)
                    $sht(a=>$au::auth_count) = 0;
                $sht(a=>$au::auth_count) = $sht(a=>$au::auth_count) + 1;
                if($sht(a=>$au::auth_count) == 3)
                    xlog("auth failed 3rd time - src ip: $si\n");
                $sht(a=>$au::last_auth) = $Ts;
            break;
        }
        www_challenge("$td"/*realm*/,"0"/*qop*/);
        exit;
    }
    $sht(a=>$au::auth_count) = 0;
} else {
    www_challenge("$td","0");
    exit;
}
...
```

Out there

- Online Tutorial
  - *Scanning Attacks => IP Banning*
    - *block rule in config*
    - *block rule in firewall - fail2ban*
  - *(friendly scanner anyone?!?!)*

- http://kb.asipto.com/kamailio:usage:k31-sip-scanning-attack

Security

Topology hiding

Topology hiding

- **goals**
  - hide sensitive IP addresses
    - contact header
    - Via stack
    - Record-Route and Route stacks
- **design**
  - stateless processing
    - no track of transactions or dialogs
  - distributed processing
    - encoding/decoding can be done by different servers
  - transparent processing
    - config writer should not care about topology hiding
    - everything is in clear while config processing

Topology hiding

- **TOPOH** module

- secret key to encode/decode
- encoded fields are SIP grammar valid
- encoding IP and prefixes can be set via parameters
- survive restarts
- no functions to be called in config file
  - everything is done automatically
  - hooks in core after receiving and before sending
  - just load the module and adjust parameters

- *use it with a media relay to hide the source of media traffic*

Topology hiding - config file

```
...
loadmodule "topoh.so"
...
# ----- topoh params -----
modparam("topoh", "mask_key", "my secret here")
modparam("topoh", "mask_ip", "10.1.1.10")
...
```

Topology hiding - INVITE in

U 2011/02/18 20:09:05.622472 192.168.178.27:40416 -> 192.168.178.26:5060
INVITE sip:101@192.168.178.26 SIP/2.0.
Via: SIP/2.0/UDP 192.168.178.27:40416;branch=z9hG4bK321149767.
From: "105" <sip:105@192.168.178.26>;tag=166646806.
To: <sip:101@192.168.178.26>.
Call-ID: 989804978-40416-6@BJC.BGI.BHI.CH.
CSeq: 50 INVITE.
Contact: "105" <sip:105@192.168.178.27:40416>.
Max-Forwards: 70.
User-Agent: Grandstream GXV3140 1.0.7.3.
Privacy: none.
P-Preferred-Identity: "105" <sip:105@192.168.178.26>.
Supported: replaces, path, timer.
Allow: INVITE, ACK, OPTIONS, CANCEL, BYE, SUBSCRIBE, NOTIFY, INFO, REFER, UPDATE, MESSAGE.
Content-Type: application/sdp.
Accept: application/sdp, application/dtmf-relay.
Content-Length: 483.
.

Topology hiding - INVITE out

U 2011/02/18 20:09:05.628883 192.168.178.26:5060 -> 192.168.178.22:1056
INVITE sip:101@192.168.178.22:1056;line=mu3z2i1j SIP/2.0.
Record-Route: <sip:192.168.178.26;lr=on>.
Via: SIP/2.0/UDP 192.168.178.26;branch=z9hG4bK8d21.062561f6.0.
Via: SIP/2.0/UDP 10.1.1.10;branch=z9hG4bKsr-JfymiMenCtp4urS5CX1ZiHvRItc.TM5nCHOBT6SfCXN94v5pswyRIRDZN80HU6gBI8LqTwDiCMe.CXm0TMNP.
From: "105" <sip:105@192.168.178.26>;tag=166646806.
To: <sip:101@192.168.178.26>.
Call-ID: 989804978-40416-6@BJC.BGI.BHI.CH.
CSeq: 50 INVITE.
Contact: "105" <sip:10.1.1.10;line=sr-ORylIHvlTJS.IXenCXNciHvPItcZTMWfC6m.T5**>.
Max-Forwards: 69.
User-Agent: Grandstream GXV3140 1.0.7.3.
Privacy: none.
P-Preferred-Identity: "105" <sip:105@192.168.178.26>.
Supported: replaces, path, timer.
Allow: INVITE, ACK, OPTIONS, CANCEL, BYE, SUBSCRIBE, NOTIFY, INFO, REFER, UPDATE, MESSAGE.
Content-Type: application/sdp.
Accept: application/sdp, application/dtmf-relay.
Content-Length: 483.
.

Questions?

Contact

- Daniel-Constantin Mierla
  - twitter: miconda
  - http://linkedin.com/in/miconda
  - daniel@asipto.com
  - http://www.asipto.com
  - http://www.kamailio.org