Internet Telephony Services Providers' Association

Recommendations for Provisioning Security

Version 1

July 2014

Contact: admin@itspa.org.uk

Contents

About ITSPA

Founded in 2004, ITSPA is a membership-led organisation that represents predominantly network operators, service providers and other businesses involved with the supply of VoIP and unified communication services to business and residential consumers within the United Kingdom.

ITSPA helps act as the voice for the sector to key stakeholders; ensures that standards created by or imposed on industry are fair; leads on developments of best practice; campaigns on key issues that members face, promotes competition and self-regulation and serves as the leading networking forum for the UK VoIP industry with events throughout the year (including the annual industry awards – www.itspaawards.org.uk)

Members also receive complimentary subscription to the dispute resolution scheme CISAS; summaries of Ofcom (and other) consultation papers; regulatory briefing documents; Government monitoring and intelligence reports; updates from legal professionals; anti-fraud information; and the opportunity to collaborate with peers to promote career development.

Summary

- **Remote Provisioning delivers substantial benefits for ITSPs & End Users, but Provisioning Servers must be secured.**
- **Be very aware that Provisioning Servers are a prime target for attack.**
- **Authenticate Provisioning requests, ideally using HTTPS client certificates.**
- **Delete SIP passwords from SIP servers as soon as provisioned, if possible.**
- **Do not use TFTP for remote provisioning.**

Introduction

The ability for ITSPs to remotely provision phones & other SIP devices greatly improves service delivery and customer experience, however, remote provisioning can also enable serious security breaches if not handled carefully, as a provisioning server is a prime target for attacks to steal SIP credentials which are then used to make fraudulent calls.

By "Provision" we mean fully automated remote configuration and subsequent management, of SIP phones. When we say phone, we're referring to any SIP User Agent, including Handsets, Gateways, ATAs or Softphones.

The aim of the document is to share Best Common Practices among ITSPA members and these recommendations should be considered a starting point rather than a complete solution.

Background

Most SIP phones have a mechanism for fully automatic remote configuration / provisioning, which is sometimes referred to as Zero Touch Provisioning (ZTP). Service providers are able to register phones in a redirection server run by the phone manufacturer. The phone then 'Calls Home' to the redirection server and will then regularly contact a provisioning server to receive configuration and firmware updates.

Remote Provisioning is supported by most SIP phones used by many ITSPs in the UK to Provision and maintain their phones in the field. There are also some distribution companies who offer phone Provisioning and management as a hosted online service.
Phones can be Provisioned using a variety of communications protocols, each with different levels of security:

Protocol	Comments	Security Rating 1-5
TFTP	Use only on a secure LAN	1
HTTP	Usernames & Passwords pass in plain text	2
FTP	Usernames and passwords pass in plain text	3
HTTPS with manufacturer or ITSP certificates	General release certificates can be compromised	4
HTTPS with unique client / device certificates	Each phone is uniquely identified	5

Provisioning Communications Protocols

There is a strong commercial advantage to be able to ship phones from the manufacturer or distributor directly to the customer without opening the box, as besides avoiding double delivery costs, the phones are configured correctly and consistently without end user intervention.

Risks

When implemented correctly, Remote Provisioning benefits ITSPs, Resellers and End Users. When implemented badly, SIP usernames and passwords risk being exposed to the world as it's easy for an attacker to predict the MAC addresses of phones and scan servers. It's also possible to follow the redirections from manufacturer's redirection servers to onwardly scan the actual provisioning servers.

Unfortunately some ITSPs have been found to be placing provisioning files on open webservers with no authentication, and have been surprised when their customers' SIP credentials were harvested and used to make fraudulent calls. The good news is that when Remote Provisioning is sensibly secured the risks are minimal to all concerned.

What to do:

1. ITSPs who deploy Remote Provisioning Servers must consider security as an integral part of the design.
2. Authenticate phones using HTTPS client certificates.
3. Don't leave SIP passwords on the provisioning server:
    a. Delete the passwords once they have provisioned, if the handsets support configuration files without passwords.
    b. Where a configuration has been created but the phone has not accessed the configuration for longer than a pre-defined period of time (e.g. 2 weeks), the configuration should be pre-emptively removed from the server until the phone is ready to be provisioned.
4. Choose phone vendors who have a documented and audited authentication system for provisioning.
5. Keep provisioning server software up to date
6. Firewall your provisioning server with rate limits - review the logs for suspicious activity.
7. Regularly review security procedures and practices

What not to do:

1. Deploy a Provisioning Server that uses TFTP
2. Hand generate provisioning files
3. Have a directory listing on the server

HTTPS with client certificate authentication

HTTPS client certificates provide an excellent way to authenticate provisioning as the Provisioning server can cryptographically know which phone it is talking to. This is the ITSPA recommended way to authenticate provisioning requests.

Requirements for using HTTPS client certificate authentication

1. Certificate and key pair securely inserted into phone at the factory
2. Key cannot be extracted from the phone
3. Phone serial number or MAC address embedded in certificate
    a. So a unique certificate for each phone
    b. Server side software can read the MAC address from the certificate
4. Phone verifies the server certificate (like a normal HTTPS transaction)
5. Server software checks the MAC/Serial number in the certificate (do not trust URL parameters)
6. Public CA certificate for the provisioning server to validate the phone's certificates
7. Some documentation from the phone manufacturer about how this works, that will pass muster by ITSPs

Advantages of client certificates

1. No pre setup needed to by ITSP
2. Tried and tested method
3. Standard tools on the server side - apache, openssl etc.

Downsides

1. You have to trust your phone vendor to
    a. Keep their CA secure
    b. securely insert the keys

Softphone Considerations

Softphones can be difficult to provision securely because most require SIP credentials to be entered manually or to use the manufacturers provisioning server. ITSPs should consider how they intend to handle and communicate account information for softphone users. Ideally, avoiding email as a delivery mechanism and instead providing a "reveal" mechanism from a web page secured by login.

Wider Security

Although the primary focus of these guidelines is on provisioning of handsets, this is only one facet of a much wider topic. This section provides some topics for discussion and consideration by Service Providers with respect to the wider security of their service. This section is neither intended to be exhaustive nor normative.

Security is often mistakenly considered as an afterthought and not part of the core or initial design of the service. There is significant literature on this topic and how to include security as part of the inherent design of the platform, however it is generally accepted that security bolted on after the fact is a poor substitute.

The recommendations in this section assume that the service provider is controlling the configuration of the devices in question.

There are many device configuration best practices which can be enforced by a provisioning server

- In general, apply the principle that if a feature is not specifically requested or used it should be disabled. This may apply to management and monitoring tools as well as the primary functions.

- Most physical SIP devices provide an embedded management interface typically over HTTP or HTTPS. If the device is configured remotely and configured to "call home" on a regular basis, then these interfaces have extremely limited use. Service providers may wish to consider enabling the web interface on install if they perform attended installations or enabling the web interface only for diagnostic purposes. Call control functions may be more suitably handled through the service provider's own web interface than the device interface where bugfixes and security can more easily be applied.

- Regardless of whether the interface is enabled on the device, a suitably secure password should protect all access. Where possible, if end users are permitted access to the web interface, only those functions absolutely necessary should be

enabled for the end user. Service provider engineers may have access to additional functions. Given the ease of programmatically changing the configuration, consideration should be given to one-time passwords for engineer or administrative access.

- Most devices will allow call control functions or call features (e.g. call forwarding) to be configured via the web interface. Where possible, these should be disabled to prevent a would-be attacker from using these as an attack vector.

- Service providers are eager to ensure quality of service across their network and this extends to testing new firmware prior to deployment. Whilst this is commendable, consideration should be given to using the latest firmware and ensuring that security notifications from the provider are passed on to appropriately technical staff for evaluation. Firmware/software upgrades should be centrally controlled and enforced. Service providers should make use of the User-Agent string to provide a monitoring mechanism to ensure that software has been upgraded correctly.

- End customers should be encouraged where possible to ensure that SIP traffic from devices is only permitted to known, trusted destinations. SME and larger customers will be able to implement SPI on LAN firewalls etc. to ensure that only traffic to/from the service provider is permitted.

- All devices should be configured to only accept SIP requests from the registrar.

- Some phones store Passwords. Check that it is not possible to extract a SIP password from a phone. Only use for a password should be for digest authentication to a SIP server. You shouldn't be able to save a backup of the settings from the phone that includes the SIP Username & password.

- Network equipment frequently have SIP-specific proxies or ALGs that may assist in providing security to the LAN and the devices. Historically, however, such ALGs have proved to be problematic and so service providers and end customers may wish to consider a specific Session Border Controller instead.

- Auto-generated SIP credentials can be much stronger than those used by users, particularly where the SIP credentials are decoupled from any login credentials the user requires.

Local PBXs

Many SIP PBX systems include a provisioning server as part of the system. Installers should check carefully that this is available only to the portion of the network where it is required and protected from attack from the Internet. Again, security should be considered as part of the design and ensured at every stage of deployment since an attacker with local network access could still pose a threat where SIP credentials are easily accessible. As a best practice, we recommend that the same principles detailed in

this document should apply to both service providers and PBXs only serving internal users.

Finally, PBXs themselves offer management facilities and typically require manual provisioning where a SIP trunk is configured to the service provider. Authentication based on the IP address is insufficient and SIP authentication challenges should be required as part of both the initial registration as well as each subsequent call. Care should be taken to ensure that the PBX management interfaces are well protected from would-be attackers and that attempted intrusions are reported appropriately.

Notes

This paper was prepared by members of the ITSPA Operations Group and the ITSPA Secretariat. This guide has been prepared by the authors (who hereby assert their moral rights) on an 'as is' basis and is not intended to constitute advice on regulatory or any other matters, whether general or specific, and accordingly the authors disclaim all liability, however arising, from any reliance placed on this guide.

Acknowledgements

The following provided suggestions, advice or inspiration while creating this document.

- Tim Bray, Provu Communications
- David Cargill, RealCalls
- Peter Cox, UM Labs
- Aled Treharne, Siphon Networks
- Dan Winfield, Voxhub
- Cal Leeming