VIPR

draft-petithuguenin-vipr-proportional-quota-00
draft-petithuguenin-vipr-reload-usage-03
draft-petithuguenin-vipr-sip-antispam-03
draft-petithuguenin-dispatch-infrastructure-overlay-01

Marc Petit-Huguenin
11/17/2011

The story so far...

We made some progresses on the VIPR, but not as much as would have been expected:

- A skeleton draft-petithuguenin-vipr-framework document was released, but too many issues were discovered to produce a meaningful document.
- The Design Team started working on issues in late September.
- There is still a huge amount of issues to think about.

Design Team

A design team was assembled to work on the issues, and had a conference call each week, starting 9/23/2011.

- Mary Barnes
- Daryl Malas
- Hakim Mehmood
- Muthu Arul Mozhi Perumal
- Jon Peterson
- Marc Petit-Huguenin
- Michael Procter
- John Ward

Many thanks to the team members for their help.

Framework document

The framework document is a new document that is made of the section that were removed from the -overview draft and from part of the -vap draft.

At the difference of the existing drafts, -framework does not assume a specific architecture, but present the VIPR protocols in a way that permit to use them in a spectrum of architectures, from an VIPR enabled device to an architecture where VIPR servers are distributed on multiple datacenters around the world.

Still too many issues to publish it.

PVP methods template

One thing that will be in the -framework document is the template for the IANA registration of new PVP methods.

Because we expect to have many PVP methods registered, a priority is associated with each method, so a PVP client tries them in a specific order.

SIP Intermediaries

The VIPR documents assume that each VIPR domain have a direct connection to the PSTN.

But in reality, enterprises uses SIP trunks, and it is not possible to prevent the provider managing the SIP trunks to also be a VIPR domain. This is what is called a SIP intermediary.

The problem is complex, so we decided to work on it later. A document containing the 3 problems created by SIP intermediaries was created: draft-petithuguenin-vipr-sip-intermediaries.

Proportional Quota

Following discussions in Quebec City, our ADs asked to move back this document in the VIPR WG.

The algorithm no longer applies to replicas, because topology changes could discard resources records (Thanks to Cisco's developers for the explanations)

The probability equation is still missing.

RELOAD Usage: Supported methods

We expect to see many new PVP methods registered, but this will create a problem for the PVP client, that will have to try all of them.

Instead the E.164 number registration in the RELOAD overlay now contains the list of PVP methods to try.

This permits to use new methods for devices that have a PSTN connection not currently supported.

This permits also to collect statistics on popular methods.

RELOAD Usage: No additional copies

Following the discussion in Quebec City and subsequent discussions in VIPR, we removed the additional copies in the RELOAD overlay.

When retrieving a VIPR-REGISTRATION record, the PVP client must also retrieve the two replicas, and use the value that is found at least 2 times.

RELOAD Usage: Multiplier

When the probability equation in -proportional-quota will be finalized, we will be able to put a recommendation on the value to use for the multiplier.

PVP: Vocabulary

The PVP selector is a set of parameters that is used to select a VCR on the PVP server side. This is always sent in clear. (e.g. Callee, Caller-ID, Time in middle of call)

The PVP secret is a piece of information that is verified by a zero-knowledge proof. It cannot be discovered if the PVP transaction fails. (e.g. start/stop time)

The PVP parameters are additional parameters sent to help the process. They are always sent in clear. (e.g. rounding, vservice id)

PVP: Hashing the Caller-ID for method “a”

The attack is described in draft-procter-vipr-privacy-concerns, and was discussed in Quebec City.

The Caller-ID in method “a” is now hashed with bcrypt. The number of rounds is part of the hash, so the complexity can be increase as hardware become faster.

The salt is also part of the hash string, so all VCRs matching the callee number need to be rehashed with the salt and number of rounds.

The minimal and default rounds will be part of the configuration.

PVP: Inverting the secret and selector

The idea is using the start/stop time of the call as PVP selector, and the callee/Caller-ID as secret.

Still need some work. Jon Peterson was suggesting to add the phone number prefix in the selector.

PVP: Method entropy

Some methods, like method “b” are probably not secure enough. The idea is that more than one call using this method would be needed before granting a SIP route and a ticket.

First solution is to not care about entropy and to either fail or give a SIP route and ticket back.

Second solution is to have a mechanism to accumulate entropy, but to do it in the PVP side.

Third solution is to add a field in the Ticket to store the accumulated entropy, so the PVP server does not have to store data for each call.

PVP: Ticket vs Certificate

The PVP ticket is a signature made with a secret key over the phone number, domain, ticket validity, etc...

The problems are that it uses a symmetrical key, lacks algorithm agility, and does not have an existing library to generate/verify it.

The proposal is to replace it by an X.509 certificate that can use RSA keys, has algorithm agility and can be generated and verified by existing and proven libraries.

SIP Antispam: Ticket renewal

Ticket expires but if having the first call using the PSTN could be acceptable, asking the end-user to periodically give up video and other advanced features simply for the purpose of renewing the Ticket is unacceptable.

The solution uses draft-ietf-mmusic-sdp-cs, which is a way to initiate a PSTN call from a SIP INVITE. The audio flows over both paths, on the Internet because we want to keep the possibility to use a wideband codec, but also on the PSTN because we need the audio for future PVP methods like fingerprinting.

This renewal method is compatible with the existing PVP mechanism, and can be used transparently.

Infrastructure Overlay

There is a whole set of issues that need to be discussed on the deployment of VIPR. One of them is the fact that VIPR will be a failure if we cannot enforce the usage of one and only one RELOAD overlay to store the phone numbers.

An Infrastructure Overlay is a RELOAD overlay that is deployed in a way that guarantees that it is unique. The draft-petithuguenin-dispatch-infrastructure-overlay document listing the requirements was submitted to DISPATCH for comments.

VIPR Troubleshooting

VIPR provisions SIP routes automatically, so there is no way to do an interop test before a SIP call is tried.

Because of this, we need tools that will permit to debug problems after failed call. But having for example the local SIPCLF logs is generally not enough, as the remote logs are also generally needed.

So we need to work on ways to provide logs, pcap files and other debugging information in a way that is secure and respect privacy.

ICE Support in RELOAD

The RELOAD overlay for VIPR can require ICE support or not.

No-ICE makes things a little bit simpler to deploy and debug, but all the RELOAD peers has to be on the Internet or in a DMZ. On the other hand, it will not be possible to have VIPR-enabled devices, where the RELOAD node is directly embedded in the device.

With ICE, all peers excepted for the bootstrap servers can be behind a firewall. Also ICE mandates to also deploy TURN servers, which can be used to further anonymize the PVP transactions.

If No-ICE is selected, it could be a good idea to mandate SCTP as the link-layer transport for RELOAD.