Семь простых шагов по укреплению SIP безопасности на Астериск

1. Не разрешайте SIP аутентификацию со ВСЕХ ИП адресов. Используйте опции “permit=” и “deny=” в sip.conf как в глобальной секции, так и в параметрах пиров. Разрешайте только ожидаемые диапазоны ИП адресов. Даже если принимаете входящие "отовсюду" (через контекст [default]) не забывайте об аутентификации!

2. Укажите “alwaysauthreject=yes” в глобальной секции файла sip.conf. Эта опция доступна давно (уже с версии 1.2?) но по дефолту она в “no”, что позволяет получить информацию о внутренних номерах даже при неудавшейся регистрации. Устанавливая этот паратметр в “yes” мы отправляем такой же "reject" для существующего внутреннего номера, как и в случае несуществующего. Это уменьшает возможности удалённых хакеров получить список номеров, по которым уже начинается атака по подбору паролей методом brute force.

3. Используйте СЛОЖНЫЕ пароли для всех SIP пиров и юзеров. Это возможно наиболее важный шаг, который вы можете предпринять. Не используйте последовательно два одинаковых слова,разделите их хоть "1". Если бы вы видели инструменты по подбору паролей вы бы поняли смысл этой казалось бы простой рекомендации, так как такое задваивание является ничтожной помехой для современных процессоров. Используйте символы, цифры и буквы обеих регистров длиной не менее 12 знаков.

4. Блокируйте доступ к порту AMI. Используйте “permit=” и “deny=” параметры в manager.conf чтобы сократить число возможных подключений только с доверенных хостов. Используйте сложные пароли минимум из 12-ти знаков в различных сочетаниях символов, цифр и букв разного регистра.

5. Разрешайте только один или два одновременных вызова с каждого внутреннего SIP абонента, если возможно. В любом случае любые ограничения против мошенников являются мудрым шагом. Не допускайте разрешённым пользователям, которые имеют доступ к настройкам, хранить пароли в обозреваемом месте (например записаные снизу на телефоне).

6. Делайте SIP usernames отличными от внутренних номеров. Обычно внутренний номер “1234” соответствует SIP пиру “1234”, который имеет аналогично SIP user “1234”, это лёгкая цель для хакеров в попытке угадать аутентифицированые SIP names. Используйте MAC адреса устройств или другие комбинации известных фраз + MD5 хэширование внутреннего номера (например исполните команду “md5 -s ThePassword5000”)

7. Убедитесь, что контекст [default] достаточно рационален. Не допускайте неаутентифицированным входящим соединениям попадать в любые контексты, откуда исполняются платные вызовы. Ограничивайте количество активных звонков в дефолтном контексте (используя функцию “GROUP” в качестве счётчика). Запретите неаутентифицированные звонки (если вы действительно их не хотите) установкой параметра “allowguest=no” в секции [general] файла sip.conf.